Intel® Authenticate

Integration Guide for Active Directory Group Policy Objects

Version 3.8

Document Release Date: 30 May 2019

Legal Notices and Disclaimers

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

Intel, Intel vPro, Intel Core, Xeon, and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Java is a registered trademark of Oracle and/or its affiliates.

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Intel is under license.

© 2016-2019 Intel Corporation

Table of Contents

Table of Contents ... **iii**

1 Introduction ... **1**
1.1 What is Intel® Authenticate? ... 1
1.2 Authentication Factors ... 2
1.2.1 Bluetooth® Proximity ... 2
1.2.2 Face Recognition ... 3
1.2.3 Fingerprint ... 4
1.2.4 Protected PIN ... 4
1.2.4.1 Protected PIN Settings ... 5
1.2.4.2 PIN Throttling Mechanism ... 5
1.2.5 Intel® AMT Location ... 6
1.2.6 Physical Smartcard ... 7
1.3 Actions ... 7
1.3.1 OS Login ... 8
1.3.1.1 Blocking the Windows* Password ... 8
1.3.2 VPN Login ... 9
1.3.3 Walk-Away Lock ... 10
1.3.4 Custom Actions ... 10
1.4 Intel Authenticate Components ... 11
1.4.1 Client and Engine ... 11
1.4.2 Policies ... 11
1.4.3 Factor Management Application ... 12
1.4.4 Intel Authenticate App ... 13
1.5 Deployment and Security Considerations ... 13
1.6 Support for Multiple Users ... 14

2 Client Platform Prerequisites ... **15**
2.1 Prerequisites for Installation ... 15
2.1.1 Data Migration After Firmware Upgrade ... 17
2.2 Prerequisites for Bluetooth Proximity ... 18
2.3 Prerequisites for Fingerprint ... 19
2.4 Prerequisites for Face Recognition ... 20
2.5 Prerequisites for Intel AMT Location ... 20
2.5.1 Configuring Home Domains Using Intel SCS ... 21
2.5.2 Configuring Home Domains Using ePo Deep Command ... 22
2.6 Prerequisites for Physical Smartcard ... 22
2.7 Minimum PowerShell Version ... 23
2.8 Firewall Policy ... 23
2.9 Using the Check Tool ... 24

*Other names and brands may be claimed as the property of others

2.9.1 Checking Installation Prerequisites 25
2.9.2 Checking Factors 27
2.9.3 Gathering Data Remotely via WMI 28

3 Setting Up VPN Login 31
3.1 Supported VPN Clients 31
3.2 Configuring the VPN Appliance 31
3.3 Defining the CA Template for VPN Login 32
3.4 Defining VPN Login in the Policy 33

4 Setting Up Certificate-Based OS Login 34
4.1 Considerations when Using Certificates 35
4.2 Defining the CA Template for OS Login 36
4.3 Defining Certificate-Based OS Login in the Policy 37

5 Setting Up Web Login 39
5.1 Defining the CA Template for Web Login 39
5.2 Defining a Web Login Action in the Policy 40

6 Integrating with GPO 42
6.1 Deployment Flow Using GPO 42
6.2 Server Requirements 42
6.3 Preparing a Digital Signing Certificate 43
6.4 Creating a Policy 45
6.5 Creating a Shared Folder 46
6.6 Creating WMI Filters for the GPOs 47
6.7 Creating a GPO to Discover Intel Authenticate 49
6.8 Creating a GPO to Install Intel Authenticate 53
6.9 Creating a GPO to Enforce the Policy 56
6.10 Creating a GPO to Reset the Policy 58
6.11 Upgrade Flow Using GPO 60

7 Troubleshooting 61
7.1 Troubleshooting Installation 61
7.2 Troubleshooting Enrollment 61
7.3 Troubleshooting OS Login 63
7.4 Troubleshooting Certificate-Based OS Login 64
7.5 Troubleshooting VPN Login 65
7.6 Troubleshooting Bluetooth Proximity 66
7.7 Troubleshooting Fingerprint 69
7.8 Troubleshooting Face Recognition 72
7.9 Troubleshooting Windows Hello 73
7.10 Using the Support Tool 74

*Other names and brands may be claimed as the property of others

7.10.1 Collecting Logs 75
7.10.2 Restarting Services and Processes 75
7.11 Event Viewer IDs 76

8 Other Certificate Management Options 79
8.1 Integrating with Third-Party Middleware 80
8.2 Manually Generating Certificates 81

*Other names and brands may be claimed as the property of others

1 Introduction

This guide describes how to integrate and use Intel® Authenticate with Active Directory Group Policy Objects (referred to in this guide as GPO).

Note:

Intel Authenticate also has separate integration packages to use when integrating with:

- McAfee* ePolicy Orchestrator (McAfee ePO)
- Microsoft* System Center Configuration Manager (SCCM)

For information about how to integrate and deploy with ePO or SCCM, refer to the guide in the relevant integration package.

1.1 What is Intel® Authenticate?

Intel Authenticate is a true multi factor authentication solution that supports the three different categories of authentication factors:

- Something the user knows, like a Personal Identification Number (PIN)
- Something the user has, like a smartphone
- Something the user is, like their fingerprint

The frequency of attacks on Enterprise environments is growing at an alarming rate. The starting point for many security breaches is a compromised login credential. These attacks are successful because most authentication systems store and process authentication data in the software layer. The process of comparing user-submitted data to the stored originals can be vulnerable to attack, modification, or monitoring when done within the environment of the operating system.

Intel Authenticate improves security for Enterprise applications and services by strengthening authentication factors and flows. Intel Authenticate supports authentication factors with different levels of security, where factors with the highest level are "hardened" and protected in the hardware of the Intel platform. This makes it difficult for malware and attackers to access or tamper with sensitive authentication data.

For each supported action (see Actions on page 7) you can define a combination of authentication factors (see Authentication Factors on the next page) that your end users can use.

Note:

On non Intel vPro systems, factor sets are limited to a maximum of two factors per set. For example, this factor set is not permitted: {Fingerprint AND Protected PIN AND Face Recognition}. Enforcing a policy that contains more than two factors in a factor set will fail on non Intel vPro systems. This restriction does not apply to Intel vPro systems. On Intel vPro systems, you can define as many factors per factor set as you want.

*Other names and brands may be claimed as the property of others

1.2 Authentication Factors

This section describes the authentication factors that are supported by Intel Authenticate.

1.2.1 Bluetooth® Proximity

This factor enables the user to enroll their personal / business smartphone as an authentication factor. The entire authentication process using the Bluetooth Proximity factor is automatic and does not require the user to do anything. All they need to do is have their enrolled phone with them when performing the action.

This factor has specific prerequisites (see Prerequisites for Bluetooth Proximity on page 18).

The security level of this factor depends on the combination of the user's phone and Windows* version.

Phone	Windows 7	Window 10 version 1607	Windows 10 version 1703 and higher
Android*	Protected	Protected	Protected
iPhone*	Protected	Soft	Protected (default) or Soft **Note:** On Windows 10 version 1703 and higher, the "Protected" security level when using iPhones can be less user friendly. For this combination you need to decide the correct balance of security versus usability for your organization.

This is how the different security levels work:

- **Protected** – The phone is enrolled to the user's platform using a secret code that only the phone and the platform share. The shared code is processed and protected by the hardware on the Intel platform. When the user performs an action for which Bluetooth Proximity is defined as an authentication factor, Intel Authenticate sends an authentication challenge to the phone. If the phone is in close proximity, then the challenge will succeed and the Bluetooth Proximity factor will be accepted. This security level requires the user to install a small app on their phone (see Intel Authenticate App on page 13).
- **Soft** – The phone is enrolled using only Windows Bluetooth pairing. As long as the operating system reports that the phone is "Connected", the Bluetooth Proximity factor will be accepted. This security level does not use any app on the phone.

*Other names and brands may be claimed as the property of others

The policy contains two entries for this factor (you only need to use one):

- **Protected Bluetooth Proximity** – Selecting this factor enables only the "Protected" security level. This means that users with Windows 10 version 1607 will NOT be allowed to enroll and use an iPhone with the Bluetooth Proximity factor.
- **Bluetooth Proximity** – Selecting this factor enables the relevant "Protected" and "Soft" security levels for each combination of phone and computer operating system (listed in the table above). For Windows 10 version 1703 and higher, the default setting for iPhone users is the "Protected" security level. But you can change the setting in the policy to make the "Soft" security level always enabled on these versions of Windows when using an iPhone.

During enrollment, Intel Authenticate automatically determines which security level to apply (based on the policy settings you defined) and the user's phone and computer operating system. The user is then guided through the necessary enrollment steps.

Changing the Security Level After Enrollment

On Windows 10 version 1703 and higher, it is possible to change the Bluetooth Proximity factor security level after the user has already enrolled their phone. To do this, you must enforce a new policy with the required security level setting. After the new policy is enforced, when the user tries to log in, authentication using their phone will fail. The user will need to log in using an alternative factor set, or their Windows password. A few minutes after login the Factor Management application will appear and display a message that they need to reenroll their phone. After reenrolling their phone, authentication with the phone will start working again.

1.2.2 Face Recognition

This factor enables the user to enroll their face and use it as an authentication factor.

This factor has specific prerequisites (see Prerequisites for Face Recognition on page 20).

Note:

This factor is not a "hardened" factor because the user's biometric data is usually only protected in the software. The level of protection depends on the security mechanism supplied by the vendor of the camera.

*Other names and brands may be claimed as the property of others

1.2.3 Fingerprint

This factor enables the user to enroll their fingerprints and use them as an authentication factor.

Intel Authenticate supports two types of fingerprint readers:

- **Protected Fingerprint Readers** – This type of fingerprint reader is designed to be fully self-contained using technology known as "Match on Chip". The Biometric data (the user's fingerprint) is protected and processed on the chip of the fingerprint reader. This makes it difficult for attackers to access or steal the user's fingerprint data.
- **Soft Fingerprint Readers** – This type of fingerprint reader is less secure because the user's Biometric data is usually only protected in the software. The level of protection depends on the security mechanism supplied by the vendor of the fingerprint reader. This type of fingerprint reader cannot provide the same level of protection as a protected fingerprint reader.

This factor has specific prerequisites (see Prerequisites for Fingerprint on page 19).

1.2.4 Protected PIN

This factor enables the user to create a Personal Identification Number (PIN) to use as an authentication factor. The PIN is created using a protected keypad displayed using Intel® Identity Protection Technology with Protected Transaction Display (Intel IPT® with PTD). These are the main security features of Intel IPT with PTD:

- Software based screen scraping or malware attacks that attempt to perform a screen capture of the keypad cannot view the actual PIN number layout. Instead, the entire keypad is blacked out.
- Each time the keypad window is presented, the numeric keypad is randomized. This means that the mouse click locations used to enter the PIN change every time. Capturing the mouse click pattern for successful PIN entry cannot be used for subsequent PIN entries.
- Mouse clicks for the PIN entry are translated and used within the protective hardware. The actual PIN value is not exposed outside of the hardware.
- A "PIN throttling mechanism" tracks the number of incorrect PIN entry attempts, and at specific intervals will refuse additional PIN attempts for a specific period of time. This feature minimizes brute force attacks on the PIN (see PIN Throttling Mechanism on the next page).
- Keyboard entry of the PIN is not allowed. This feature minimizes keyboard logger attacks.

Note:

When using multiple monitors, on some system configurations the keypad will be displayed on only one of the monitors and blacked out on the remaining monitors. And on some system configurations the keypad will be displayed on all of the monitors. This is expected behavior.

*Other names and brands may be claimed as the property of others

1.2.4.1 Protected PIN Settings

The Protected PIN settings enable you to define the complexity requirements for a valid PIN. When defining the Protected PIN factor in the policy, you can define these settings for the PIN:

- **Minimum PIN Length** – The minimum number of digits that the user must define for their PIN code. Valid values 4 – 10. The number of ascending sequential numbers the user can define in their PIN is limited to one less than the value of this setting. For example with a setting of 5, a PIN of "12345" is not valid, but a PIN of "12349" is valid.
- **Minimum Unique Digits** – The minimum number of unique digits that the user must define for their PIN code. Valid values 3 – 10. (The value cannot be higher than the value of the Minimum PIN Length.)

Note:

- The maximum PIN length that the user can define is 10 digits.
- If you change these settings, the new policy settings will not overwrite existing settings until the user re-enrolls the Protected PIN factor.

1.2.4.2 PIN Throttling Mechanism

The Protected PIN authentication factor has a built-in PIN throttling mechanism. This means that when a user enters an invalid PIN, an invalid PIN counter is started. After a number of invalid PIN entries, the system will enter a mode where PIN entry is locked out for a specific period of time. When locked, the user will be temporarily unable to complete any action for which Protected PIN is a mandatory authentication factor. This feature limits the effectiveness of brute force attacks against a user's PIN. As more invalid PIN attempts are made, the PIN entry lockout time period increases.

Number of Incorrect PIN Attempts	Time (in minutes) before Next PIN Attempt
1 – 4	0
5 – 7	1
8 – 11	10
12 +	30

The invalid PIN counter will reset to zero 60 minutes after the last invalid PIN attempt.

Note:

- The PIN throttling mechanism does not support separate invalid PIN counters for each user. The throttling mechanism, when activated, is activated for all users. (This means that all users of the platform will need to wait the required time before they can enter their PIN.)
- Entering a valid PIN does not reset the invalid PIN counter back to zero. If the counter was already a high value (because of several invalid PIN entries), future invalid PIN entries will activate the mechanism sooner than necessary.

*Other names and brands may be claimed as the property of others

1.2.5 Intel® AMT Location

This factor utilizes the Environment Detection feature of Intel® Active Management Technology (Intel® AMT). Mobile platforms typically operate in two distinct network environments:

- Inside the organization's network
- Outside the organization's network, for example using public hotspots and home networks

The Environment Detection feature is used to discover in which type of network the platform is operating. The feature is enabled by configuring DNS suffix names of "home domains" in Intel AMT. These home domains are networks that are considered to be a trusted part of the organization's network.

The Intel AMT Location authentication factor utilizes Environment Detection to enable you to define different authentication policies based on the location of the platform. Typically, you will define that actions will require more or stricter authentication factors when the platform is located outside your organization's network.

For example, you can define a combination of authentication factors like this:

Intel AMT Location **AND** Bluetooth Proximity

OR

Protected PIN **AND** Bluetooth Proximity

This combination means that when the platform is operating inside one of the home domains, the only required authentication factor is Bluetooth Proximity. But when operating outside the home domains, the user will also be required to authenticate using the Protected PIN factor.

This factor does not require any user input, but does require some configuration preparations on the platform before it can be used. For more information, see Prerequisites for Intel AMT Location on page 20.

Note:

- If the platform is connected through WLAN but no WLAN profiles are set, the Intel AMT Location factor enrollment will always fail.
- Typically, you will use this factor in conjunction with other factors. Using this factor as a single authentication factor effectively means that the authentication flow will only be possible if the platform is located inside your organization's network.
- If the user connects to the organization's network via a VPN connection, the Intel AMT Location factor will consider the platform to be outside the organizations network.

*Other names and brands may be claimed as the property of others

1.2.6 Physical Smartcard

This factor enables the user to enroll a physical Smartcard and use it as an authentication factor. The Smartcard is challenged as part of the authentication process and Intel Authenticate validates the correctness of the response. Intel Authenticate does not utilize the cryptographic secrets in the Smartcard for any actual cryptographic operations. To use this factor, you (and the user) must agree to allow Intel Authenticate to store and use the Smartcard PIN during authentication.

This factor has specific prerequisites (see Prerequisites for Physical Smartcard on page 22).

When defining the Physical Smartcard factor in the Intel Authenticate policy, you can define these settings:

- **Add Certificate** – To enroll and use this factor, the Intel Authenticate policy must contain a certificate from the certificate chain configured in the Smartcard. You can add up to five certificates to the policy. To add a Smartcard certificate to the policy you must prepare a ".cer" file in the X509 format.
- **If configured, allow Smartcard PINs to be stored and used by Intel Authenticate (if the user agrees)** – You must select this check box if you want to include the Physical Smartcard factor in the policy. During enrollment, if the Smartcard is configured to use a PIN, the user will be asked if they agree to allow Intel Authenticate to store and use the PIN. If the user does not agree, then they will not be permitted to enroll and use the Physical Smartcard factor. If the user agrees, after entering their PIN, the factor is enrolled. After the factor is enrolled the user will not be asked to enter the Smartcard PIN when authenticating using Physical Smartcard.
- **OIDs** – The Object Identifiers defined in the certificate configured on the Smartcard. When this field contains OIDs, only Smartcards that have all of these OIDs configured in their certificate are accepted by Intel Authenticate.
- **Reader Name (partial)** – The name of the Smartcard reader. This is NOT the name as it appears in "Device Manager > Smart card readers". To find the name of the Smartcard reader, use certutil.exe ("certutil.exe -scinfo -silent"). When this field contains text, only Smartcard readers that have this text in their name are accepted by Intel Authenticate. You can enter a partial name. If you use this field, make sure that the text you enter exists in all Smartcard readers that will be used with Intel Authenticate.

1.3 Actions

This section describes the actions that are supported by Intel Authenticate.

Note:

For most actions, you can define multiple authentication factors. More factors means more security, but usually reduces the usability for your end users. When defining the number and type of factors for each action, you need to balance the security requirements of your organization with the user experience.

*Other names and brands may be claimed as the property of others

1.3.1 OS Login

This action allows users to log in to the Windows operating system using Intel Authenticate instead of their Windows password. During login, a visual indication is shown in the Windows login screen letting the user know that they can use Intel Authenticate to log in. The user can then press Enter to log in to Windows using the authentication factors that you defined. The user will not be asked to supply their Windows password.

During login, the Intel Authenticate factors that you defined for OS Login are verified. If successful, Intel Authenticate releases credentials to Windows to complete the login process. If the platform is connected to a Domain, the user will also be automatically logged into the Domain. Windows takes care of the actual connection to the Domain, including any connected services such as Integrated Windows Authentication (IWA) and Active Directory Federation Services (ADFS).

You can define which type of credentials Intel Authenticate releases to Windows:

- **The User's Windows Password** – This is the default.
- **A Certificate** – When certificate-based authentication is enabled for OS Login, the login process is completed using a certificate. The certificate is generated and protected in the hardware of the Intel platform using Intel® Identity Protection Technology with Public Key Infrastructure (Intel® IPT with PKI). If authentication of the factors is successful, Intel Authenticate unlocks the certificate for Windows to complete the login process. Using this option can reduce the use of Windows passwords in your environment to a minimum. This option requires additional setup (see Setting Up Certificate-Based OS Login on page 34).

When the OS Login action is enabled using passwords, Intel Authenticate needs to save the user's Windows password. This means that the first login after enrollment must be performed using the Windows password. After that, the user can start to log in using Intel Authenticate.

1.3.1.1 Blocking the Windows* Password

To improve the chances that users will not try to bypass the requirements that you set for OS Login with Intel Authenticate, you have three different options. (Only implement one option.)

> **Note:**
>
> In both option #1 and option #2, after authentication is complete, it is still the Windows password that is released to Windows to complete the login process.

Option #1: Increase the Complexity of the Windows Password

To discourage your users from using their Windows password, you can increase the complexity of the requirements for the Windows password. When faced with the requirement to remember and enter a complex and long password, most users will simply opt to use Intel Authenticate to log in.

Option #2: Block the Password in the Policy

This option forces the user to log in by authenticating using the Intel Authenticate factors that you defined in the policy. To enable this option, in the Intel Authenticate policy, select the option named: **Block the user from using their Windows password to login**.

When this option is selected, after a user has successfully logged in using Intel Authenticate, the option to log in using their Windows password is disabled. Instead, a message is displayed telling the user that the IT department has disabled Windows password login.

Note:

In certain conditions, Intel Authenticate will still allow the user to log in with their Windows password:

- If Intel Authenticate detects that there is a system error or some other problem that will prevent the user from logging in with Intel Authenticate.
- If Intel Authenticate detects that it does not have the user's Windows password saved in the secure data store. (For example, the user changed their password or the password has expired.)

Option #3: Use Certificate-Based OS Login and Block the Password in Active Directory

This is the most secure option. When this option is fully enabled, the Windows password is never used. To enable this option:

1. Enable the certificate-based option of OS Login (see Setting Up Certificate-Based OS Login on page 34).
2. Make sure that your users have successfully enrolled their factors and can log in using Intel Authenticate and a certificate.
3. In Active Directory user account properties, select the option: **Smart card is required for interactive logon**.

Note:

When this option is enabled, the option to log in using a Windows password is still displayed to the user. But if they try to log in with a password, an error message is shown, like this: **You must use a smart card to sign in**.

1.3.2 VPN Login

This action allows users to log in to your organizations Virtual Private Network (VPN) using the authentication factors supported by Intel Authenticate. You configure the VPN client to use a certificate for authentication instead of a password. The certificate is generated and protected in the hardware of the Intel platform using Intel® Identity Protection Technology with Public Key Infrastructure (Intel® IPT with PKI). During login, the Intel Authenticate factors that you defined for VPN Login are verified. If successful, Intel Authenticate unlocks the certificate and passes it to the VPN client to log in to the VPN.

Before you can use this action, you need to configure the client systems and the VPN access point. For more information, see Setting Up VPN Login on page 31.

*Other names and brands may be claimed as the property of others

1.3.3 Walk-Away Lock

When this feature is enabled, the workstation is automatically locked when the user's enrolled phone is not in proximity (the user has "walked away" with his phone). When the user returns to their workstation, they will need to log in again using Intel Authenticate.

This feature depends on how accurately the phone / operating system report that the phone has moved out of range. This accuracy can differ between different phone models. In addition, the location of the phone (for example in the user's pocket) can cause false locks. To minimize false locks, before locking the computer all screens are dimmed for 5 seconds. If the user moves his mouse or uses his keyboard during these 5 seconds, the screen is not locked and Walk-Away lock is temporarily disabled. When a successful connection is re-established with the phone, Walk-Away Lock is enabled again.

Note:

- Walk-Away Lock is not a substitute for locking idle workstations after a certain period of time via your IT policies.
- Walk-Away lock is enabled using the Bluetooth Proximity factor (see Bluetooth® Proximity on page 2).
- Walk-Away lock is only available if the OS Login action or the VPN Login action is enabled in the policy.

1.3.4 Custom Actions

In addition to the built-in actions, Intel Authenticate also supports two types of "custom" action:

- **Web Login** - Allows users to log in to a specific web site that you define in the action. This type of action is supported for web sites that allow certificate based authentication. The certificate is generated and protected in the hardware of the Intel platform using Intel IPT with PKI. During login, the Intel Authenticate factors that you defined for the action are verified. If successful, Intel Authenticate unlocks the certificate and passes it to the web server to complete log in to the web site.
- **Application Login** - Allows users to log in to a specific third-party application that you define in the action. This type of action requires the third-party application vendor to integrate their product with Intel Authenticate. The third-party application vendor will define if they use certificate-based authentication or a different method.

You add custom actions in the Intel Authenticate policy. Web Login actions require additional setup (see Setting Up Web Login on page 39).

*Other names and brands may be claimed as the property of others

1.4 Intel Authenticate Components

This section describes the main components used by Intel Authenticate.

1.4.1 Client and Engine

Intel Authenticate software on the client platform is installed in these locations:

- `C:\Program Files\Intel\Intel Authenticate`
- `C:\Program Files (x86)\Intel\Intel Authenticate`

The software components on the client platform are divided into two logical levels: "Client" and "Engine". Each set of components is installed in a sub folder with the same name (Client and Engine).

On the client platform, Intel Authenticate relies on two services, described in this table.

Service Display Name	Description
Intel Authenticate: Client	This service mainly handles tasks at the operating system level. This includes communications with the Factor Management application (see Factor Management Application on the next page).
Intel Authenticate: Engine	This service mainly handles tasks that require communications with software applets in the firmware of the platform. Intel Authenticate installs and uses several applets in the Intel Dynamic Application Loader (Intel DAL). In addition, this service also manages Bluetooth connections used by Intel Authenticate.
Note: Both of these services must be running for Intel Authenticate to operate correctly.	

1.4.2 Policies

Policies contain the settings of Intel Authenticate that you want to enforce on the client platform. This includes the actions you want to enable, and the combination of authentication factors you want to define for each action. The method that you use to create and deploy the policy depends on the integration option that you decide to use (SCCM, GPO, ePO). After you create the policy, the policy is deployed to the client platforms and enforced. The user is then required to enroll the authentication factors defined in the enforced policy (see Factor Management Application on the next page).

Each client platform can have only one policy. But you can replace and then re-enforce policies as often as necessary when your requirements change.

Note:

Policies are protected by a signing certificate (see Preparing a Digital Signing Certificate on page 43). You can only replace a policy if the new policy is signed with the same certificate that was used to sign the existing policy on the platform. If you want to use a different signing certificate, you must first reset (remove) the existing policy before you can set the new policy.

*Other names and brands may be claimed as the property of others

1.4.3 Factor Management Application

The Factor Management application is a simple wizard that guides the end user through the process of enrolling the authentication factors. The Factor Management application automatically pops-up:

- Immediately after an Intel Authenticate policy is enforced (and no policy is currently enforced)
- At 24 hour intervals (from the last automatic pop-up), but only if:
  - Intel Authenticate detects that the user does not have enough factors enrolled to be able to successfully authenticate any action defined in the Intel Authenticate policy. This can occur if the user has not yet enrolled enough factors for an action or has unenrolled a factor and now does not have enough factors enrolled.
  - The Intel Authenticate policy was updated or renewed and now requires additional factors, not yet enrolled, to be able to successfully authenticate an action. (If you want the Factor Management application to pop-up immediately after a policy change, you will need to reset Intel Authenticate before enforcing the new policy. But that will require the user to reenroll all their factors.)
  - Walk-Away Lock is activated but the required Bluetooth Proximity factor is not enrolled

When enrollment is complete, the user can then start to use the features of Intel Authenticate, according to the settings you defined in the policy. The user cannot change the settings in the policy that you enforced.

After enrollment, the user can also open the Factor Management application at any time and use it to manage (re-enroll) their enrolled factors. For example, they can change their Protected PIN, or change the phone that they use for Bluetooth Proximity. When a user wants to re-enroll a factor, they must first authenticate themselves. By default, the user must authenticate using the same factor that they want to reenroll. If the user fails to authenticate during reenrollment, they will be asked to authenticate using other factors that are enrolled for the OS Login action. If the policy does not contain the OS Login action, they will be asked to authenticate factors that are enrolled for the VPN Login action.

Note:

- The Factor Management application is dynamic and displays screens and instructions according to the settings in the enforced policy. The enrollment process is fairly simple and takes only a few minutes. But it is recommended that you become familiar with the flow before deploying to your end users.
- A minimum screen resolution of 1024 x 768 is required to use the Factor Management application (lower resolutions are not supported).

*Other names and brands may be claimed as the property of others

1.4.4 Intel Authenticate App

The Bluetooth Proximity factor requires the user to install a small app on the phone that they want to use with Intel Authenticate.

> **Note:**
>
> The "Soft" security level of the Bluetooth Proximity factor does not use the app. During enrollment, users with this security level will not be asked to install the app or enter an enrollment code. For more information, see Bluetooth® Proximity on page 2.

The apps are published in Google Play (for Android phones) and the App Store (for iPhones):

- App Store: https://itunes.apple.com/app/intel-authenticate/id1171157350
- Google Play: https://play.google.com/store/apps/details?id=com.intel.auth13217

The Factor Management application includes download buttons in the Bluetooth Proximity page. The user will be asked to download and install the Intel Authenticate app directly to their phone as part of the enrollment processes. Alternatively, you can send the above links to your users and ask them to install the relevant app on their phone in advance of the actual enrollment process.

> **Note:**
>
> - On Android phones, the app is run as a background service. By default, many Android phones prevent background services from starting automatically. On these phones, the user will need to manually allow the Intel Authenticate app to automatically start. (If the app is not running in the background, Bluetooth Proximity verification will fail.)
> - On iPhones, the user must make sure that they do not close the app. Also, after the phone is restarted they will need to manually open the app.

1.5 Deployment and Security Considerations

The critical components of Intel Authenticate run in a Trusted Execution Environment (TEE) and thus have increased protection against attacks that might access or modify critical data or flows. However some Intel Authenticate components and interfaces must run at the operating system level.

Intel recommends performing the initial deployment and configuration in a controlled and secure environment. As Intel Authenticate cannot authenticate the administrator who performs the initial configuration, it does not conduct any checks during the initial configuration stage. All subsequent administrative actions (for example, setting a new policy), however, are permitted only if they are authorized under the credentials (certificate) set in the initial configuration.

Intel Authenticate provides mechanisms that will enable the administrator to verify that the current policy is the expected policy. For more information, refer to the attestation guide in the `Tools` > `Attestation` folder.

Intel Authenticate also provides a reset mechanism to clear the policy and all enrollment data on the platform. For example, an administrator might use this "reset" functionality if the currently configured credentials are suspect or corrupt. Performing a reset deletes all enrolled data.

*Other names and brands may be claimed as the property of others

1.6 Support for Multiple Users

Intel Authenticate supports enrolling and using up to five different user accounts on the same computer.

These are important points to understand before you implement multiple users:

- Enrollment of more than five users is not blocked. But if you do enroll more than five users, Intel Authenticate will not work as expected.
- After dismissing the Windows 10 curtain, the login process will not start automatically. The user will have to either press Enter or click **Log on** to actually log in to Windows.
- When using the Bluetooth Proximity factor, having more than one user signed in at the same time is NOT supported. This means that before a different user can log in:
  - All other users must first completely log off. Simply locking the computer when changing users is not supported.
  - The "Switch User" option is not supported. You can block the "Switch User" option in group policy by enabling this setting: `Computer Configuration` > `Administrative Templates` > `System` > `Login` > `Hide Entry Points for Fast User Switching`.

*Other names and brands may be claimed as the property of others

2 Client Platform Prerequisites

This section describes the prerequisites for Intel Authenticate on the client platforms.

Note:

- The versions listed in this section are the minimum versions that are supported. But, unless stated otherwise, it is always recommended to use the latest released version for each prerequisite.
- You can use the Check tool to determine if a platform meets the prerequisites (see Using the Check Tool on page 24).

2.1 Prerequisites for Installation

This table describes the minimum requirements for installing Intel Authenticate on the client platforms.

Prerequisite	Details
Processor	The platform must have a 6th generation (or higher) processor belonging to one of these families of processors: • Intel® Core™ • Intel® Core™ M • Intel® Core™ vPro™ • Intel® Core™ M vPro™ • Intel® Xeon® E3 (v5 or higher) • Intel® Xeon® E-2186M • Intel® Xeon® E-2176M

Intel ME Firmware	Intel Authenticate is supported on Intel Management Engine Firmware Corporate SKU version 11.8.50.3399 or higher.
	
	Note:
	• Although not supported, installation on some earlier versions is not blocked:
	  • Intel ME 11.7
	  • Intel ME 11.6: Version 11.6.0.1117 or higher
	  • Intel ME 11.0: Version: 11.0.0.1157 or higher (version 11.0.0.1202 is the minimum version for platforms that have the Intel Sensor Service enabled)
	• For security reasons, it is highly recommended to upgrade earlier Intel ME Firmware versions to 11.8.50.3399 or higher. For more information, refer to the official communication here.
	• The Consumer SKU is NOT supported.

*Other names and brands may be claimed as the property of others

Prerequisite	Details
Intel ME Software	Intel Management Engine Software must be installed. The minimum supported version is 11.6.0.1019 (but always install the latest version available for the platform). **Note:** The latest versions of Intel ME Software can also be installed using individual ".inf" files for each component. If installation was done using .inf files, then the "Intel Management Engine Components" entry will not exist in "Program and features". The Check tool will report a failure if any of these components are not installed: • Intel Capability Licensing Service TCP IP Interface Service (installed by `iclsClient.inf`) • Intel Dynamic Application Loader Host Interface Service (installed by `DAL.inf`) • Intel Management and Security Application Local Management Service (installed by `LMS.inf`) • Intel Management Engine Interface service (installed by `heci.inf`)

Operating System	• Windows* 10 version 1903 (64-bit):
	  • Minimum version: 10.0.18362.86
	• Windows 10 version 1809 (64-bit):
	  • Minimum version: 10.0.17763.55
	• Windows 10 version 1803 (64-bit):
	  • Minimum version: 10.0.17134.48
	• Windows 10 version 1709 (64-bit):
	  • Minimum version: 10.0.16299.125
	• Windows 10 version 1703 (64-bit):
	  • Minimum version: 10.0.15063.540
	• Windows 10 version 1607 (64-bit):
	  • Minimum version: 10.0.14393.222
	• Windows 7 (32-bit and 64-bit)
	Note: On Windows 7 only, this hotfix is also required: KB3033929. If not installed, the OS Login certificate-based option will not work.

Integrated Graphics	Version 21.20.16.4481 or higher of the Intel HD Graphics driver must be installed. **Note:** Some Intel Authenticate features rely on capabilities provided by Intel IPT with Protected Transaction Display. These capabilities require an Intel CPU with integrated graphics to be defined as the primary graphics driver. On some platforms that also have discrete graphics, a switchable graphics feature might be enabled. Intel Authenticate only supports the switchable graphics feature if the discrete graphics driver can automatically transfer ownership to the integrated graphics when Intel IPT with PTD is required.

*Other names and brands may be claimed as the property of others

Prerequisite	Details
Transport Layer Security	Transport Layer Security (TLS) must be enabled
.NET Framework	The Factor Management application requires .NET Framework version 4.5.2 or higher

2.1.1 Data Migration After Firmware Upgrade

Most upgrades of the Intel ME Firmware do not affect the data stored in the Intel ME Firmware. But sometimes, for security reasons, the firmware upgrade changes the Platform Binding Key (PBK). The PBK is a unique security identifier in the Intel ME Firmware that is used to secure the data. When the PBK changes, the data in the Intel ME Firmware is rendered invalid. You have two choices how to deal with this type of upgrade:

- **Reset Intel Authenticate** - This is the default behavior. After upgrade, to make Intel Authenticate work again, you will need to reset Intel Authenticate and then set the policy again. In addition, the end users will need to re-enroll all their factors. (To reset Intel Authenticate, see Creating a GPO to Reset the Policy on page 58.)
- **Enable Data Migration** - When this option is enabled, if Intel Authenticate detects that the PBK has changed the data will be automatically "migrated" to use the new PBK. This means that there is no need to reset Intel Authenticate. After data migration has occurred, the user will be asked to login once with their Windows password. After that, Intel Authenticate will continue to work as normal.

> **Note:**
>
> When the PBK changes, all certificates used for VPN Login, certificate-based OS Login, and custom actions are also rendered invalid and must be renewed. If Intel Authenticate is defined to manage these certificates, they will be automatically renewed after data migration. But if Intel Authenticate is not managing the certificates you will need to manually renew them.

To enable data migration, change the default value of this registry key (after installation):

- `HKLM\SOFTWARE\Intel\Intel Authenticate\Engine\DataMigrationOptIn`
- New value: **1**

*Other names and brands may be claimed as the property of others

2.2 Prerequisites for Bluetooth Proximity

The Bluetooth Proximity factor requires an Intel wireless card with integrated Bluetooth on the platform, and a smartphone. The smartphone can be the user's personal or business phone and can be an Android phone or an iPhone. This table describes the minimum requirements for Bluetooth Proximity (and Walk-Away Lock).

Prerequisite	Details
Wireless Card	• Intel WiFi 6 AX200 • Intel Wireless-AC 9560 • Intel Wireless-AC 9260 • Intel Dual Band Wireless-AC 8265 • Intel Tri-Band Wireless-AC 18265 • Intel Dual Band Wireless-AC 3168 • Intel Dual Band Wireless-AC 8260 • Intel Tri-Band Wireless-AC 18260 • Intel Dual Band Wireless-AC 7265 • Intel Dual Band Wireless-AC 3165 **Note:** These wireless cards are only supported by Intel Authenticate when they are installed on a platform and operating system that are fully supported by the wireless card.
Drivers	Both the network adapter driver and the Intel® Wireless Bluetooth® driver of the card must be installed on the platform. **Note:** The minimum supported version of the Intel Wireless Bluetooth driver is 19.00.1626.3453. But Intel recommends to use version 20.60.0.4 or higher.
Operating System on Phone	• On Android Phones: Android version 6.0 to version 9.0 • On iPhones: iOS version 10.1 to version 12.1
App on the Phone	• On Android Phones: `IntelAuthenticate.apk` • On iPhones: `IntelAuthenticate.ipa` ("Protected" security level only) **Note:** For more information, see Intel Authenticate App on page 13.

Note:
• On Windows 10 version 1803, when using Android phones, the minimum supported version is 10.0.17134.320.
• Bluetooth Proximity (and Walk-Away Lock) using iPhones:
  • Is only supported when using iPhone* 5S or higher (iPhone 5 and iPhone 5C are not supported).
  • Is only supported on Windows 7 if the platform has an Intel Dual Band Wireless-AC 8260 card.	

*Other names and brands may be claimed as the property of others

2.3 Prerequisites for Fingerprint

The Fingerprint factor has these basic prerequisites:

- A fingerprint reader with the correct fingerprint reader driver installed
- On Windows 7, the Fingerprint Management Application (FMA) supplied with the fingerprint reader must be installed. (On Windows 10, Intel Authenticate integrates with the Windows Biometric Framework which is part of Windows 10.)

How the fingerprint reader will be supported by Intel Authenticate depends on additional prerequisites. To identify the type of fingerprint reader on a platform, you can use the `/F /V` flags of the Check tool (see Checking Factors on page 27).

Protected Fingerprint Readers

Intel Authenticate supports a fingerprint reader as a "Protected Fingerprint" reader only if both of these prerequisites exist:

1. The fingerprint reader has one of these hardware IDs (in Device Manager > Biometric devices > Details):

VID_138A&PID_0090	VID_06CB&PID_009A
VID_138A&PID_0092	VID_06CB&PID_00A2
VID_138A&PID_0097	VID_06CB&PID_00BD
VID_138A&PID_009D	VID_06CB&PID_00BE
VID_138A&PID_00A4	VID_06CB&PID_00C2
VID_138A&PID_00AB	
VID_138A&PID_00B6	

2. The installed fingerprint reader software supports integration with Intel Authenticate.

Soft Fingerprint Readers

Any platform that does not have all the "Protected Fingerprint" prerequisites is supported as a "Soft Fingerprint" reader.

Note:

In the Intel Authenticate policy settings you can specifically select which type of fingerprint factor you want to enable. If the policy contains only the "Protected Fingerprint" factor, it will not be possible to enroll the fingerprint factor on platforms that have a Soft Fingerprint reader. If your network contains PCs with both types of reader, it is recommended to define only the "Fingerprint" factor in the policy. Setting only the "Fingerprint" factor in the policy actually means that you want to allow either type of factor to be enrolled and used. Intel Authenticate will automatically detect and enroll the fingerprint factor according to the type of fingerprint reader that exists on the platform ("Protected" or "Soft").

*Other names and brands may be claimed as the property of others

2.4 Prerequisites for Face Recognition

The Face Recognition factor has these specific prerequisites:

- Windows 10.0.14933.222 or higher
- A camera that is supported by Windows Hello. Supported cameras are usually three-dimensional, infra-red cameras that can use the Windows Biometric Framework (WBF). For more information, refer to the Microsoft documentation.
- The GPO computer configuration policy must allow the user to log on using biometrics. In Windows 10, if you do not enable the relevant GPO settings, the Windows Hello options in the "Sign-in options" page are disabled (see Troubleshooting Windows Hello on page 73).

2.5 Prerequisites for Intel AMT Location

The Intel AMT Location factor has these specific prerequisites:

- Platform: Intel® vPro™ system
- Intel ME Firmware: Version 11.0.15.1003 or higher
- Configuration status: Intel AMT must be configured with home domains (if Intel AMT is configured, but no home domains are configured, enrollment and use of this factor will fail)
- IP address: Dynamic IP address (Static IP addresses are NOT supported)

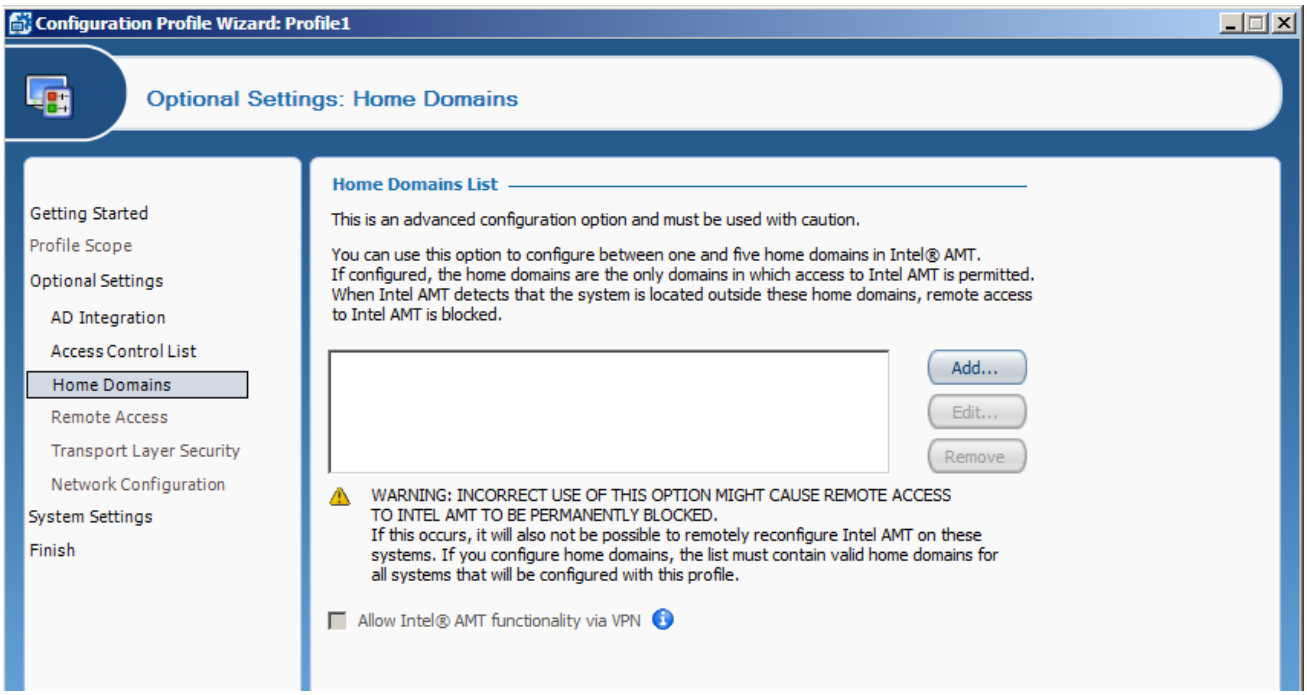
Intel AMT includes many different options and configuration methods. The only requirement for the Intel AMT Location factor is that Intel AMT is configured with home domains. You can configure Intel AMT using host-based configuration (easiest method) or remote configuration (requires more setup). After home domains are configured you can use the Intel AMT Location authentication factor.

You can configure Intel AMT using Intel® Setup and Configuration Software (Intel® SCS), or using McAfee ePO Deep Command. Configuring Intel AMT is beyond the scope of this guide. The information presented here is to help you understand the location of the home domains settings. For complete information about configuring Intel AMT, refer to the documentation of Intel SCS or McAfee ePO Deep Command.

*Other names and brands may be claimed as the property of others

2.5.1 Configuring Home Domains Using Intel SCS

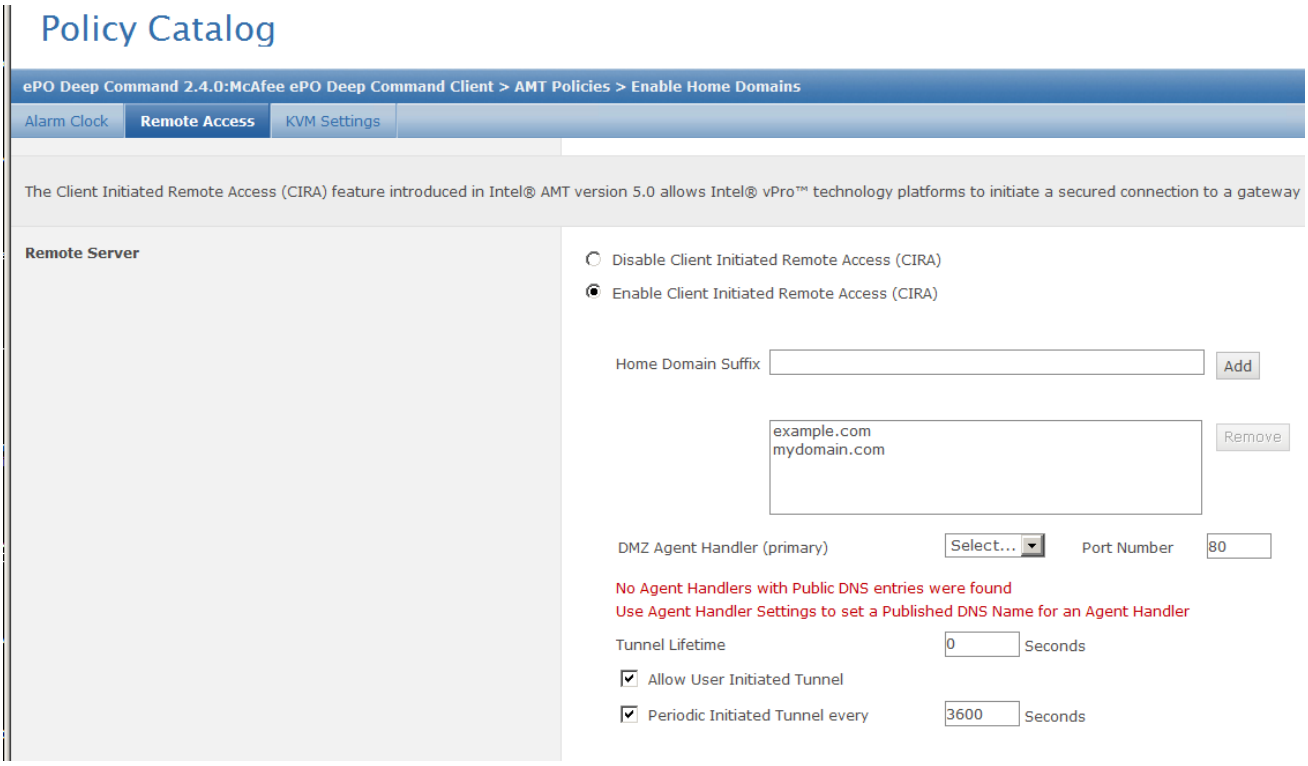
When using Intel SCS, the quickest option to configure Intel AMT is to use the Intel AMT Configuration Utility. You do not need to install the Remote Configuration Service (RCS) component of Intel SCS. When defining the configuration profile (using the Configuration Profile Wizard), define the home domains in the Home Domains window. You can define between one and five home domains.



*Other names and brands may be claimed as the property of others

2.5.2 Configuring Home Domains Using ePo Deep Command

In McAfee ePO Deep Command, the home domains settings are located in the Remote Access tab of the policy. The home domains settings are also used to implement the Client initiated Remote Access (CIRA) capability of Intel AMT. To use the Intel AMT Location factor, you only need to configure the host domains. It is not necessary to setup your environment for CIRA.



2.6 Prerequisites for Physical Smartcard

The Physical Smartcard factor has these specific prerequisites:

- Windows 10.0.14393.222 or higher
- A Smartcard reader that is either integrated into the platform, or connected to the platform via USB
- The Smartcard reader must support the Chip Card Interface Device (CCID) protocol
- To enroll and use this factor, the Intel Authenticate policy must contain a certificate from the certificate chain configured in the Smartcard. You can add up to five certificates. To add a Smartcard certificate to the policy, you must prepare a ".cer" file in the X509 format.

*Other names and brands may be claimed as the property of others

2.7 Minimum PowerShell Version

This integration solution relies on scripts that were written in PowerShell 3.0. For these scripts to work correctly, version 3.0 or higher of PowerShell must be installed. This means that you must make sure that PowerShell version 3.0 or higher is installed on all client platforms where you want to use this integration solution. You can check the PowerShell version using this PowerShell command: `get-host`.

2.8 Firewall Policy

When using a Firewall, some policies can prevent Intel Authenticate from working when the user is outside the organizations network. This can occur if the Firewall policy blocks access to a service named "JHI_SERVICE.exe". On any Firewall that blocks traffic to local host, this rule needs to be applied on all client platforms:

Allow incoming traffic:

- From: LocalHost
- To process: JHI_SERVICE.EXE
- Port: Any

*Other names and brands may be claimed as the property of others

2.9 Using the Check Tool

The Check tool is a CLI-based tool, located in the `Tools > CheckTool` folder. The Check tool is also installed on the client platforms in this folder: `C:\ProgramData\Intel\Intel Authenticate\Engine\CheckTool`.You can use this tool to verify the status of prerequisites on the platforms. The CLI syntax is not case-sensitive. This is the syntax:

```
Authenticate_Check.exe { /P | /F | /? | /WMI | /SCCM } /V
```

Flag	Details
`/P`	Checks if the platform meets the installation prerequisites for Intel Authenticate (see Checking Installation Prerequisites on the next page)
`/F`	Checks the status of each authentication factor supported by Intel Authenticate (see Checking Factors on page 27)
`/V`	Adds more detailed information to the output (only when used with the `/F` flag)
`/WMI`	Generates WMI discovery data for collection by third party tools (see Gathering Data Remotely via WMI on page 28)
`/SCCM`	Generates WMI discovery data for collection by Microsoft SCCM (see Gathering Data Remotely via WMI on page 28)
`?`	Help

Note:

The Check tool:

- Must be run from a command prompt that was opened with administrator privileges.
- Requires .NET Framework version 4.5.2 or higher.
- Relies on the Intel MEI driver to run some of the tests. If the Intel MEI driver is not installed, these tests might fail.
- On Windows 7, if a message shows stating that a DLL named "`api-ms-crt-runtime-[1-1-0.dll`" is missing, run Windows update. Alternatively you can install this KB2999226.

*Other names and brands may be claimed as the property of others

2.9.1 Checking Installation Prerequisites

Intel Authenticate is only supported on platforms that meet the installation prerequisites (see Prerequisites for Installation on page 15). The `/P` flag of the Check tool provides information about the status of these prerequisites, and determines if the platform is supported.

Note:

- The installation prerequisites are the minimum requirements for the platform to be supported. Some of the authentication factors also have additional prerequisites that you can check using the `/F` flag.
- You can also use the `/P` flag to help troubleshoot problems when Intel Authenticate is not working correctly. For example, if the Intel DAL service is not running, Intel Authenticate will not work correctly.

To check the installation prerequisites:

```
Authenticate_Check.exe /P
```

When all tests pass, the result summary is highlighted in green.

```
D:\CheckTool>Authenticate_Check.exe /p

#######  Intel(R) Authenticate Prerequisites Test #######


     1. PASS - CPU : Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz
     2. PASS - Intel ME Software version : 11.7.0.1043
     3. PASS - Intel ME Firmware version : 11.8.50.3425
     4. PASS - Intel ME Firmware type : Corporate
     5. PASS - OS version : Windows 10 (x64) (10.0.15063.726)
     6. PASS - Transport Layer Security: Enabled
     7. PASS - Intel DAL service : Installed and running
     8. PASS - Intel DAL version : 11.7.0.1043
     9. PASS - Intel Graphics Driver version : 22.20.16.4785

Status: This platform includes all prerequisites for Intel Authenticate


#### Prerequisites Test Passed ##################
```


*Other names and brands may be claimed as the property of others

If one of the tests fail, the result summary is highlighted in red. For each failed test, details are shown.

```
D:\Tools\CheckTool>Authenticate_Check.exe /p

#######  Intel(R) Authenticate Prerequisites Test #######


    1. PASS - CPU : Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz
    2. FAIL - Intel ME Software version : 11.0.4.1186
    3. WARN - Intel ME Firmware version : 11.0.0.1202
    4. PASS - Intel ME Firmware type : Corporate
    5. PASS - OS version :  Windows 10 (x64) (10.0.14393.447)
    6. PASS - Transport Layer Security: Enabled
    7. PASS - Intel DAL service : Installed and running
    8. PASS - Intel DAL version : 11.0.4.1186
    9. FAIL - Intel Graphics Driver version : 20.19.15.4402
Status: This platform does not support Intel Authenticate

Details:
    Test # 2: Supported Intel ME Software version: 11.6.0.1019 or higher
    Test # 3: By default, installation is blocked on any Intel ME Firmware version lower than version 11.8.50.3399. For
more information, refer to the documentation.
    Test #9:  Supported Intel Graphics Driver version: 21.20.16.4481 or higher


#### Prerequisites Test Failed ###################
```

This table describes the tests run by the `/P` flag.

Test	Details
1	Checks that the processor belongs to one of the supported families of processors. **Note**: Test #1 shows a warning on engineering sample, pre-quality sample, and quality sample platforms. This is because on these types of platforms the CPU returns an unrecognized value. Ignore this warning.
2	Checks the registry to verify that the installed version of Intel ME Software is supported. In addition, this test also checks that the Intel MEI driver is installed. The driver is usually located in the "System devices" section of the Device Manager window. If the driver is not installed, some of the remaining tests will fail (because they depend on communications via the driver).
3	Checks that the Intel ME Firmware version is supported
4	Checks that the Intel ME Firmware is the Corporate SKU (the Consumer SKU is not supported)
5	Checks that the operating system is supported
6	Checks that the Transport Layer Security is enabled **Note:** If the Intel ME Software is not installed, this test will fail and return a value of "Unknown". This will cause the platform status to be reported as not supported (even though there is a good chance that it can support Intel Authenticate). Install the ME Software and run the tool again.
7	Checks that the Intel DAL service is installed and running (the name shown in the Services window is "Intel Dynamic Host Application Loader Host Interface Service")
8	Checks communications with Intel DAL by trying to get the version number of Intel DAL via an API of Intel DAL
9	Checks that the Intel Graphics Driver is installed and that the version is supported

2.9.2 Checking Factors

Each of the authentication factors supported by Intel Authenticate have different dependencies that must be present on the platform before they can be used. The `/F` flag of the Check tool provides information for each factor and determines if the factor is supported.

To check the status of factors:

```
Authenticate_Check.exe /F
```

> **Note:**
>
> For more detailed information about each factor, add the `/V` flag.

```
####### Intel (R) Authenticate Factors Test #######


Factor:         Bluetooth Proximity (Android)
Status:         Ready For Use

Factor:         Bluetooth Proximity (iOS)
Status:         Ready For Use

Factor:         Intel AMT Location
Status:         Supported

Factor:         Fingerprint
Status:         Ready For Use

Factor:         Protected PIN
Status:         Ready For Use

Factor:         Face Recognition
Status:         Not Supported
Reason:         A supported facial recognition camera was not detected.

Factor:         Physical Smartcard
Status:         Supported
```


*Other names and brands may be claimed as the property of others

This table describes the output reported by the `/F` flag.

Section	Details
Factor	The name of the factor

Status	These are the possible statuses for each factor:
	• **Not Supported** – The factor is not supported by the current configuration of the platform. This can include missing software or unsupported versions of hardware or software. The details are shown in the "Reason" section. You can run the tool again after you have fixed the detected problems that are possible to fix (for example, by upgrading software).
	• **Supported** – The factor is supported but not ready for use by Intel Authenticate. This status is expected for these factors:
	  • Face Recognition – The status will change to "Ready For Use" only after Intel Authenticate is installed.
	  • Soft Fingerprint – The status will change to "Ready For Use" only after Intel Authenticate is installed.
	  • Intel AMT Location – This factor can only be used for authentication after the IT Admin has configured home domains in Intel AMT. (Even after home domains are configured, this factor does not return a value of "Ready For Use".)
	  • Physical Smartcard - This factor will never show a status of "Ready For Use".
	• **Ready For Use** – All prerequisites for the factor exist on the platform and the factor is ready for use by Intel Authenticate.

Reason	This section is shown when the status of a factor is "Not Supported". Information is shown for each problem that is preventing Intel Authenticate from using a factor.
Info	This section is shown when you supply the `/Verbose` flag and provides additional information about the dependencies for each factor.

2.9.3 Gathering Data Remotely via WMI

Windows Management Instrumentation (WMI) is a built-in component of the Windows operating system that you can use to remotely collect data from platforms in your network. The Check tool has two different flags that can prepare this data on the platforms:

- `/WMI` - Generates WMI discovery data in "`root\cimv2`" for collection by third party tools
- `/SCCM` - Generates WMI discovery data in "`\root\cimv2\sms`". This data can then be automatically collected by the hardware inventory mechanism of SCCM. Run this command only on platforms that are managed by SCCM. For the data to be collected to the SCCM database, you must also install the Intel® Authenticate Add-on for Microsoft* SCCM on the SCCM server.

For instructions how to use WMI, refer to the Microsoft documentation.

The following sections describe the Intel Authenticate WMI classes and their content.

*Other names and brands may be claimed as the property of others

Class: Intel_Authenticate_System

This class is always populated and includes the data returned by the `/P` flag and some additional information.

Key_Name	Value	More_Info
Intel Authenticate Supported	• Not Supported • Not Ready • Supported	In most cases this field will contain a value of N/A (Not Applicable). But if there is a problem with one of the prerequisites, then this field will contain the failure reasons.
CPU	The processor name	
Intel Authenticate Engine-only installed	Yes / No **Note:** If the value is "Yes", then you must uninstall the Engine component before you can install the full Intel Authenticate product.	
Intel Authenticate Installed	Yes / No	
Intel ME Software Version	The Intel ME Software version	
Intel DAL service	Installed and running / Unknown	
Intel DAL version	The Intel DAL version / Unknown	
Intel Graphics Driver version	The Intel Graphics Driver version	
Intel ME Firmware type	Corporate / Consumer	
Intel ME Firmware version	The Intel ME Firmware version	
Intel ME Software version*	The Intel ME Software version	
OS version	The operating system version	
Policy Applied*	Yes / No	
Transport Layer Security	Enabled / Not Supported / Unknown **Note:** A value of "Unknown" usually occurs because the Intel ME Software is not installed. This will cause the platform status to be reported as Not Supported (even though there is a good chance that it can support Intel Authenticate). Install the ME Software and run the tool again.	
* These entries will only exist if Intel Authenticate is installed		

*Other names and brands may be claimed as the property of others

Class: Intel_Authenticate_Factors

This class is always populated and includes the data returned by the `/F` flag.

Factor	Status	Info	Reason
The authentication factor. Possible values: • Bluetooth Proximity (iOS) • Bluetooth Proximity (Android) • Face Recognition • Fingerprint • Intel AMT Location • Protected PIN • Physical Smartcard	The status of the factor. Possible values: • Not Supported • Supported • Ready For Use	Contains additional information about the dependencies for the factor	If the value of "Status" is "Not Supported", this field contains information for each problem that is preventing Intel Authenticate from using the factor.

Class: Intel_Authenticate_Actions

This class only exists if the policy has been set.

Action	Policy
Contains the factor authentication "sets" that are configured for each of the actions defined in the policy configured on the platform. Each action will have several entries with numbers (X in this example) per the number of factor sets defined for the action. The number of the set defines the order in which the sets will be authenticated for that action. Possible values: • OS_Login_Setx • VPN_Login_Setx • WalkAwayLock_Setx	Contains a list of the factors defined for this action set

Class: Intel_Authenticate_Users

This class only exists if the user has enrolled some factors.

User	Enrolled Factors
Contains an entry for each user	Contains a list of all the factors that the user has actually enrolled

*Other names and brands may be claimed as the property of others

3 Setting Up VPN Login

This section describes what you need to prepare before you can use the VPN Login action.

3.1 Supported VPN Clients

Intel Authenticate supports VPN clients that use the standard Microsoft Cryptographic Application Programming Interface (CAPI) to the Credential Service Provider (CSP). These specific VPN clients were tested and validated to work with Intel Authenticate:

- Cisco*
- Microsoft*

Additional VPN clients, for example Juniper*, are expected to work but have not been fully validated.

3.2 Configuring the VPN Appliance

To use the VPN Login action, you must configure your VPN appliance to use certificates instead of passwords. For instructions how to define your VPN appliance to use certificates, refer to the documentation supplied with your VPN appliance.

Object Identifiers (OIDs)

Most VPN appliances use Object Identifiers (OIDs) to enable them to identify the VPN certificate in the certificate store. If your VPN appliance uses OIDs, you will be asked to define this OID when setting up the VPN appliance. You must make sure that you define the same OID in the VPN appliance and in the VPN certificate template. To define the OID in the certificate template, use the -o <OIDs> flag of the Certificate Template Tool (see Defining the CA Template for VPN Login on the next page).

Note:

- Check the maximum number of characters supported by your VPN appliance. Many VPN appliances limit the size of the OID to less than 30.
- Microsoft VPN does not use OIDs.

*Other names and brands may be claimed as the property of others

3.3 Defining the CA Template for VPN Login

The Certificate Template tool is a simple executable used to create certificate templates with settings that are ready to work with the Intel Authenticate certificate-based features. It is recommended to verify that the template works as expected before making any changes to the settings defined by the tool.

Note:

- The tool requires .NET Framework version 4.5.1 or higher. If not installed, the tool will throw an exception.
- You must run the tool with a user account that has the necessary permissions to create and publish certificate templates in your network environment. The user account used to run the tool will be made the owner of the certificate template that is created.

To create a VPN certificate template:

1. Copy the `Tools\CertificateTemplateTool` folder to the server where you want to create the VPN certificate template.
2. Open a command prompt as an administrator (in the `CertificateTemplateTool` folder).
3. Type in this command:

```
CertificateTemplateSetup.exe -c create -s no -n <template_name>
-d <display_name> -o <oids>
```

Parameter / Variable	Description
`-n <template_name>`	The name of the template (cannot contain spaces)
`-d <display_name>`	An optional display name
`-o <oids>`	Use this parameter to add OIDs to the Application Policies Extension. This is a requirement for most VPN appliances (see Configuring the VPN Appliance on the previous page). Each OID must be separated with a "," . OIDs can be defined using names or numbers. For example: -o "secure email,1.3.6.1.2000"

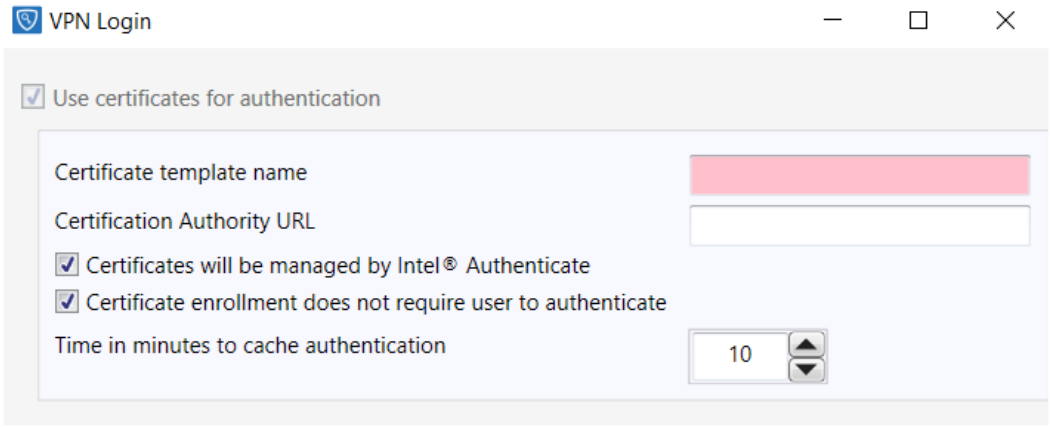
4. Press <Enter>. The Select Certification Authority window opens.
5. Select the CA on which you want to create the template and click **OK**. The template is installed and issued.

*Other names and brands may be claimed as the property of others

3.4 Defining VPN Login in the Policy

When VPN Login is enabled, each user account requires a VPN certificate to be installed in their certificate store on the client platform. This section describes important settings in the Intel Authenticate policy that define how these certificates are generated. Refer back to this section when you define the policy (see Creating a Policy on page 45).

The settings are located in the Advanced Settings section of the VPN Login action:



Setting	Description
Use certificates for authentication	This check box cannot be disabled because VPN Login is only supported when using certificates.
Certificate template name	The exact name of the certificate template to use for VPN Login. This field is mandatory when certificates are managed by Intel Authenticate.
Certification Authority URL	Only relevant when certificates are managed by Intel Authenticate. Valid values: • The HTTPS URL of the enrollment server • ComputerName\CAName - Where ComputerName is the network name of the server, and CAName is the common name of the Certification Authority • If left empty, Intel Authenticate will try all Certification Authorities in the Domain until the certificate is created
Certificates will be managed by Intel® Authenticate	When this check box is selected, Intel Authenticate will automatically manage certificates for this action. The certificate is automatically enrolled as soon as the user has enrolled enough factors to use the VPN Login action. In addition, 10 days before the enrolled certificate expires, Intel Authenticate will automatically start trying to renew the certificate. If you do not select this check box, you must manage the certificates using an alternative method (see Other Certificate Management Options on page 79).

*Other names and brands may be claimed as the property of others

Setting	Description
Certificate enrollment does not require user to authenticate	Only relevant when certificates are managed by Intel Authenticate. When this check box is selected, the certificate is enrolled silently without asking the user to do anything. When not selected, during enrollment the user must authenticate using the factors you defined for this action. (If the user does not authenticate successfully, then the certificate enrollment will fail.)
Time in minutes to cache authentication	The time (in minutes) during which a successful authentication remains valid (and therefore does not require the user to re-authenticate)

4 Setting Up Certificate-Based OS Login

Note:

- The instructions in this section are only necessary if you want to enable the certificate-based option of OS Login (see OS Login on page 8).
- If you want to implement certificate-based OS Login, Intel recommends that you implement on Windows 10 version 1709 or higher. From version 1709, Microsoft made several improvements to the infrastructure layers used by the certificate-based option.

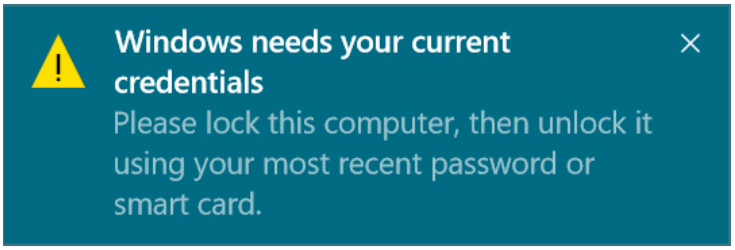
The certificate-based option of OS Login is implemented using the "Virtual Smartcard" infrastructure of Microsoft.

*Other names and brands may be claimed as the property of others

4.1 Considerations when Using Certificates

These are important points to understand before you implement certificate-based OS Login:

- Canceling the certificate-based option after it has been implemented on a platform requires you to:
  - Reset Intel Authenticate (will require the user to enroll their factors again)
  - Set a new policy without the **Use certificates for authentication** option selected
- When the certificate-based option is implemented, the login process can take slightly longer to complete (one or two seconds). This is because authentication using certificates involves more actions than simply checking that the correct password was supplied.
- The very first login using a certificate will take longer than all subsequent logins (approximately 10 seconds). This is because several actions are completed during the first login that are necessary to setup and confirm trust. This additional time only occurs during the very first login when the certificate is used for the first time.
- Sometimes, after changing between power states, login can take between 7 and 15 seconds to complete. (On Windows 10 version 1709 the response time in these cases has improved and only takes up to 6 seconds.)
- In some network environments, when using certificate based authentication, your users might occasionally see pop-up messages asking them to provide their credentials:

  In most cases, the user can simply ignore this message. But if access to the network really is blocked, all the user needs to do is to lock the PC and then login again using Intel Authenticate. This message is generated by Windows, and usually indicates that Windows considers that an authentication ticket has expired and therefore re-authentication is required. If these messages occur in your network environment, check your Active Directory configuration settings. Pay particular attention to the Kerberos configuration settings in your network. For more information, refer to the relevant Microsoft documentation.

*Other names and brands may be claimed as the property of others

4.2 Defining the CA Template for OS Login

The Certificate Template tool is a simple executable used to create certificate templates with settings that are ready to work with the Intel Authenticate certificate-based features. It is recommended to verify that the template works as expected before making any changes to the settings defined by the tool.

Note:

- The tool requires .NET Framework version 4.5.1 or higher. If not installed, the tool will throw an exception.
- You must run the tool with a user account that has the necessary permissions to create and publish certificate templates in your network environment. The user account used to run the tool will be made the owner of the certificate template that is created.

To create a certificate template for OS Login:

1. Copy the `Tools\CertificateTemplateTool` folder to the server where you want to create the OS Login certificate template.
2. Open a command prompt as an administrator (in the `CertificateTemplateTool` folder).
3. Type in this command:

   ```
   CertificateTemplateSetup.exe -c create -s yes -n <template_name> -d <display_name>
   ```

   Where `<template_name>` is the name of the certificate template and `<display_name>` is an optional display name.

   Note:

   Make sure that the certificate template name is identical to the name that you enter in the policy.

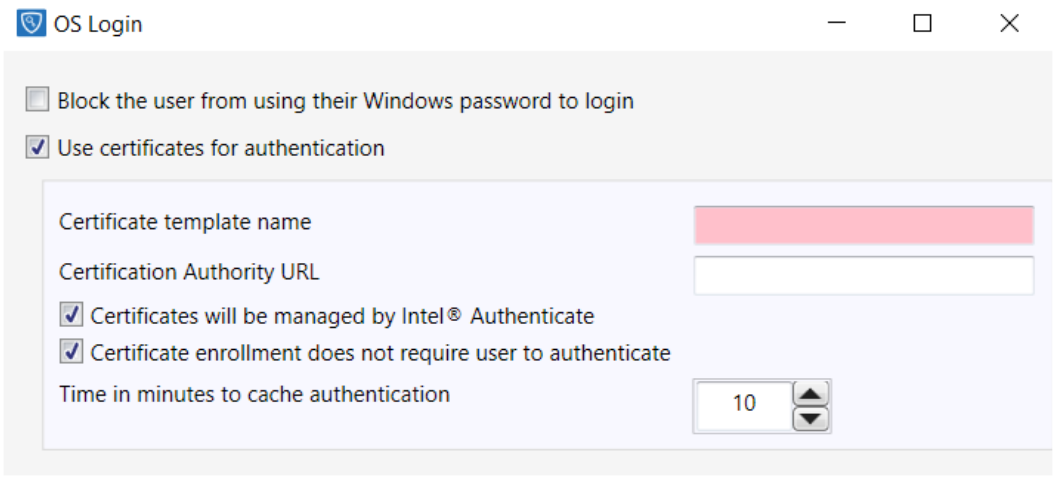
4. Press <Enter>. The Select Certification Authority window opens.
5. Select the CA on which you want to create the template and click **OK**. The template is installed and issued.

*Other names and brands may be claimed as the property of others

4.3 Defining Certificate-Based OS Login in the Policy

When the certificate-based option of OS Login is enabled, each user account requires a certificate to be installed in their certificate store on the client platform. This section describes important settings in the Intel Authenticate policy that define how these certificates are generated. Refer back to this section when you define the policy (see Creating a Policy on page 45).

The settings are located in the Advanced Settings section of the OS Login action:



Setting	Description
Use certificates for authentication	This check box enables the certificate-based option of OS Login. When selected, the login process is completed using a certificate and the Windows password is not used.
Certificate template name	The exact name of the certificate template to use for OS Login. This field is mandatory when certificates are managed by Intel Authenticate.
Certification Authority URL	Only relevant when certificates are managed by Intel Authenticate. Valid values: • The HTTPS URL of the enrollment server • ComputerName\CAName - Where ComputerName is the network name of the server, and CAName is the common name of the Certification Authority • If left empty, Intel Authenticate will try all Certification Authorities in the Domain until the certificate is created

*Other names and brands may be claimed as the property of others

Setting	Description
Certificates will be managed by Intel® Authenticate	When this check box is selected, Intel Authenticate will automatically manage certificates for this action. The certificate is automatically enrolled as soon as the user has enrolled enough factors to use the OS Login action. In addition, 10 days before the enrolled certificate expires, Intel Authenticate will automatically start trying to renew the certificate. If you do not select this check box, you must manage the certificates using an alternative method (see Other Certificate Management Options on page 79).
Certificate enrollment does not require user to authenticate	Only relevant when certificates are managed by Intel Authenticate. When this check box is selected, the certificate is enrolled silently without asking the user to do anything. When not selected, during enrollment the user must authenticate using the factors you defined for this action. (If the user does not authenticate successfully, then the certificate enrollment will fail.)
Time in minutes to cache authentication	The time (in minutes) during which a successful authentication remains valid (and therefore does not require the user to re-authenticate)

*Other names and brands may be claimed as the property of others

5 Setting Up Web Login

This section describes what you need to prepare before you can use a "Web Login" custom action.

Note:

- Web login is only supported on the Chrome* and Internet Explorer* browsers.
- Some of the instructions in this section are also relevant for "Application Login" custom actions (see Custom Actions on page 10). But each application vendor will need to supply specific instructions how to define the settings for their application.

5.1 Defining the CA Template for Web Login

The Certificate Template tool is a simple executable used to create certificate templates with settings that are ready to work with the Intel Authenticate certificate-based features. It is recommended to verify that the template works as expected before making any changes to the settings defined by the tool.

Note:

- The tool requires .NET Framework version 4.5.1 or higher. If not installed, the tool will throw an exception.
- You must run the tool with a user account that has the necessary permissions to create and publish certificate templates in your network environment. The user account used to run the tool will be made the owner of the certificate template that is created.

To create a web login certificate template:

1. Copy the `Tools\CertificateTemplateTool` folder to the server where you want to create the web login certificate template. (This tool requires .NET Framework version 4.5 or higher. If not installed, the tool will throw an exception.)
2. Open a command prompt as an administrator (in the `CertificateTemplateTool` folder).
3. Type in this command:

```
CertificateTemplateSetup.exe -c create -s no -n <template_name>
-d <display_name>
```

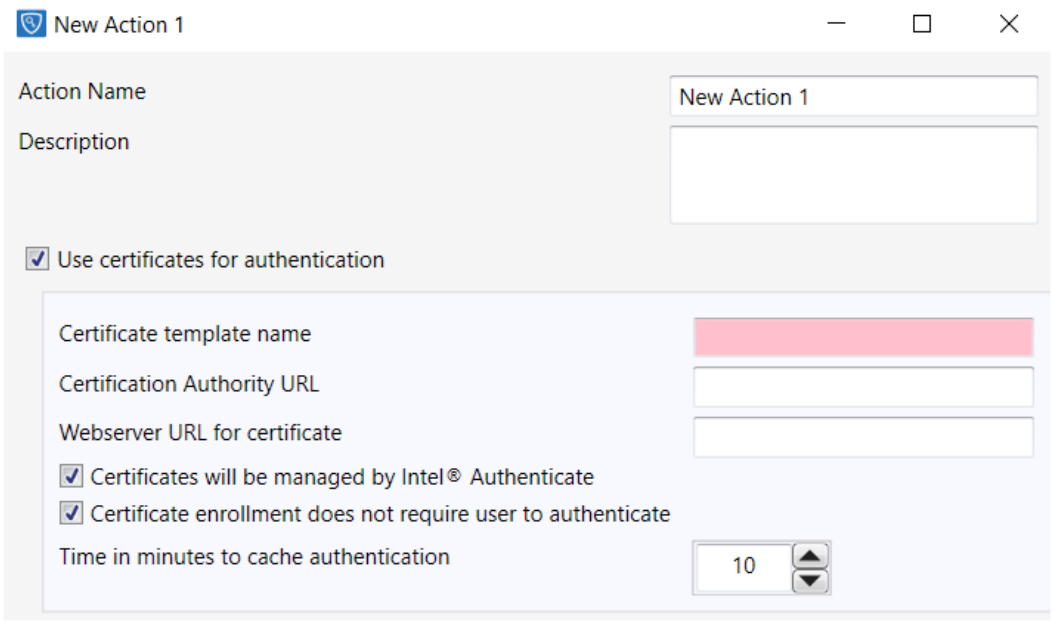
Parameter / Variable	Description
`-n <template_name>`	The name of the template (cannot contain spaces)
`-d <display_name>`	An optional display name

4. Press <Enter>. The Select Certification Authority window opens.
5. Select the CA on which you want to create the template and click **OK**. The template is installed and issued.

5.2 Defining a Web Login Action in the Policy

When a custom action is defined to use certificates for authentication, each user account requires a certificate to be installed in their certificate store on the client platform. This section describes important settings in the Intel Authenticate policy that define how these certificates are generated. Refer back to this section when you define the policy (see Creating a Policy on page 45).

The settings are shown when you click **Add Action** in the Policy Editor:



Setting	Description
Acton Name	The name of the action. This name is displayed in the Factor Management application when the user enrolls their factors.
Description	An optional description (not displayed to the user)
Use certificates for authentication	For a web login action, you must select this check box
Certificate template name	The exact name of the certificate template to use for this custom action. This field is mandatory when certificates are managed by Intel Authenticate.

*Other names and brands may be claimed as the property of others

Setting	Description
Certification Authority URL	Only relevant when certificates are managed by Intel Authenticate. Valid values: • The HTTPS URL of the enrollment server • ComputerName\CAName - Where ComputerName is the network name of the server, and CAName is the common name of the Certification Authority • If left empty, Intel Authenticate will try all Certification Authorities in the Domain until the certificate is created
Webserver URL for certificate	The URL of the webserver site that is responsible for authenticating the certificate for this action. (This is not always the same as the actual webserver site of the action.) If you do not supply this URL, when multiple certificates exist on a platform, the user will need to select the certificate from a list when trying to log in. **Note:** For this option to work with the Internet Explorer* browser, make sure that the **Enable Protected Mode** check box in the Security tab is NOT selected.
Certificates will be managed by Intel® Authenticate	When this check box is selected, Intel Authenticate will automatically manage certificates for this custom action. The certificate is automatically enrolled as soon as the user has enrolled enough factors to use the custom action. In addition, 10 days before the enrolled certificate expires, Intel Authenticate will automatically start trying to renew the certificate. If you do not select this check box, you must manage the certificates using an alternative method (see Other Certificate Management Options on page 79).
Certificate enrollment does not require user to authenticate	Only relevant when certificates are managed by Intel Authenticate. When this check box is selected, the certificate is enrolled silently without asking the user to do anything. When not selected, during enrollment the user must authenticate using the factors you defined for this action. (If the user does not authenticate successfully, then the certificate enrollment will fail.)
Time in minutes to cache authentication	The time (in minutes) during which a successful authentication remains valid (and therefore does not require the user to re-authenticate)

*Other names and brands may be claimed as the property of others

6 Integrating with GPO

This section describes how to use the contents of the GPO integration package to integrate Intel Authenticate with GPO. After integration you can use GPO to configure and manage Intel Authenticate.

Note:

- The procedures in this section show how to create GPOs using Windows Server 2008 R2. Other versions might have differences in the required steps or the GUI. Refer to the Microsoft documentation for information about differences between versions.
- The procedures in this section use the default location (on the C drive) for the operating system. If the Windows installation on your client platforms is in a different location, make sure that you make the necessary adjustments when following the procedures.

6.1 Deployment Flow Using GPO

These are the main steps required to deploy and configure Intel Authenticate using GPO:

1. Make sure that your server is supported (see Server Requirements below).
2. Create a policy for Intel Authenticate (see Creating a Policy on page 45).
3. Create a shared folder on the server for the files that will be downloaded to the client platforms (see Creating a Shared Folder on page 46).
4. Create two WMI filters that will be used by the GPOs (see Creating WMI Filters for the GPOs on page 47).
5. Create a GPO to discover which of the platforms in your organization support Intel Authenticate (see Creating a GPO to Discover Intel Authenticate on page 49).
6. Create a GPO to install Intel Authenticate on the platforms (see Creating a GPO to Install Intel Authenticate on page 53).
7. Create a GPO to enforce the Intel Authenticate policy on the platforms (see Creating a GPO to Enforce the Policy on page 56).
8. After the policy is enforced on a client platform, the user can enroll the factors that you defined in the policy and start to use Intel Authenticate. For more information about the enrollment process, refer to the enrollment guide included in the integration package.

6.2 Server Requirements

The server that you use to integrate Intel Authenticate with GPO must be a domain controller with one of these operating systems:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

*Other names and brands may be claimed as the property of others

6.3 Preparing a Digital Signing Certificate

All Intel Authenticate policies must be signed by a "Digital Signing" certificate. Signing the policy is a mandatory step in the Policy Editor before you are allowed to save the policy. If you do not have a valid certificate you will not be allowed to save the policy. It is recommended to prepare a certificate that will be used only by Intel Authenticate. After acquiring a certificate for use with Intel Authenticate, you need to install it on the computer where you intend to run the Policy Editor.

Certificate Requirements

- The certificate must be issued by a trusted Certification Authority (CA) and contain a valid private key.
- The certificate does NOT need to be a Code Signing certificate.
- The key size must be either 2048 bits or 4096 bits (all other key sizes are not supported).
- Make sure that you install the certificate in the machine store or the user certificate store of the user running the Policy Editor. Only certificates installed in these certificate stores will be shown as available in the Policy Editor. If you install the certificate in the machine store you must run the Policy Editor with administrator privileges. In addition, the root certificate must be installed in the Trusted Root Certificate store.

Obtaining a Certificate

You can use digital signing certificates generated by an external CA, or an internal CA located in your network. To get a certificate, you must apply to the CA by sending a Certificate Signing Request (CSR). The process for acquiring a certificate varies according to the vendor and is beyond the scope of this guide.

Note:

The Select Signing Certificate button in the Policy Editor displays a list of signing certificates that are already installed on the computer where you run the Policy Editor. For testing purposes, you can use any of the certificates that are marked as valid (in the Valid column). If no certificates are valid, you can create a test certificate, as described in the procedure below.

Creating a Test Certificate

From PowerShell version 5, you can use the `New-SelfSignedCertificate` command to create a certificate. (PowerShell 5 is included by default in Windows 10). This procedure creates a test certificate and installs it in the Personal certificate store of the current user.

To create and install a test certificate:

1. Select the computer on which you intend to run the Policy Editor and create the Intel Authenticate policy.
2. Login to the computer with an Administrator user.

*Other names and brands may be claimed as the property of others

3. Open a command prompt and run this command:

```
New-SelfSignedCertificate –Subject "CN=TestCert" –KeyUsageProperty All
–KeyAlgorithm RSA –KeyLength 2048 –KeyUsage DigitalSignature
–CertStoreLocation "Cert:\CurrentUser\My"
```

   In this example, a certificate named "TestCert" is installed in the Personal certificates store. You can use any name for your own test certificate. After the command completes, you must manually copy the certificate to the Trusted Root Certificate store of the current user. The remaining steps describe how to do that using Microsoft Management Console.

4. Click **Start**, type mmc.exe, and then press <Enter>. The Microsoft Management Console window opens.
5. Select **File** > **Add/Remove Snap-in**. The Add or Remove Snap-ins window opens.
6. From the list of available snap-ins (in the left pane of the window), select **Certificates** and click **Add**. The Certificates snap-in window opens.
7. Select **My user account** and click **Finish**. The Certificates snap-in window closes and the "Certificates – Current User" snap-in is added to the list of selected snap-ins.
8. Click **OK**. The Add or Remove Snap-ins window closes and the snap-ins are added to the Console Root tree (in the left pane of the window).
9. In the left pane, select **Certificates** - **Current User** > **Personal** > **Certificates**.
10. In the right pane, right-click **TestCert** and select **Copy**.
11. In the left pane, right-click **Certificates** - **Current User** > **Trusted Root Certification Authorities** > **Certificates**and select **Paste**.
12. A security warning message appears. Click **Yes**. The TestCert certificate is copied to the Trusted Root Certification Authorities store.
13. Close the Microsoft Management Console window. The test certificate is now ready to be used. When you run the Policy Editor on this computer, the test certificate will appear in the list of valid certificates.

*Other names and brands may be claimed as the property of others

6.4 Creating a Policy

Policies for Intel Authenticate are created using the Policy Editor. (Microsoft .NET Framework version 3.5 or higher must be installed on the computer where you want to run the Policy Editor.)

To create a policy:

1. Copy the `PolicyEditor` folder to the platform that you will use to create and manage policies for Intel Authenticate (the platform on which you installed the digital signing certificate).
2. Right-click **PolicyEditor.exe** and select **Run as administrator**.
3. Click **New**. A new empty policy opens.
4. In the Signing Certificate section, click **Select Signing Certificate** and select a certificate that will be used to sign the policy (see Preparing a Digital Signing Certificate on page 43).

   Note:

   The list contains all certificates found in the relevant certificate stores. But you can only select a certificate if it is marked as valid (in the Valid column). If the certificate is shown as invalid because the chain cannot be validated, try connecting the platform to the Internet or manually install the missing certificate(s) in the chain.

5. Define the settings that you want to include in this policy. Most of the settings include tool-tips to explain the setting. For detailed information about the settings, click the help icon.

   Note:

   On non Intel vPro systems, the number of mandatory factors that you can define for each action is limited to two factors. Enforcing a policy that contains an action with more than two mandatory factors will fail on non Intel vPro systems. This restriction does not apply to Intel vPro systems. On Intel vPro systems, you can define as many mandatory factors per action as you want.

6. Click **Save** or **Save As**. The Save As window opens.
7. Specify the name and the location where you want to save the policy and click **Save**. The Save As window closes and the policy is saved. The policy remains open in the Policy Editor and the name of the policy is shown.
8. Close the Policy Editor

Note:

The XML file of the policy is now ready to be used. Later on, you will need to place this XML file in the shared folder that you created (see Creating a Shared Folder on the next page).

*Other names and brands may be claimed as the property of others

6.5 Creating a Shared Folder

The `HostFiles` folder located in the root of this package contains the installers, scripts, and batch files that will be used to configure and manage Intel Authenticate. These files need to be placed in a shared folder on the server that you want to use to manage GPO for Intel Authenticate. The client platforms must be able to access the shared folder on the server. Give read permissions on the shared folder to domain computers.

This table describes the main contents of the `HostFiles` folder.

Item	Description
`Authenticate_Check.exe`	This executable checks if the platform has all the prerequisites for installing Intel Authenticate (see Prerequisites for Installation on page 15).
`Setup_x64.exe`	The installer for 64-bit systems
`Setup_x86.exe`	The installer for 32-bit systems
`CopyFilesLocally.bat`	This batch file copies the contents of the shared folder on the server to a temporary folder on the client platform. The remaining batch files and scripts are then run locally on the client platform. The default setting is to copy the files to `C:\Windows\Temp`. Please edit this default location according to your corporate policies.
`DetectIntelAuthenticate.bat`	This batch file is used to make sure that the VBSript `DetectIntelAuthenticate.vbs` is run from the cscript engine.
`DetectIntelAuthenticate.vbs`	This VBScript runs the `Authenticate_Check.exe` tool and saves the output in the CIMv2 namespace on the client platform. Other tools and scripts can then query this data using WQL queries. It is recommended to run this script periodically to update the status of the Intel Authenticate entries in the CIMv2 namespace.
`RunInstaller.ps1`	This PowerShell script checks if the system is a 32-bit or 64-bit system and then runs the relevant version of the installer.
`EnforcePolicy.ps1`	This PowerShell script enforces the policy of Intel Authenticate on the client platform. A few minutes after the policy is enforced, the Factor Management application will open to enable the user to enroll the factors that you defined in the policy.
`ResetIA.ps1`	This PowerShell script removes all the Intel Authenticate policy settings and enrollment data from the client platform.

Note:

Make sure that you also place the policy XML file that you created in the shared folder.

*Other names and brands may be claimed as the property of others

6.6 Creating WMI Filters for the GPOs

Some of the GPOs for Intel Authenticate use WMI filters.

- This filter checks if the platform supports Intel Authenticate:
  SELECT * FROM Intel_Authenticate WHERE Supported = "true"
- This filter checks if Intel Authenticate is installed on the platform:
  SELECT * FROM Intel_Authenticate WHERE isClientInstalled ="true" AND isEngineInstalled = "true"

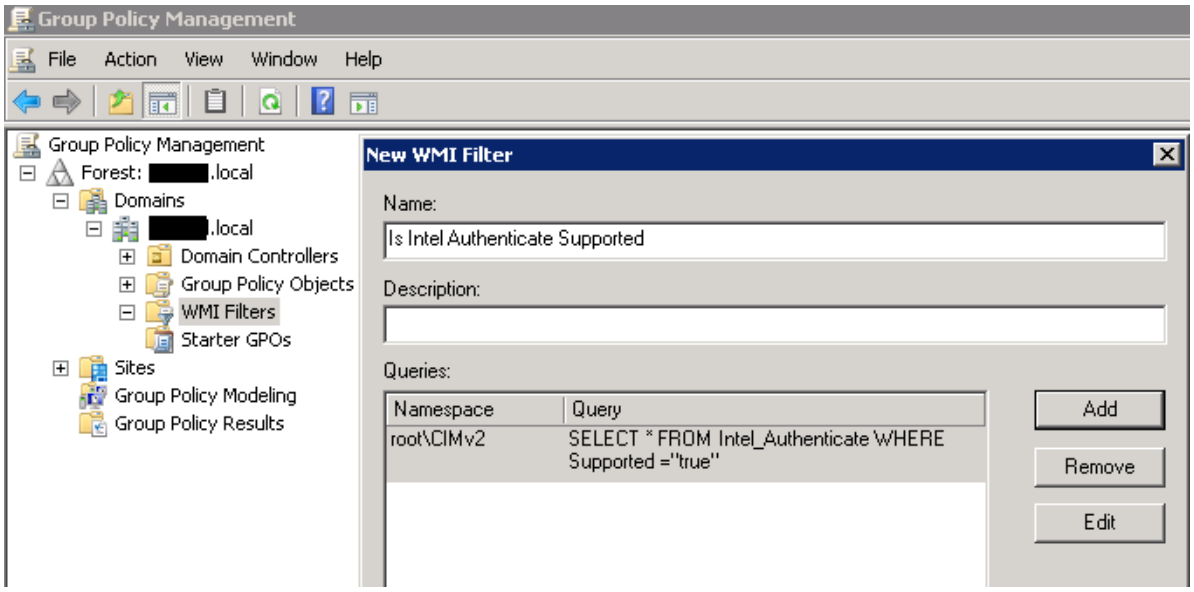
To create the WMI filters:

1. Open the Group Policy Management window. (Press the Windows key + R, in the Run dialog type **gpmc.msc** and press enter.)
2. Do these steps to create the WMI filter to detect if Intel Authenticate is supported on the client platform:

   a. In the Group Policy Management tree, select the relevant domain or OU, right click **WMI Filters** and select **New**. The New WMI filter window opens.

   b. Enter a descriptive name for this WMI Filter (for example: Is Intel Authenticate Supported), and click **Add**. The WMI Query window opens.

   c. In the Query field, define this query:
   SELECT * FROM Intel_Authenticate WHERE Supported ="true"



   d. Click **OK** and **Save**.

*Other names and brands may be claimed as the property of others

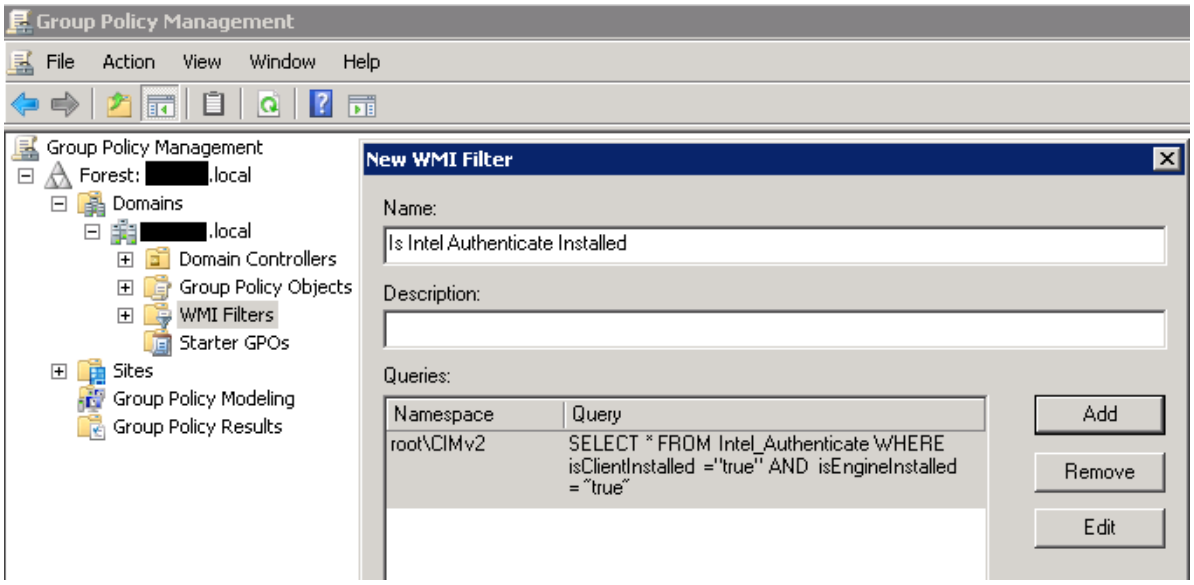
3. Do these steps to create a WMI filter to detect if Intel Authenticate is installed on the client platform:

   a. On the same domain/OU where you created the first filter, right click **WMI Filters** and select **New**. The New WMI filter window opens.

   b. Enter a descriptive name for this WMI Filter (for example: Is Intel Authenticate Installed), and click **Add**. The WMI Query window opens.

   c. In the Query field, define this query:

   ```
   SELECT * FROM Intel_Authenticate WHERE isClientInstalled ="true" AND isEngineInstalled ="true"
   ```



   d. Click **OK** and **Save**.

*Other names and brands may be claimed as the property of others

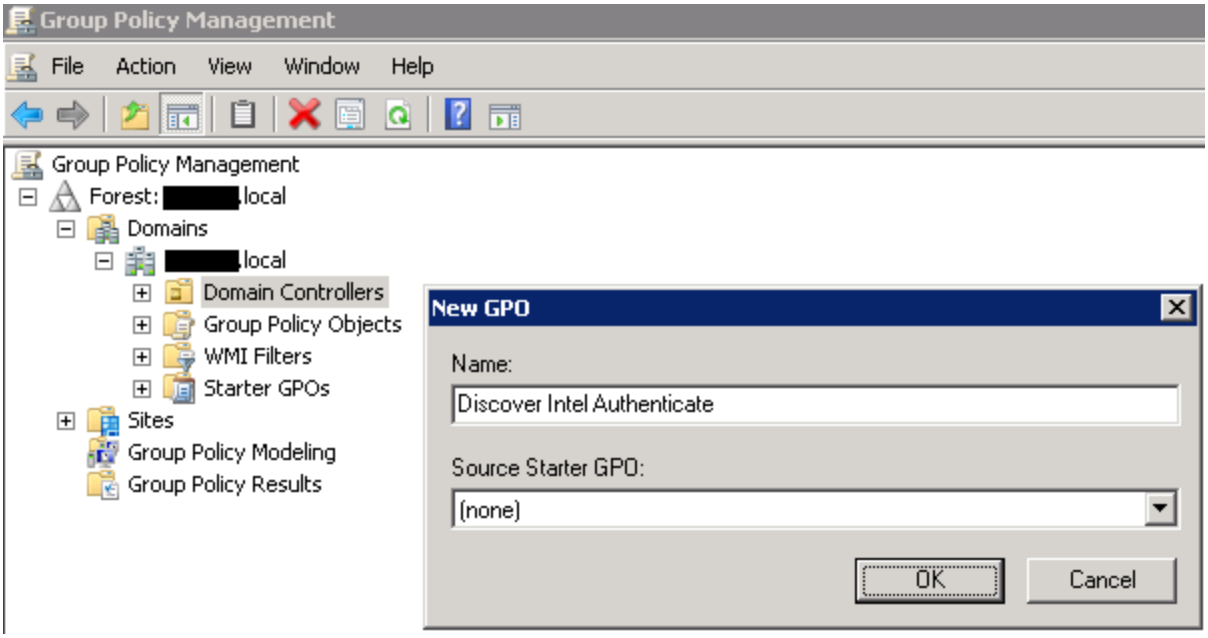
6.7 Creating a GPO to Discover Intel Authenticate

The first GPO that you need to create is used to "discover" if the platform includes all the prerequisites for Intel Authenticate. This table describes the items that need to be defined in this GPO.

Item	Details
Task #1	Run the `CopyFilesLocally.bat` batch file
Task #2	Run the `DetectIntelAuthenticate.bat` batch file

To create the "discovery" GPO:

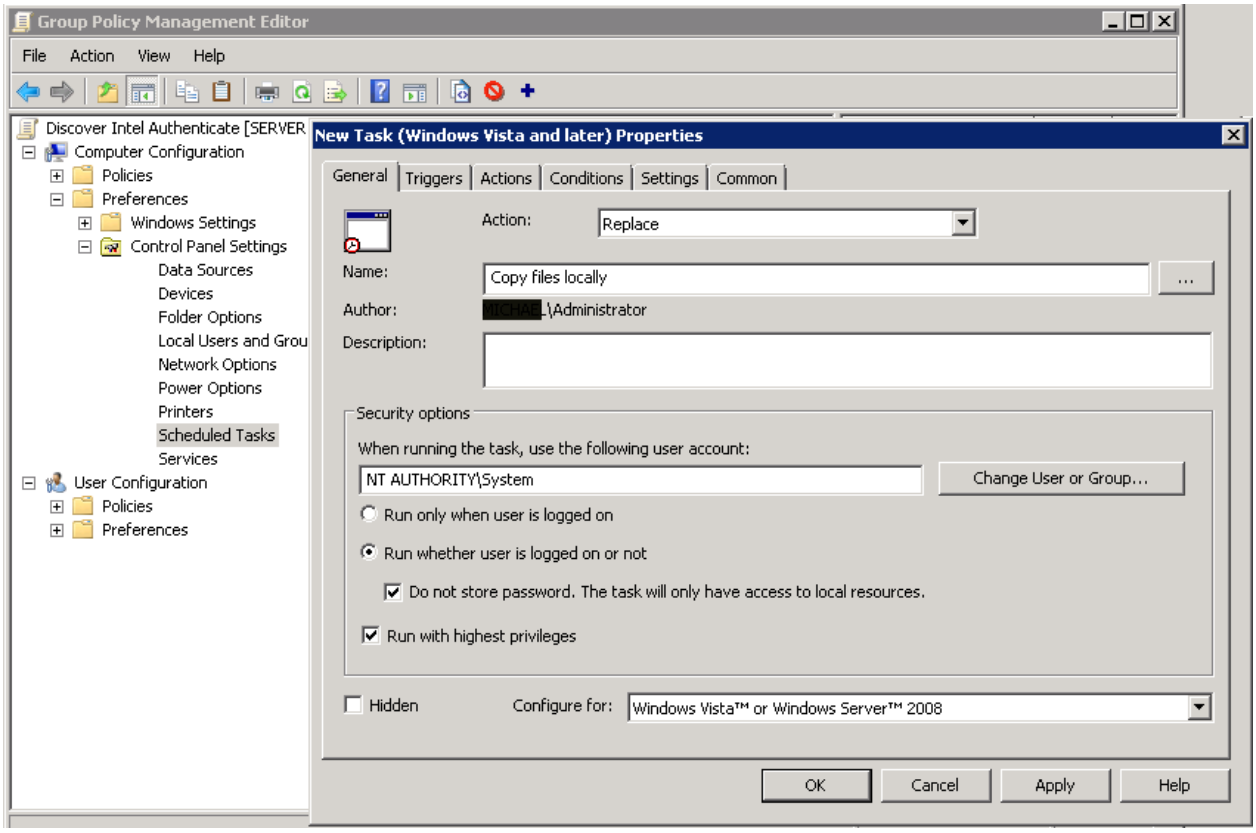
1. Open the Group Policy Management window.
2. In the Group Policy Management tree, right-click the relevant domain or OU, and **select Create a GPO in this domain and Link it here**. The New GPO window opens.



3. Enter a descriptive name for this GPO (for example: Discover Intel Authenticate) and click **OK**.
4. Right-click the GPO that you just created and select **Edit**. The Group Policy Management Editor window opens.

*Other names and brands may be claimed as the property of others

5. In the tree, select **Computer Configuration** > **Preferences** > **Control Panel Settings**, right-click **Scheduled Tasks** and select **New** > **Scheduled Task (At least Windows 7)**. (In Windows Server 2008 R2, select **Scheduled Task (Windows Vista and later)**). The New Task Properties window opens.



6. Select the **General** tab and do these steps:

   a. From the Action drop-down list, select **Replace**.

   b. In the Name field, enter a descriptive name for this task (for example: Copy files locally).

   c. Click **Change User or Group**, in the object name field type "SYSTEM", and click **OK**. The value of the user account field will now show "NT Authority\System".

   d. Select **Run whether user is logged on or not**.

   (A window will open asking for the password of the system account. Click **Cancel** to close this window.)

   e. Select both of these check boxes:

   - **Do not store password. The task will only have access to local resources.**
   - **Run with highest privileges**

7. Select the **Triggers** tab and do these steps:

   a. Click **New**. The New Trigger window opens.

   b. From the Begin the task drop-down list, select **At task creation/modification** and click **OK**.

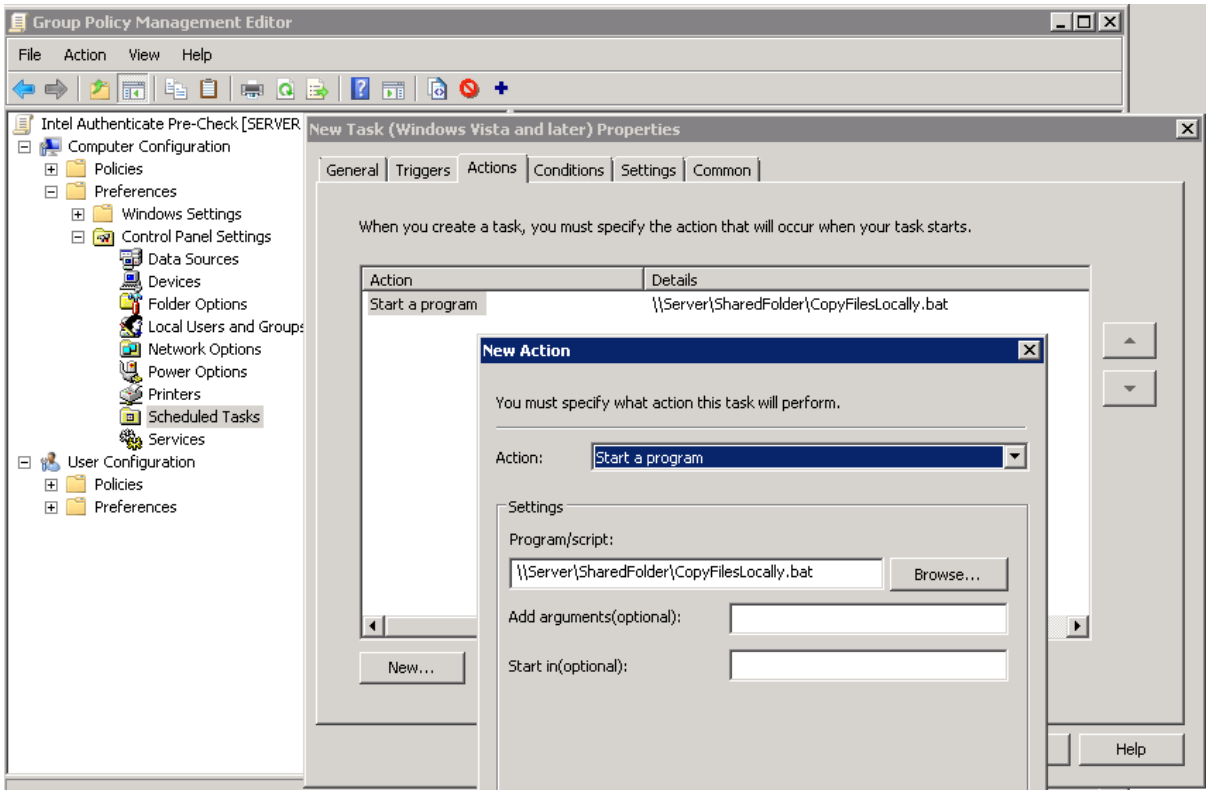
8. Select the **Actions** tab and do these steps:

   a. Click **New**. The New Action window opens.

   b. From the Action drop-down list, select **Start a program**.

   c. In the Program/script field, enter the Universal Naming Convention (UNC) path to the `CopyFilesLocally.bat` file located in the shared folder that you prepared.

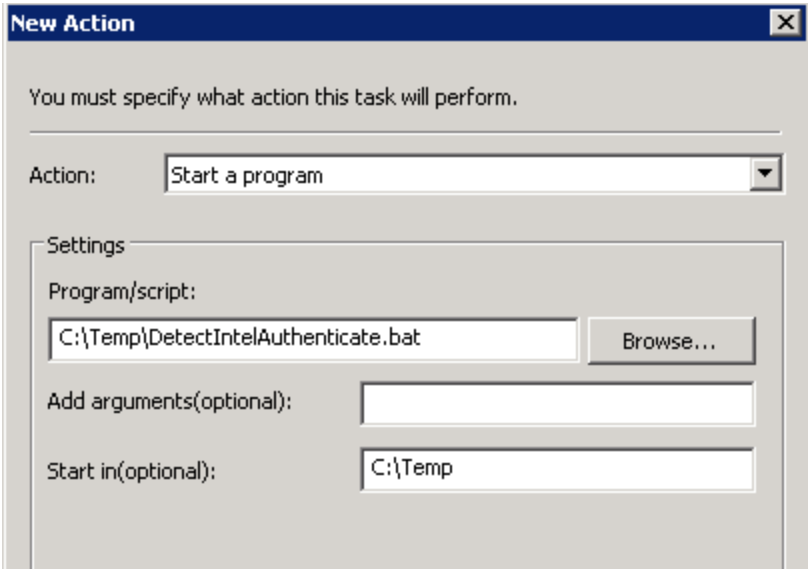
   d. Click **OK** twice to close the New Action and New Task windows.



*Other names and brands may be claimed as the property of others

9. Repeat steps 5-8 to create a task to run the Check tool to discover if the platform supports Intel Authenticate. When creating this task, use these specific settings:
   - Use a descriptive name for this task (for example: Detect Intel Authenticate).
   - In the Triggers tab, select the **Delay task for** check box, and from the drop-down list select **30 minutes**.
   - In the Program/script field of the New Action window, enter:
     C:\Temp\DetectIntelAuthenticate.bat
   - In the Start in field of the New Action window, enter:
     C:\Temp

     (Make the necessary adjustments to the paths if you edited the folder location in the `CopyFilesLocally.bat` file.)



10. When complete, you will have two tasks defined for the discovery GPO. Close the Group Policy Management Editor window.

*Other names and brands may be claimed as the property of others

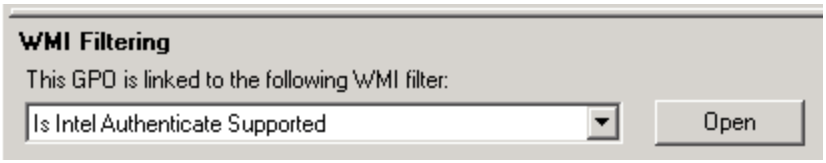
6.8 Creating a GPO to Install Intel Authenticate

The second GPO that you need to create is used to install Intel Authenticate if the platform meets the prerequisites check run by the "discovery" GPO. This GPO will only be deployed on client platforms where Intel Authenticate is supported. This table describes the items that need to be defined in this GPO.

Item	Details
WMI Filter	SELECT * FROM Intel_Authenticate WHERE Supported ="true"
Task #1	Run the `RunInstaller.ps1` PowerShell script
Task #2	Run the `DetectIntelAuthenticate.bat` batch file

To create the "installation" GPO:

1. Open the Group Policy Management window.
2. In the Group Policy Management tree, right-click the relevant domain or OU, and **select Create a GPO in this domain and Link it here**. The New GPO window opens.
3. Enter a descriptive name for this GPO (for example: Install Intel Authenticate) and click **OK**.
4. In the tree, select the GPO that you just created, and from the drop-down list in the WMI Filtering section select the "Is Intel Authenticate Supported" WMI filter (see Creating WMI Filters for the GPOs on page 47). Click **Yes** in the dialog box that opens.



5. Right-click the GPO and select **Edit**. The Group Policy Management Editor window opens.
6. In the tree, select **Computer Configuration** > **Preferences** > **Control Panel Settings**, right-click **Scheduled Tasks** and select **New** > **Scheduled Task (At least Windows 7)**. (In Windows Server 2008 R2, select **Scheduled Task (Windows Vista and later)**). The New Task Properties window opens.

*Other names and brands may be claimed as the property of others

7. Select the **General** tab and do these steps:
    a. From the Action drop-down list, select **Replace**.
    b. In the Name field, enter a descriptive name for this task (for example: Install Intel Authenticate).
    c. Click **Change User or Group**, in the object name field type "SYSTEM", and click **OK**. (The value of the user account field will now show "NT Authority\System")
    d. Select **Run whether user is logged on or not**.
    (A window will open asking for the password of the system account. Click **Cancel** to close this window.)
    e. Select both of these check boxes:
        - **Do not store password. The task will only have access to local resources.**
        - **Run with highest privileges**
8. Select the **Triggers** tab and do these steps:
    a. Click **New**. The New Trigger window opens.
    b. From the Begin the task drop-down list, select **At task creation/modification**.
    c. Select the **Delay task for** check box, and from the drop-down list select **30 minutes**.
    d. Click **OK**.

*Other names and brands may be claimed as the property of others

9. Select the **Actions** tab and do these steps:

   a. Click **New**. The New Action window opens.

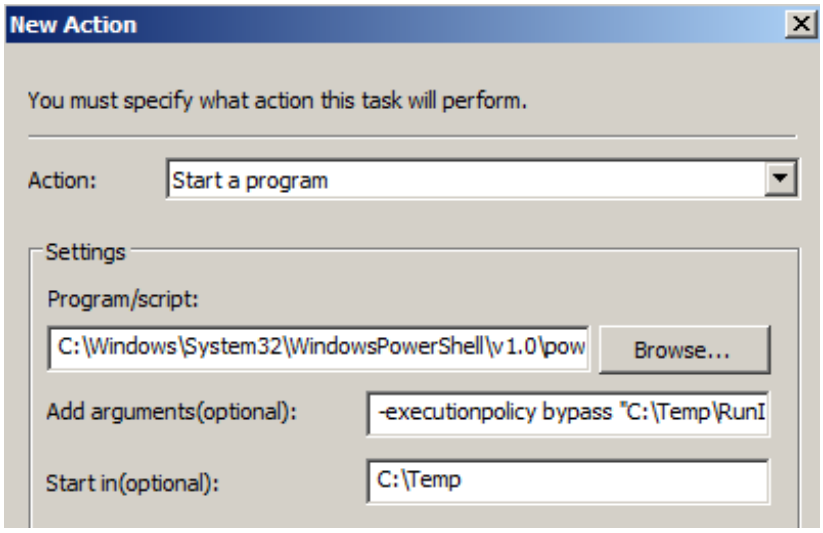
   b. From the Action drop-down list, select **Start a program**.

   c. In the Program/script field, enter:
   ```
   C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
   ```

   d. In the Add argument field, enter:
   ```
   -executionpolicy Bypass C:\Temp\RunInstaller.ps1
   ```

   e. In the Start in field, enter:
   ```
   C:\Temp
   ```

   f. Click **OK** twice to close the New Action and New Task windows.



10. Repeat steps 6-9 to create a task to run the Check tool again after installation has completed. This task is necessary to update the entries in the CIMv2 namespace on the client platform with the fact that Intel Authenticate is now installed. When creating this task, use these specific settings:
    - Use a descriptive name for this task (for example: Update data for WMI filter).
    - In the Advanced Settings section of the Triggers tab, select the **Delay task for** check box and select **30 minutes**.
    - In the Program/script field of the New Action window, enter:
      ```
      C:\Temp\DetectIntelAuthenticate.bat
      ```
    - In the Start in field of the New Action window, enter:
      ```
      C:\Temp
      ```
      (Make the necessary adjustments to the paths if you edited the folder location in the `CopyFilesLocally.bat` file.)
11. When complete, you will have two tasks defined for the installation GPO. Close the Group Policy Management Editor window.

6.9 Creating a GPO to Enforce the Policy

The third GPO that you need to create is used to enforce the Intel Authenticate policy. This GPO will only be deployed on client platforms where Intel Authenticate is already installed. This table describes the items that need to be defined in this GPO.

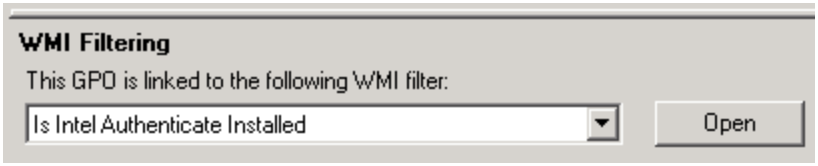
Item	Details
WMI Filter	SELECT * FROM Intel_Authenticate WHERE isClientInstalled ="true" AND isEngineInstalled = "true"
Task	Run the `EnforcePolicy.ps1` PowerShell script

Note:

It is recommended to schedule recurring policy enforcements to make sure that your company policy has not been replaced with a policy signed by a different certificate. (Replacing a policy is only possible if the user has administrator permissions on the platform and can reset the policy.) The `EnforcePolicy.ps1` script includes a mechanism to detect if the policy was replaced by a policy signed with a different certificate than the current policy. If a different signing certificate is detected, the script automatically resets the policy. The user will then need to re-enroll their factors.

To create the enforce policy GPO:

1. Open the Group Policy Management window.
2. In the Group Policy Management tree, right-click the relevant domain or OU, and **select Create a GPO in this domain and Link it here**. The New GPO window opens.
3. Enter a descriptive name for this GPO (for example: Enforce Intel Authenticate Policy) and click **OK**.
4. In the tree, select the GPO that you just created, and from the drop-down list in the WMI Filtering section select the "Is Intel Authenticate Installed" WMI filter (see Creating WMI Filters for the GPOs on page 47). Click **Yes** in the dialog box that opens.



5. Right-click the GPO and select **Edit**. The Group Policy Management Editor window opens.
6. In the tree, select **Computer Configuration** > **Preferences** > **Control Panel Settings**, right-click **Scheduled Tasks** and select **New** > **Scheduled Task (At least Windows 7)**. (In Windows Server 2008 R2, select **Scheduled Task (Windows Vista and later)**). The New Task Properties window opens.

*Other names and brands may be claimed as the property of others

7. Select the **General** tab and do these steps:
   a. From the Action drop-down list, select **Replace**.
   b. In the Name field, enter a descriptive name for this task (for example: Deploy Policy).
   c. Click **Change User or Group**, in the object name field type `SYSTEM`, and click **OK**. (The value of the user account field will now show "NT Authority\System")
   d. Select **Run whether user is logged on or not**.
      (A window will open asking for the password of the system account. Click **Cancel** to close this window.)
   e. Select both of these check boxes:
      - **Do not store password. The task will only have access to local resources.**
      - **Run with highest privileges**
8. Select the **Triggers** tab and do these steps:
   a. Click **New**. The New Trigger window opens.
   b. From the Begin the task drop-down list, select **On a schedule**.
   c. Select **Daily**.
   d. Select the **Delay task for** check box, and from the drop-down list select **30 minutes**.
   e. Click **OK**.

   Note:

   These schedule settings are a recommendation. You can set a different schedule if you prefer. But always set a delay of 30 minutes to make sure that installation has completed before the policy is enforced.
9. Select the **Actions** tab and do these steps:
   a. Click **New**. The New Action window opens.
   b. From the Action drop-down list, select **Start a program**.
   c. In the Program/script field, enter:
      `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`
   d. In the Add argument field, enter:
      `-executionpolicy Bypass C:\Temp\EnforcePolicy.ps1 C:\Temp\MyPolicy.xml`
      (Substitute the name of the policy file that you created. And make the necessary adjustments to the paths if you edited the folder location in the `CopyFilesLocally.bat` file.)
   e. In the Start in field, enter:
      `C:\Temp`
   f. Click **OK** twice to close the New Action and New Task windows.

*Other names and brands may be claimed as the property of others

10. Close the Group Policy Management Editor window.

6.10 Creating a GPO to Reset the Policy

The fourth GPO is optional and is used to remove the Intel Authenticate policy settings and enrollment data.

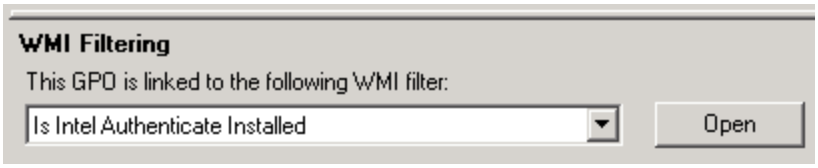
> **Note:**
>
> Do NOT enable this GPO by default. If you only want to reset the settings on some individual client platforms, use the `ResetIA.ps1` script directly on those platforms. If you deploy this GPO on a domain or OU you will remove Intel Authenticate policy settings and enrollment data from all client platforms in the domain/OU.

This table describes the items that need to be defined in this GPO.

Item	Details
WMI Filter	SELECT * FROM Intel_Authenticate WHERE isClientInstalled ="true" AND isEngineInstalled = "true"
Task	Run the `ResetIA.ps1` PowerShell script

To create the reset policy GPO:

1. In the Group Policy Management tree, right-click the relevant domain or OU, and **select Create a GPO in this domain and Link it here**. The New GPO window opens.
2. Enter a descriptive name for this GPO (for example: Reset Intel Authenticate Policy) and click **OK**.
3. In the tree, select the GPO that you just created, and from the drop-down list in the WMI Filtering section select the "Is Intel Authenticate Installed" WMI filter (see Creating WMI Filters for the GPOs on page 47). Click **Yes** in the dialog box that opens.



4. Right-click the GPO and select **Edit**. The Group Policy Management Editor window opens.
5. In the tree, select **Computer Configuration** > **Preferences** > **Control Panel Settings**, right-click **Scheduled Tasks** and select **New** > **Scheduled Task (At least Windows 7)**. (In Windows Server 2008 R2, select **Scheduled Task (Windows Vista and later)**). The New Task Properties window opens.

*Other names and brands may be claimed as the property of others

6. Select the **General** tab and do these steps:
   a. From the Action drop-down list, select **Replace**.
   b. In the Name field, enter a descriptive name for this task (for example: Reset Policy).
   c. Click **Change User or Group**, in the object name field type "SYSTEM", and click **OK**. (The value of the user account field will now show "NT Authority\System")
   d. Select **Run whether user is logged on or not**.
      (A window will open asking for the password of the system account. Click **Cancel** to close this window.)
   e. Select both of these check boxes:
      - **Do not store password. The task will only have access to local resources.**
      - **Run with highest privileges**
7. Select the **Triggers** tab and do these steps:
   a. Click **New**. The New Trigger window opens.
   b. From the Begin the task drop-down list, select **At task creation/modification** and click **OK**.
8. Select the **Actions** tab and do these steps:
   a. Click **New**. The New Action window opens.
   b. From the Action drop-down list, select **Start a program**.
   c. In the Program/script field, enter `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`.
   d. In the Add argument field, enter a command line argument to open PowerShell and run the `ResetIA.ps1` script:
      ```
      -executionpolicy Bypass C:\Temp\ResetIA.ps1
      ```
      (Make the necessary adjustments to the path if you edited the folder location in the `CopyFilesLocally.bat` file.)
   e. In the Start in field, enter `C:\Temp`.
   f. Click **OK** twice to close the New Action and New Task windows
9. Close the Group Policy Management Editor window.

*Other names and brands may be claimed as the property of others

6.11 Upgrade Flow Using GPO

If you have already deployed an earlier version of Intel Authenticate in your network, you can upgrade the existing installations.

> **Note:**
>
> Upgrade is only supported from Intel Authenticate version 3.0 or higher.

To upgrade existing installations:

1. If you are using Bluetooth Proximity, it is recommend to ask your existing users to upgrade the Intel Authenticate app on their phones to the latest version. (Except for "Soft" iPhone users that did not install the Intel Authenticate app.)
2. On the server, replace all the files in the shared folder with the new versions of the files located in the `Hostfiles` folder of the new integration package.

   > **Note:**
   >
   > You do not need to make any changes to the existing GPOs or the WMI filters that you created for deployment of Intel Authenticate. The `RunInstaller.ps1` script automatically detects if an existing installation exists and then performs the upgrade if necessary.

3. It is recommended to update the existing policy XML file by opening it with the new version of the Policy Editor in the new integration package. If any fields or settings have been changed or added between versions, they will be updated when you save the policy.
4. If you are upgrading from version 3.0 or 3.1, and you implemented either of these options, then you must set a new policy created using the new Policy Editor:
   - The certificate-based option of OS Login - By default, the certificate is now only generated if you define that certificates will be managed by Intel Authenticate (see Defining Certificate-Based OS Login in the Policy on page 37).
   - Attended VPN certificate enrollment - By default the user is no longer required to authenticate when the VPN certificate is generated (see Defining VPN Login in the Policy on page 33).
5. After the upgrade has finished, the user will be asked to reboot their computer. This is important to make sure that all files and services were successfully upgraded.

*Other names and brands may be claimed as the property of others

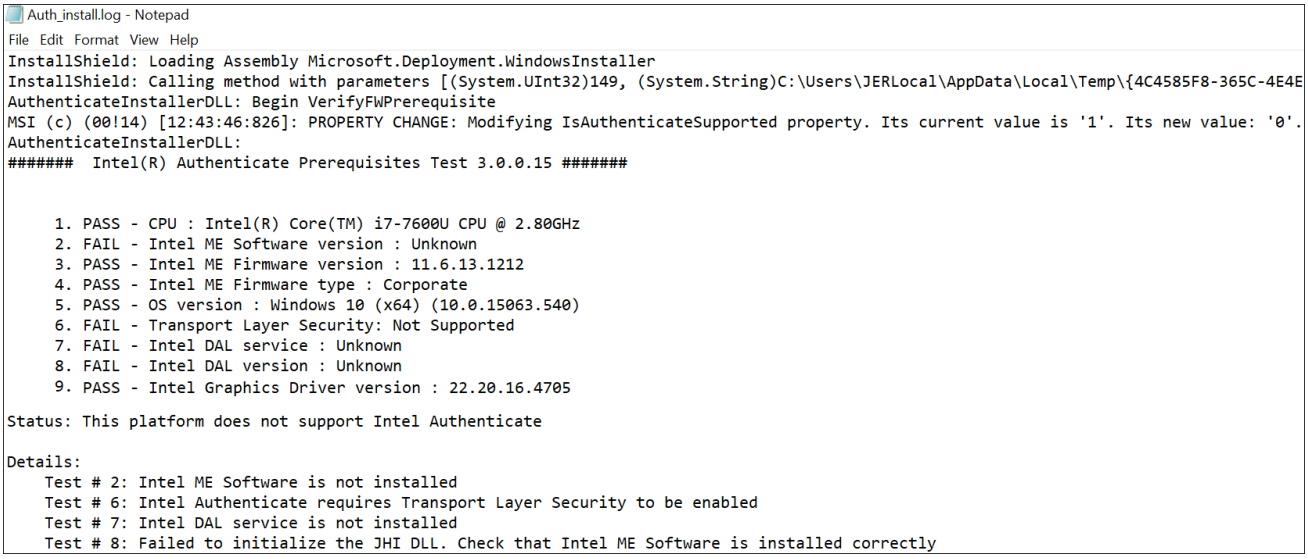
7 Troubleshooting

This section describes problems you might find when using Intel Authenticate, and provides their solutions.

> **Note:**
>
> For information about support options for Intel Authenticate, go to Intel Customer Support.

7.1 Troubleshooting Installation

Before installation, the installer runs the Check tool /P prerequisites test. If the test fails, then installation is aborted and the results are added to the installer log file.



7.2 Troubleshooting Enrollment

This section describes how to troubleshoot problems that can occur during the enrollment process.

For more information about the enrollment process, refer to the enrollment guide in the integration package.

The Factor Management application fails to open, or crashes immediately after opening

The Factor Management application requires .NET Framework version 4.5.2 or higher to be installed on the platform. In some cases, the application opens if an earlier version of .NET Framework is installed, but does not work correctly. If you are experiencing problems with the Factor management application, make sure that .NET Framework version 4.5.2 or higher is installed on the platform.

The Factor Management application shows a message: “No Factors To Manage”

This message is shown when Intel Authenticate has been installed, but a valid policy is not enforced. Make sure that you have deployed the policy to the platform, and that the policy is a valid policy containing at least one action and one authentication factor.

*Other names and brands may be claimed as the property of others

The user deferred enrollment, but now wants to enroll their factors

The user can manually open the Factor Management application by opening the Search window and typing "Intel Authenticate".

Problems with Bluetooth Proximity enrollment

Enrollment of the Bluetooth Proximity factor includes a number of steps, each of which can fail for different reasons. The main steps are described here, in order, with possible problems and their solutions:

1. Make sure that Bluetooth is enabled on the user's computer and the user's phone that they are trying to enroll.
2. The "Protected" security level of the Bluetooth Proximity factor requires the Intel Authenticate app to be installed on the phone. Make sure that the user has installed the app on the phone that they are trying to enroll. The Bluetooth Proximity page in the Factor Management application includes links to download and install the app. The user might have continued in the enrollment process without first installing the app. Ask the user to find and open the app on their phone. They will need to use the app later in the enrollment process anyway.
3. The first step in the Bluetooth Proximity enrollment process is to detect the user's phone. The Factor Management application displays a list of nearby phones. The list includes paired and unpaired phones. If the user's phone does not appear in the list:
   - For Android phones, ask the user to open the app and click the "Make Discoverable" button.
   - For iPhones:
     - "Protected" security level: The Intel Authenticate app must be open on the phone before the Factor Management application can detect the phone. If they have not already done so, ask the user to open the app on their phone.
     - "Soft" security level: Ask the user to open the Settings > Bluetooth page on their phone.
   - In the Factor Management application, ask the user to click **Refresh the list** to scan for the phone again.
   - If the user's phone still does not appear in the list, make sure that Windows itself can detect the phone. In Windows, ask the user to verify that their phone is shown in the list of Bluetooth devices detected by Windows. The Factor Management application can only detect and enroll a phone if it is successfully detected by Windows. If the phone is not detected by Windows, you will need to fix the underlying problems with Bluetooth connectivity before the user can enroll their phone.
   - If the phone is already paired in Windows, but still does not appear in the list, ask the user to check the status of the phone in the Device Manager window. The user's paired phone appears as an entry under the Bluetooth section. If a yellow warning icon appears next to the phone name, right-click the phone name and select **disable** and then **enable**. The Factor Management application cannot detect phones that are disabled or have warnings in the Device Manager window.
4. After the user's phone is successfully detected, the user must select their phone from the list. If the phone is not already paired, the user is shown a pairing code and asked to confirm pairing the phone. The user must confirm this request on both the phone and on the computer:
   - The pairing code is sometimes not easily visible on the phone because it can open in the background. If the user hears a notification sound, but the pairing code is not visible, ask them to swipe down and find the code.
   - If the user made a mistake, (for example, confirming on the phone but denying on the computer) they will need to wait until the Bluetooth connection is "released" before they can try again.

*Other names and brands may be claimed as the property of others

5. For the "Protected" security level, after the phone is paired the final step is to enroll the phone with Intel Authenticate:
   - Before continuing, the user must open the Intel Authenticate app and make sure it is showing a "waiting for a signal" message. If the app is not open, an error message is shown. To continue, the user must click **Try again** in the Factor Management application.
   - A code is shown in the Factor Management application. The user must enter this code in the Intel Authenticate app. If an incorrect code is entered, error messages are shown in the Factor Management application and on the phone. To continue, the user must click **Start Again** in the app, and **Try again** in the Factor Management application.

7.3 Troubleshooting OS Login

This section describes how to troubleshoot problems that can occur when using the OS Login action.

OS Login with Intel Authenticate fails

These are the most common reasons why a user cannot login to Windows using Intel Authenticate:

- After enrollment, the user tried to log in using Intel Authenticate without first logging in using their Windows password. The first login after enrollment must be performed using the Windows password. After that, the user can start to log in using Intel Authenticate.
- The user has changed their password. The first login after changing the Windows password must be performed using the Windows password. After that, the user can continue to log in using Intel Authenticate.
- The user has not enrolled enough required factors for the OS Login action. If this is the cause of the problem, the status of the OS Login section in the Factor Management application will show the message: "Not enough factors enrolled".
- One of the required services is not running (see Client and Engine on page 11).
- If Bluetooth Proximity is defined as a required factor, login will only succeed if the enrolled phone is detected (see Troubleshooting Bluetooth Proximity on page 66).

Unsupported User Accounts

Intel Authenticate does not support:

- Built-in Window's system accounts.
- Microsoft accounts
- User accounts without a password or with a blank password. (After enrollment with Intel Authenticate, it will no longer be possible to log in to Windows with that user account.)

*Other names and brands may be claimed as the property of others

7.4 Troubleshooting Certificate-Based OS Login

This section describes how to troubleshoot problems that can occur when using certificate-based OS Login.

Login takes a long time in an Intranet only environment

On client platforms that are connected to an Intranet, but have no access to the Internet, OS Login using the Smartcard option can take up to 17 seconds. This is because repeated attempts are made to access the Internet to check the Certificate Revocation List. You can solve this problem by adding a key to the registry of the client platforms in this location:

`HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters`

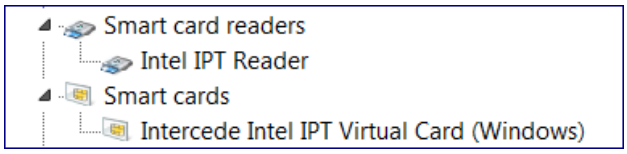
Add a new DWORD Value with these properties:

- Value name: `UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors`
- Value data: 1

OS Login using certificates is not working

When Intel Authenticate is managing the certificates:

- Make sure that you defined the template correctly (see Defining the CA Template for OS Login on page 36).
- Check in the user's personal certificate store that a certificate was issued based on the template name you defined for OS Login.
- In Device Manager:
  - Make sure that the "Intel IPT Reader" exists and also that it is the first entry in the list.
  - Make sure that a Smart card named "Intercede Intel IPT Virtual Card" exists.



Note:

In Windows 10, the "Smart cards" are hidden by default. To show these devices, select **View > Show hidden devices**.

If either of these components are missing, there was a problem during installation.

Note:

If you are using the MyID external certificate manager, the names of these components are different. For troubleshooting the MyID external certificate manager, refer to the MyID documentation.

*Other names and brands may be claimed as the property of others

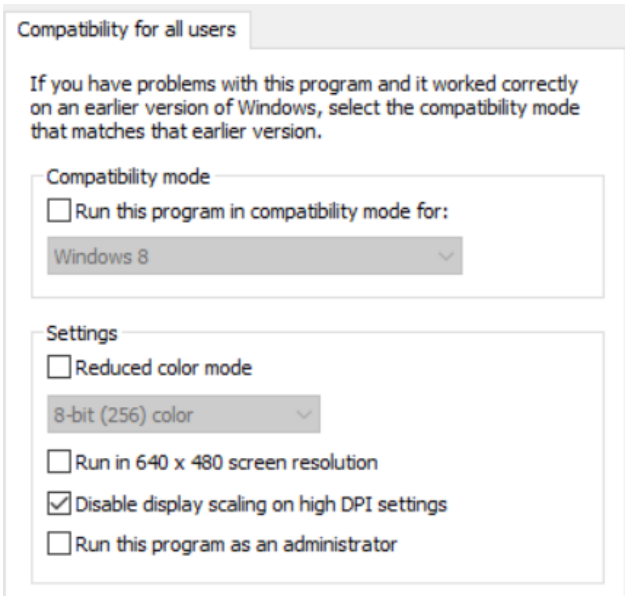
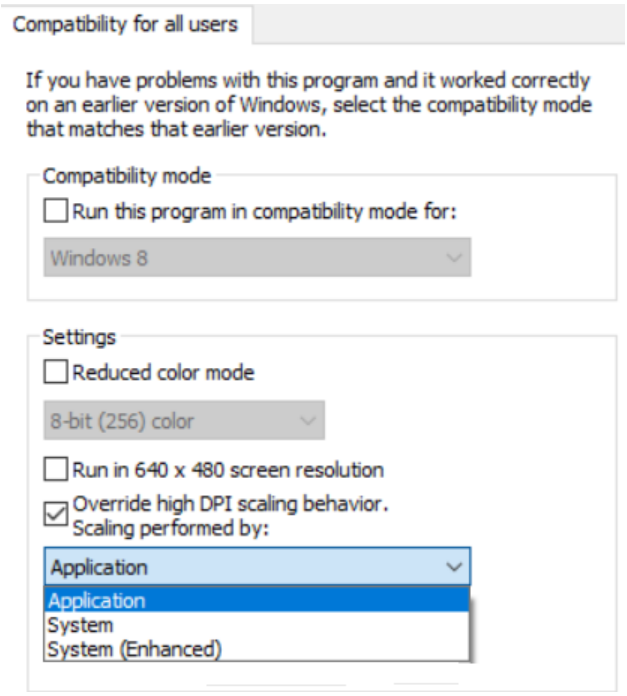
7.5 Troubleshooting VPN Login

In certain conditions during VPN Login, the display of the VPN Client application "shrinks" and the user cannot see the PIN pad and enter their Protected PIN. This problem only occurs if both these conditions are true:

- Protected PIN is defined as an authentication factor for the VPN Login action.
- The platform is configured with high DPI settings for text and other items.

You can solve this problem by changing a compatibility setting of the VPN Client application that you are using on the platform:

1. Locate the executable of the VPN application. For example, the Cisco* VPN application is located here: `C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\vpnui.exe`.
2. Right-click the file, select **Properties** > **Compatibility**, and then click **Change settings for all users**.
3. Define the required setting as described in this table.

Windows 7 and Windows 10 Version 1607	Windows 10 Version 1703 and Higher
	
Select the **Disable display scaling on high DPI** settings check box.	The "**System (Enhanced)**" setting is currently NOT supported by Intel Authenticate. (This setting is set by default by the latest Cisco installers). We recommend to change the selection to "**System**".

*Other names and brands may be claimed as the property of others

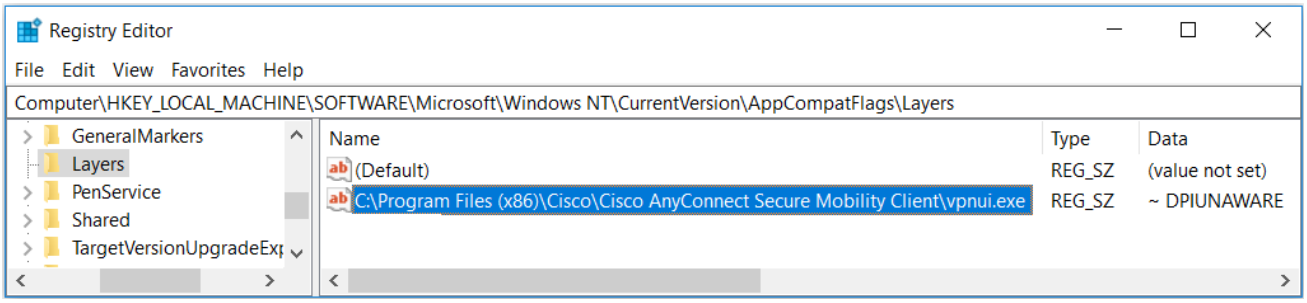
You can define this setting directly in the registry of the platform. If you want to apply this setting for all users of the platform, define the setting in this location:

```
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\AppCompatFlags\Layers
```

The registry key, when set with the values described in the table, has these properties:

- Value name: The full path and name of the VPN Client application executable
- Value data (Windows 7 and Windows 10 version 1607): ~ HIGHDPIAWARE
- Value data (Windows 10 version 1703 and higher): ~ DPIUNAWARE

Example:



7.6 Troubleshooting Bluetooth Proximity

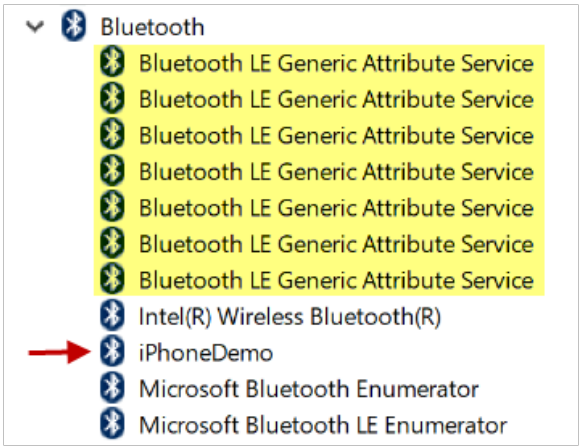
These are the most common reasons why Bluetooth Proximity might stop working:

- The Intel Authenticate app is not running on the user's phone ("Protected" security level only):
  - On many Android phones, background applications are denied from starting up automatically. Make sure that the user has enabled the Intel Authenticate app to always restart automatically. On some Android phones, after upgrading the Android operating system, you might need to manually restart the app.
  - If the user is using an iPhone, make sure that they have not accidentally closed the app. Also, if the user restarted their iPhone, they will need to open the app once and bring it into the foreground. Then ask them to wait for a minute for the computer and the iPhone to re-establish communications. After that, they can move the app back to the background (but they must not close the app).
- There are Bluetooth connection problems with the user's phone. Ask the user to try restarting their phone.
- The user's phone is not in range of their computer.
- The Bluetooth on the user's computer or phone is turned off.
- The user's phone has a low battery, is in airplane mode, or is in a sleep mode that has disabled Bluetooth.
- The user has uninstalled the app from their phone. Uninstalling the app breaks the enrollment connection with the computer ("Protected" security level only). Ask the user to reenroll the Bluetooth Proximity factor. During reenrollment, they will be asked to authenticate using factor sets defined for OS Login (or VPN Login if OS Login is not defined in the policy).
- The user has unpaired their iPhone from the computer. An iPhone generates a new unique Bluetooth address each time it is paired. This means that the address used to pair the iPhone with Intel Authenticate no longer exists. to reenroll the Bluetooth Proximity factor.

*Other names and brands may be claimed as the property of others

Missing Bluetooth LE Generic Attribute Services (Windows 10)

When Bluetooth Proximity using an iPhone fails consistently on Windows 10, it is recommended to check the status of the Bluetooth entry in Device Manager. When an iPhone is enrolled with Intel Authenticate, an entry for the enrolled phone will exist (in this example "iPhoneDemo"). In addition, at least seven entries with the name "Bluetooth LE Generic Attribute Service" must also exist.



If any or all of these entries are missing, this means that an error has occurred in the Microsoft BLE stack. This is an issue that Microsoft is investigating and working to solve in the Windows 10 operating system.

These are the steps to get the missing services back:

1. Turn off the iPhone (complete power down).
2. On the computer, turn Bluetooth OFF and then back ON again.
3. Turn on the iPhone.
4. On the iPhone, open the Intel Authenticate app.
5. Wait for a few minutes for communications between the computer and the iPhone to be restored.
6. Open Device Manager > Bluetooth and verify that at least seven "Bluetooth LE Generic Attribute Service" entries exist.

Problems with Android Security Lock Screen

On some Android phones the security lock screen settings prevent the Intel Authenticate service from starting up again after the phone is restarted. This causes authentication with Bluetooth Proximity to fail. This issue has been seen on Google Pixel 1 and Google Pixel 2 phones. After restarting these phones, you must unlock the screen once to allow the Intel Authenticate service to start up again. After that authentication will succeed.

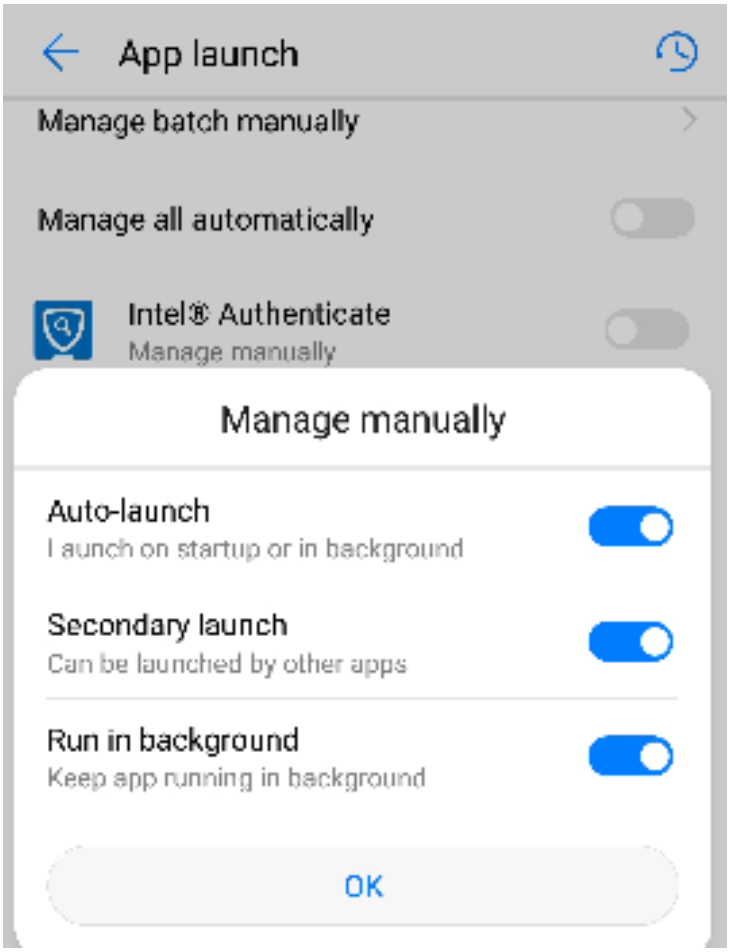
Problems with Xiaomi Phones

On some Xiaomi* phones, if you close the Intel Authenticate app the operating system also closes the Intel Authenticate service. This is because these phones do not allow the Intel Authenticate service to continue running in the background when the app is closed. This means that on these phones you must make sure that the Intel Authenticate app is always running (similar to iPhones).

Problems with New Android Battery Power Saving Settings

From Android 8.0 and higher, new battery power saving options were added to the Android operating system. Some Android phone manufacturers implemented these settings in ways that can shut down the Intel Authenticate service and cause authentication with Bluetooth Proximity to fail. On these phones you must make sure that the power saving settings will not close the Intel Authenticate service. For example:

- On Google Pixel 2 phones, if the battery power saving mode is activated, the Intel Authenticate service is prevented from automatically starting after the phone is restarted. After restarting the phone, you must manually open the Intel Authenticate app once to restart the service.
- On Huawei P20 Pro phones got to `Battery` > `App launch` > `Intel Authenticate` and select **Manage manually**. In the Manage manually screen, make sure that all three options are turned on.



Problems with Huawei Ultra Battery mode

On some Huawei phones, if you turn on the Ultra Battery mode, Bluetooth is turned off (as expected). But when you turn off the Ultra Battery mode, the operating system does not notify the Intel Authenticate app that Bluetooth is now available again. This causes authentication with Bluetooth Proximity to fail, even though Bluetooth is turned on. To fix this issue, open the Intel Authenticate app to refresh the connection.

*Other names and brands may be claimed as the property of others

7.7 Troubleshooting Fingerprint

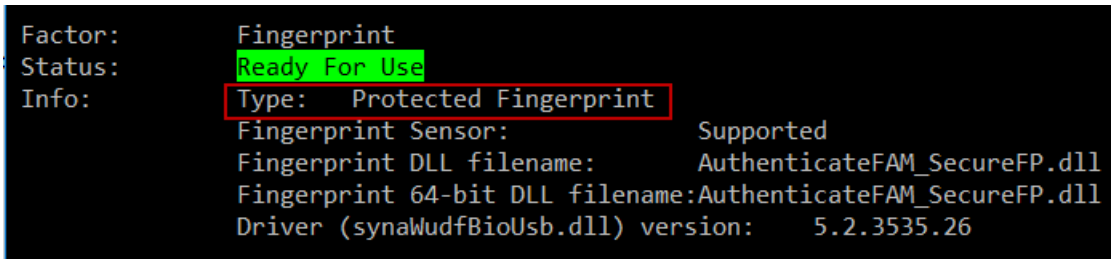
The first thing to check is the status and type of the fingerprint reader. Run this command in the Check tool:

```
Authenticate_Check.exe /f /v
```

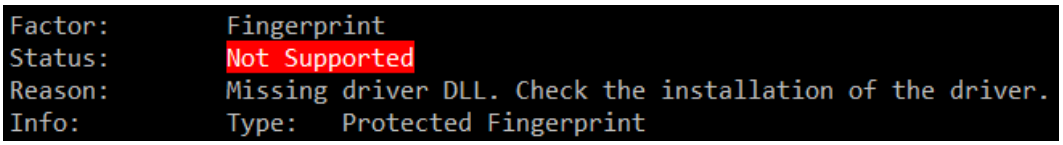
Check the type of fingerprint reader (in the "Info" section).

Protected Fingerprint Readers

Only fingerprint readers with a specific hardware ID are supported as Protected Fingerprint readers (see Prerequisites for Fingerprint on page 19). If the correct fingerprint driver is installed, then the Status field will show "Ready For Use" and the DLL filenames and driver version are displayed.



If there is a problem with the fingerprint driver installation, then the Status will show "Not Supported".



Note:

- If you do not correct the problem before installing Intel Authenticate, then the Soft Fingerprint reader will be implemented instead (see Required Protected Fingerprint DLLs on the next page).
- Installing the correct driver after the user has already enrolled Soft Fingerprint will cause the Soft Fingerprint factor to stop working. To move the user to Protected Fingerprint all you need to do is set the policy again. The user will then need to enroll the Fingerprint factor again in the Factor Management application. After that they will be using the Protected Fingerprint (see Recognizing which type of fingerprint reader is being used on page 71).

*Other names and brands may be claimed as the property of others

Required Protected Fingerprint DLLs

For a fingerprint reader to work as a Protected Fingerprint reader, the fingerprint driver installer must install some special integration DLLs. For the Protected Fingerprint factor to work as expected, Intel Authenticate must successfully detect these DLLs. Intel Authenticate currently uses two detection methods to find the DLLs.

First, Intel Authenticate looks in the `C:\Windows\System32` and `C:\Windows\syswow64` folders for DLLs with these names:

- `AuthenticateFAM_SecureFP.dll`
- `AuthenticateFAM_SecureFP_UI.dll`

If the DLLs are found, then the Protected Fingerprint reader is implemented and no further action is required.

If the DLLs are not found, then Intel Authenticate uses an older detection method. (This detection method will be deprecated after all driver installers have moved to the new method that does not use registry entries). For this method, Intel Authenticate checks the content of these registry keys:

- `HKLM\SOFTWARE\Intel\Intel Authenticate\Engine\Factors\SecureFP\DLLPath`
- `HKLM\SOFTWARE\Wow6432Mode\Intel\Intel Authenticate\Engine\Factors\SecureFP\DLLPath`

The `DLLPath` registry key contains the full path and name of the DLLs. In the old detection method, these were the names of the DLLs:

- `IPTSecureFP.dll`
- `IPTSecureFPUI.dll`

If the DLLs are found, then the Protected Fingerprint reader is implemented and no further action is required.

Note:

- On Lenovo platforms, these versions of the Synaptics fingerprint driver do not work with Intel Authenticate:
  - Version 5.2.351.26 (the issue was fixed from version 5.2.3535.26 and higher)
  - Version 5.1.330.26 (the issue was fixed from version 5.1.335.26 and higher)
- On HP systems, some versions of the Synaptics fingerprint driver installers have a bug where they do not install the `IPTSecureFPUI.dll`. Without a GUI DLL, the fingerprint reader cannot display a GUI for the user to provide their fingerprint. This causes OS Login and VPN Login using the fingerprint factor to fail on these platforms. This issue was fixed in version 5.2.5016.26 and higher of the driver. To fix the issue, upgrade the driver.
- You can check exactly which files a fingerprint driver has installed using Device Manager. In the **Driver** tab, click **Driver Details** to display all the installed files.

*Other names and brands may be claimed as the property of others

Soft Fingerprint Readers

Before Intel Authenticate is installed, the Status field will show "Supported":

```
Factor:         Fingerprint
Status:         Supported
Reason:         The Soft Fingerprint DLLPath registry key is missing. (This registry key, and the DLL to which it
                points, are added when Intel Authenticate is installed.)
```

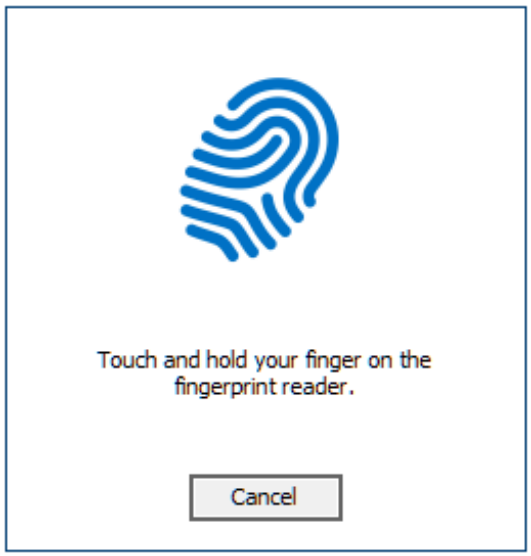
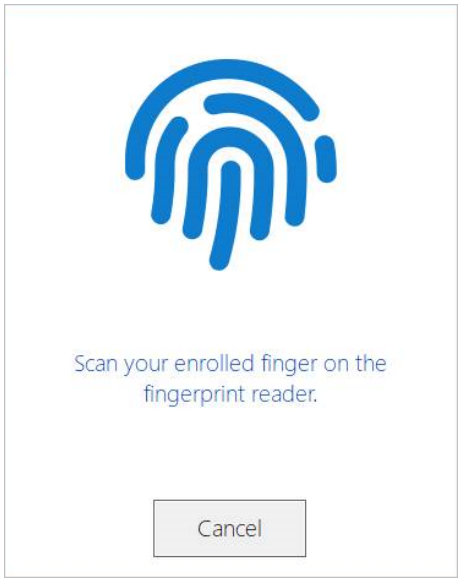
This is expected because the required DLLs are installed by Intel Authenticate (in `C:\Program Files\Intel\Intel Authenticate\Engine\Factors\SoftFP`).

After Intel Authenticate is installed, the Status field must show "Ready For Use".

```
Factor:         Fingerprint
Status:         Ready For Use
Info:           Type:    Soft Fingerprint
                Fingerprint Sensor:              Supported
                Fingerprint DLL filename:        SoftFingerPrint.dll
                Fingerprint 64-bit DLL filename:SoftFingerPrint64.dll
```

Recognizing which type of fingerprint reader is being used

The GUI displayed to the end user is different for each type of fingerprint reader.

"Protected" Fingerprint	"Soft" Fingerprint
	

*Other names and brands may be claimed as the property of others

Fingerprint enrollment fails to read the fingerprints

For the fingerprint factor of Intel Authenticate to work as expected, the fingerprint reader must be capable of reliably reading the user's fingerprints. If the fingerprint reader has difficulty reading the user's fingerprints, then authentication using the fingerprint factor of Intel Authenticate will also be problematic. The first place to identify this type of problem is during enrollment of the user's fingerprints. If during enrollment there is a problem with recognizing fingerprints, then you need to investigate with the platform manufacturer what is the cause of these problems.

Note:

When this problem occurs, try registering a different finger. Sometimes the fingerprint of specific fingers are too fine or too deteriorated for the fingerprint reader to reliably read them.

7.8 Troubleshooting Face Recognition

To use the Face Recognition factor, the user must first be able to enroll their face with Windows. The first thing to check is that the user can successfully enroll their face in Windows. Any failure to enroll face in Windows must be solved before you can enroll and use the Face Recognition factor (see Troubleshooting Windows Hello on the next page).

The camera fails to authenticate the user's face

During authentication, messages are shown on the screen telling the user why the camera is having difficulty authenticating their face. Usually, after following the instructions, authentication will succeed. Differences in the level of light available to the camera can also cause authentication to fail. Most users will enroll their face when at the office, which often has very different lighting than their home environment. If authentication is failing when they are at home, ask the user to enroll their face again, when at home. To do this they just need to click **Improve recognition** in the Sign-in options page. They do not need to re-enroll the factor in Intel Authenticate.

*Other names and brands may be claimed as the property of others

7.9 Troubleshooting Windows Hello

Troubleshooting Windows Hello is beyond the scope of this guide. But because on Windows 10 the Face Recognition factor depends on Windows Hello, this section includes some information that might help you. For full instructions how to troubleshoot Windows Hello, refer to the Microsoft documentation.

All Windows Hello setup options are disabled in the “Sign-in options” page

Depending on the Windows version, Microsoft have made several changes to how Windows Hello is activated and enabled. These articles explain some of the changes that might disable the Windows Hello setup options:

- Changes to convenience pin
- Windows Hello for Domain Users

The face recognition option is missing in the “Sign-in options” page

This option is only displayed if a valid camera driver is installed (see Prerequisites for Face Recognition on page 20). In Device Manager, make sure that a supported camera driver is installed and functioning correctly. Refer to the manufacturers website to verify that you have the correct driver installed for the platform.

We have seen that on some platforms, for example the Dell XPS 13 9365, the Face Recognition option is not available on Windows 10 version 1607. But, after upgrading to Windows 10 version 1703, the option was added to the Sign-in options page.

The fingerprint option is missing in the “Sign-in options” page

This option is only displayed if a valid fingerprint driver is installed. In Device Manager, make sure that the fingerprint driver is installed and functioning correctly. Refer to the manufacturers website to verify that you have the correct driver installed for the platform.

The fingerprint or face recognition enrollment GUI do not open

On some platforms when you click the **Set up** button to open the fingerprint or the face recognition enrollment GUI, nothing happens. Instead, the GUI “flashes” for a split second but does not open.

To fix this issue:

1. Open the Group Policy Editor.
2. Browse to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.
3. Right-click **User Account Control: Admin Approval Mode for the Built-in Administrator account** and select **Properties**.
4. Select **Enabled**.
5. Restart the computer.
6. Go back to the Sign-in options page and open the fingerprint or face recognition enrollment GUI.

*Other names and brands may be claimed as the property of others

7.10 Using the Support Tool

The Support tool is a CLI-based tool, located in the `Tools > SupportTool` folder. The Support tool is also installed on the client platforms in this folder: `C:\ProgramData\Intel\Intel Authenticate\Engine\SupportTool`.

You can use the Support tool to:

- Start or stop debug logging sessions
- Collect and package end-user logs into a zip file
- Restart all services and processes of Intel Authenticate (this can sometimes "fix" problems)

The CLI syntax is not case-sensitive. Only one flag can be used per call. This is the syntax:

```
Authenticate_Support.exe [ /StartDebug | /StopDebug
 /CollectLogs | /Restart | /? ]
```

Flag	Details
`/StartDebug`	Creates a debug logging session and begins collecting logs into an ETL file
`/StopDebug`	Stops any active debug logging session
`/CollectLogs`	Collects all existing Intel Authenticate logs and places them in a zip file
`/Restart`	Restarts all associated Intel Authenticate services and processes
`/?`	Help

*Other names and brands may be claimed as the property of others

7.10.1 Collecting Logs

Intel Authenticate saves logs in several locations. The Support tool enables you to easily collect all the logs. Once collected, the tool then packages the logs into a zip file in the folder from which it was run. You can then send the zip file to your customer or field support engineer for debugging. The zip file is automatically named using this format: `AuthenticateLogs_HostName_YYYY-MM-DD-HH-MM-SS.zip`.

For information about support options for Intel Authenticate, go to Intel Customer Support.

To collect logs:

1. Open a command prompt as an administrator.
2. Start a debug logging session:
   ```
   Authenticate_Support.exe /StartDebug
   ```
3. Perform the problematic action. Note the platform system time when the action was initiated. This will help the support engineer pinpoint the relevant area in the log files.
4. Collect the logs:
   ```
   Authenticate_Support.exe /CollectLogs
   ```
5. Stop the debug logging session:
   ```
   Authenticate_Support.exe /StopDebug
   ```
6. Send the collected logs zip file to the support engineer handling your support ticket.

7.10.2 Restarting Services and Processes

The Support tool restarts:

- jhi_service.exe (service)
- IAClientService.exe (service)
- IAEngineService.exe (service)
- IAMonitor.exe (process)

The tool also uninstalls and reinstalls Intel Authenticate applets. The `Restart` command must be run in elevated mode.

Restarting Intel Authenticate processes retains the end-user's provisioned policy and stored enrollment data. This is less disruptive to the end-user than a system or factor reset which deletes policy and enrollment data.

To restart associated services and processes:

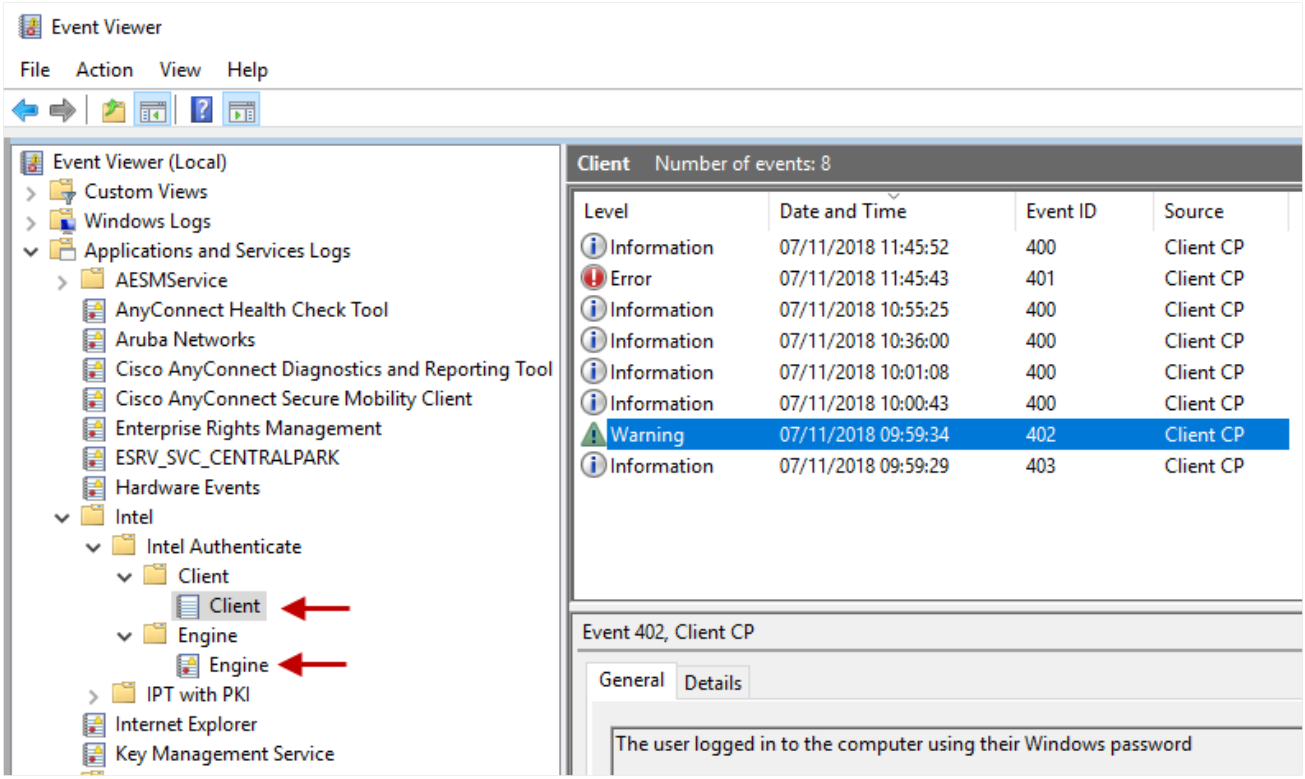
```
Authenticate_Support.exe /Restart
```


*Other names and brands may be claimed as the property of others

7.11 Event Viewer IDs

Intel Authenticate records events for many actions in the Event Viewer. Depending on which component recorded the event, the events are located in these locations:

- Intel > Intel Authenticate > Client
- Intel > Intel Authenticate > Engine



This table describes the events recorded by Intel Authenticate.

Event ID	Description	Event Type
100	The policy was applied successfully	Informational
101	Failed to apply the policy **Note:** When setting a policy, one event with this ID is always generated with the details "No credentials set on client". You can ignore these event instances.	Error
102	Admin credentials were set successfully	Informational
103	Failed to set administrative credentials	Error
104	Intel Authenticate was reset successfully	Informational
105	Failed to reset Intel Authenticate	Error

*Other names and brands may be claimed as the property of others

Event ID	Description	Event Type
106	Upgrade completed successfully	Informational
107	Upgrade failed	Error
120	Bluetooth Proximity factor enrolled successfully (Soft)	Informational
121	Bluetooth Proximity factor enrolled successfully (Protected)	Informational
122	Protected PIN factor enrolled successfully	Informational
123	Face Recognition factor enrolled successfully	Informational
124	Fingerprint factor enrolled successfully (Soft)	Informational
125	Fingerprint factor enrolled successfully (Protected)	Informational
126	Intel AMT Location factor enrolled successfully	Informational
127	Physical Smartcard factor enrolled successfully	Informational
140	Failed to enroll the Bluetooth Proximity factor (Soft)	Error
141	Failed to enroll the Bluetooth Proximity factor (Protected)	Error
142	Failed to enroll the Protected PIN factor	Error
143	Failed to enroll the Face Recognition factor	Error
144	Failed to enroll the Fingerprint factor (Soft)	Error
145	Failed to enroll the Fingerprint factor (Protected)	Error
146	Failed to enroll the Intel AMT Location factor	Error
147	Failed to enroll the Physical Smartcard factor	Error
160	Bluetooth Proximity factor unenrolled successfully (Soft)	Informational
161	Bluetooth Proximity factor unenrolled successfully (Protected)	Informational
162	Protected PIN factor unenrolled successfully	Informational
163	Face Recognition factor unenrolled successfully	Informational
164	Fingerprint factor unenrolled successfully (Soft)	Informational
165	Fingerprint factor unenrolled successfully (Protected)	Informational
166	Intel AMT Location factor unenrolled successfully	Informational
167	Physical Smartcard factor unenrolled successfully	Informational
180	Failed to unenroll the Bluetooth Proximity factor (Soft)	Error

*Other names and brands may be claimed as the property of others

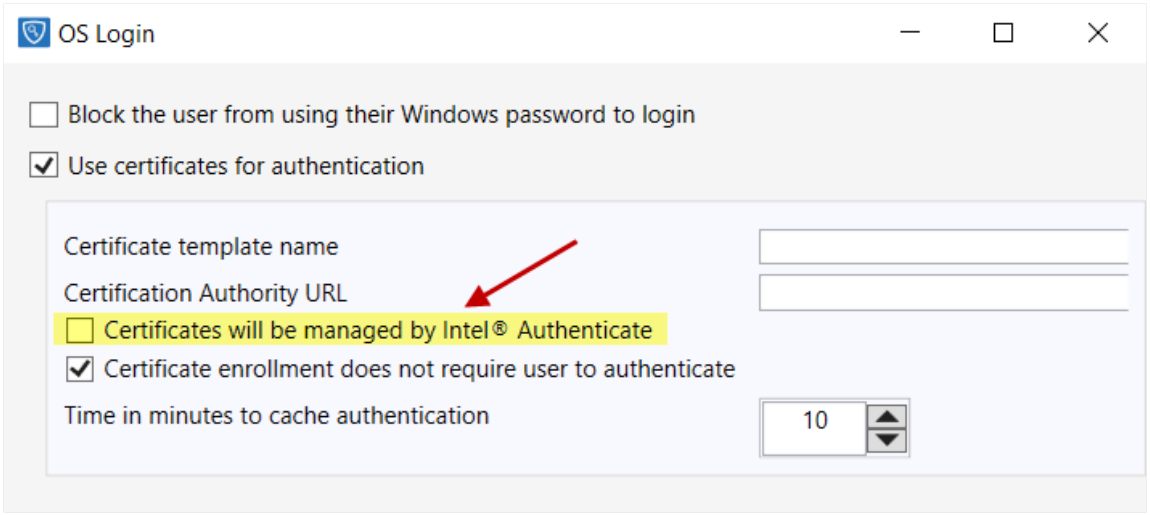
Event ID	Description	Event Type
181	Failed to unenroll the Bluetooth Proximity factor (Protected)	Error
182	Failed to unenroll the Protected PIN factor	Error
183	Failed to unenroll the Face Recognition factor	Error
184	Failed to unenroll the Fingerprint factor (Soft)	Error
185	Failed to unenroll the Fingerprint factor (Protected)	Error
186	Failed to unenroll the Intel AMT Location factor	Error
187	Failed to unenroll the Physical Smartcard factor	Error
400	OS Login completed successfully	Informational
401	OS Login failed	Error
402	The user logged in to the computer using their Windows password **Note:** Sometimes the user will be required to login using their Windows password. For example, the first login after the policy is set (or reset) and the user has enrolled their factors. But if you see a lot of these events, this can indicate there is a problem with the installation or that the user is circumventing Intel Authenticate.	Warning
403	The user failed to login to the computer using their Windows password	Informational
420	Failed to authenticate Bluetooth Proximity (Soft)	Error
421	Failed to authenticate Bluetooth Proximity (Protected)	Error
422	Failed to authenticate Protected PIN	Error
423	Failed to authenticate Face Recognition	Error
424	Failed to authenticate Fingerprint (Soft)	Error
425	Failed to authenticate Fingerprint (Protected)	Error
426	Failed to authenticate Intel AMT Location	Error
427	Failed to authenticate Physical Smartcard	Error
500	The computer was locked because Walk-Away Lock was activated	Informational
501	Walk-Away Lock was activated, but the user disabled the action with the keyboard or mouse	Informational

*Other names and brands may be claimed as the property of others

8 Other Certificate Management Options

This section describes alternative methods for managing the certificates used by the certificate-based authentication options of Intel Authenticate. Each action in the Intel Authenticate policy (OS Login, VPN Login, Custom Action) has a check box named "Certificates will be managed by Intel® Authenticate".

For example:



When the **Certificates will be managed by Intel® Authenticate** check box is selected, Intel Authenticate will automatically manage certificates for the action. The certificate is automatically enrolled as soon as the user has enrolled enough factors to use the action. In addition, 10 days before the enrolled certificate expires, Intel Authenticate will automatically start trying to renew the certificate.

If you do not select this check box, you must manage the certificates using one of these methods:

- Integrating with Third-Party Middleware on the next page
- Manually Generating Certificates on page 81

*Other names and brands may be claimed as the property of others

8.1 Integrating with Third-Party Middleware

The built-in certificate management option of Intel Authenticate is only supported when using a Microsoft CA. If your organization does not have a Microsoft CA, you will need to generate and manage the certificates using scripts or third-party middleware. If you are using third-party certificate management software in your organization you also can configure it to manage certificates for Intel Authenticate.

To integrate with Intel Authenticate, you must make changes to your scripts/middleware.

Changes required for integration with Intel Authenticate:

1. The script/middleware must inform Intel Authenticate the name of the action for which the certificate will be generated. To do this, you must use the **CertificateUtility.exe** of Intel Authenticate.

Location	"C:\Program Files\Intel\Intel(R) Identity Protection Technology with PKI\CertificateUtility.exe"	This utility is installed on every client PC when Intel Authenticate is installed
Syntax	`CertificateUtility.exe -c prepare_cert_enroll -a <action name>`	Valid values for <action name>: • **OSLogin** – The OS Login action • **VPNLogin** – The VPN Login action • **<Custom Action Name>** – The name of a custom action, exactly as defined in the Intel Authenticate policy

   Example:

```
CertificateUtility.exe -c prepare_cert_enroll -a OSLogin
```

2. The **prepare_cert_enroll** command must be called immediately before calling the command to generate the key pair for the Certificate Signing Request (CSR). After the prepare_cert_enroll command is run, the command to generate the key pair for the CSR must be called within 60 seconds.
3. The command used to generate the key pair for the CSR must use one of these Intel Authenticate providers:
   - "Intel IPT CSP - Non-Exportable Keys"
   - "Intel IPT Non-Exportable Key Storage Provider"
4. If you want to use the Smartcard option of OS Login, then complete steps 1-3, but with these additions/changes:
   a. In step #3, you must use one of these providers instead:
      - "Microsoft Base Smart Card Crypto Provider"
      - "Microsoft Smart Card Key Storage Provider"
   b. You must use this smart card reader name: "Intercede Virtual Reader 0".

*Other names and brands may be claimed as the property of others

8.2 Manually Generating Certificates

> **Note:**
>
> This method is only available when using a Microsoft CA.

During installation of Intel Authenticate, a utility named `CertificateUtility.exe` is installed on each platform. The utility is installed in this folder: `C:\Program Files\Intel\Intel(R) Identity Protection Technology with PKI`. You can use this utility to manually generate certificates on the client platforms. This is the syntax:

```
CertificateUtility.exe -c create_cert -a <action name> [-u <ca_url>] [-t <template name>]
```

Parameter / Variable	Details
`-a <action name>`	The action name for which to issue the certificate. Valid values: • **OSLOGIN** – The OS Login action • **VPNLogin** – The VPN Login action • **<Custom Action Name>** – The name of a custom action, exactly as defined in the Intel Authenticate policy
`-u <ca_url>`	The certificate authority URL. If not supplied, the tool will loop over all CAs found on the Domain and try to send the request to each CA.
`-t <template_name>`	The name of the certificate template. Make sure that you spell the name exactly as you defined it in the certificate template.

Example of generating a certificate for OS Login:

```
CertificateUtility.exe -c create_cert -a OSLogin -t <template_name>
```

Example of generating a certificate for VPN Login:

```
CertificateUtility.exe -c create_cert -a VPNLogin -t <template_name>
```

Example of generating a certificate for a custom action:

```
CertificateUtility.exe -c create_cert -a <action_name> -t <template_name>
```


*Other names and brands may be claimed as the property of others