Intel® Authenticate

Release Notes

Version 3.5.2

Document Release Date: 18 July, 2018

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.

© 2016-2018 Intel Corporation

Table of Contents

1 Introduction

This document describes new features and changes made in version 3.5 of Intel® Authenticate. This document also describes limitations and known issues with this version.

2 Changes and New Features

This section describes the main new features and changes included in Intel Authenticate 3.5.

2.1 Support for New Processors

Intel Authenticate now supports platforms with these new processors:

- Intel 8th Generation Core processors
- Intel® Xeon® E-2186M
- Intel® Xeon® E-2176M

2.2 New Check Tool Data Gathering Options

Two new flags were added to the Check tool:

- `/WMI` - Generates WMI discovery data in "`root\cimv2`" for collection by third party tools
- `/SCCM` - Generates WMI discovery data in "`\root\cimv2\sms`". This flag can only be used on platforms that are managed by SCCM. This data can be automatically collected by the hardware inventory mechanism of SCCM. This flag is used in the new integration method of SCCM (see New Simplified Microsoft* SCCM Integration on page 7).

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

The data collected by these commands will help you to identify which platforms in your network support Intel Authenticate. The data also includes information about the status of the factors that they can support. For information about the classes created by these commands and the data that they contain, refer to the "Gathering Data Remotely via WMI" section in the integration guide.

2.3 Changes to Factor Re-enrollment

For increased security, whenever a user wants to re-enroll an already enrolled factor they must authenticate before they can continue. For example, if they want to replace their enrolled phone or change the PIN they defined for Protected PIN. By default, the user must authenticate using the same factor that they want to re-enroll. But sometimes that might not be possible. For example, if they lost their currently enrolled phone or forgot their PIN. In previous versions, these scenarios required a reset of Intel Authenticate.

In version 3.5, 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. This change will help users to be more self-sufficient in managing their factor enrollments, and also reduce support calls.

2.4 New Custom Actions

> 📝 **Note:**
>
> Custom actions are currently not supported when deploying via McAfee ePO.

In addition to the built-in actions, Intel Authenticate now 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.
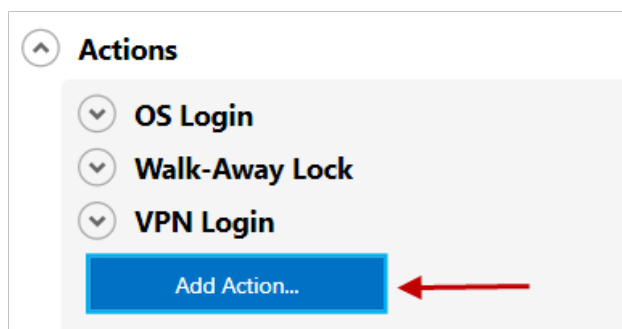
For an example how to define a Web Login action, refer to the "Setting Up Web Login" section in the integration guide.

2.5 New Policy Settings for Certificate-Based Actions

> 📝 **Note:**
>
> These new policy settings are currently not supported when deploying via McAfee ePO.

In version 3.5, new options were added to the policy for all actions that can support certificate-based authentication (OS Login, VPN Login, custom actions). These options enable you to define, for each action, if authentication will be certificate-based. In addition, you can define who will manage the certificates.

To define the new settings, click **Action Settings** in the relevant action. Here is an example of the new settings.

☑ Use certificates for authentication

Certificate template name	
Certification Authority URL	
☑ Certificates will be managed by Intel® Authenticate	
☑ Certificate enrollment does not require user to authenticate	
Time in minutes to cache authentication	10

Setting	Description
Use certificates for authentication	If this check box is selected, certificates will be used for authentication of the action
Certificate template name	The exact name of the certificate template to use for the action. 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 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 manually generate and manage the certificates.

Setting	Description
Certificate enrollment does not require user to 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)

2.6 New Certificate Template Tool

Actions and features of Intel Authenticate that use certificates require a certificate template to exist on the Certification Authority (CA). For example, the VPN Login action requires a certificate template. The `Tools` folder now includes a new tool (`CertificateTemplateSetup.exe`) that you can use to create these certificate templates on the CA. The certificate templates are created with all settings that are required by Intel Authenticate.

This is the syntax:

```
CertificateTemplateSetup.exe -c
create [-s <yes | no >] [-n <template_name>] [-d <display_name>] [-o <oids>]
remove [-n <template_name>]
```

Parameter / Variable	Description
`create`	Creates the certificate template on the CA
`remove`	Removes the certificate template from the CA
`-s <yes | no >`	The certificate template type. Valid values: • `yes` - Smartcard template (used only for the OS Login action) • `no` - Template for non Smartcard use (VPN Login, custom actions)
`-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. 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"

2.7 Changes to the OS Login Smartcard Option

In previous versions, it was not possible to control when the Smartcard option of OS Login was activated. If Intel Authenticate detected a Smartcard certificate template (with a specific name) on the CA, then the Smartcard option was automatically activated for all users. This also made it impossible to define separate policies to enable the Smartcard option only for certain users.

In version 3.5, the Smartcard option is now enabled / disabled in the policy.

For more information, refer to the "Defining Smartcard in the Policy" section in the integration guide.

> **📝 Note:**
>
> If you implemented the Smartcard option using an earlier version, the option will continue to work on client platforms where it is already enabled. But the option will not be enabled for new users unless you set a new policy with the new settings.

2.8 New Data Migration Option

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, (for example during upgrade to version 11.8.50.339), the data in the Intel ME Firmware is rendered invalid. You now 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.

- **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, Smartcard, 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**

2.9 New Policy Editor

> 📝 **Note:**
>
> This section is not relevant for deployment via McAfee ePO.

The "Profile Editor" component of Intel SCS has been replaced with a new "Policy Editor" specifically created to manage policies for Intel Authenticate. In addition, the method for defining which factors will be used for each action has been simplified. Now all you need to do is define the "combinations" of factors that you want the user to supply for authentication. The order in which you define the combinations is the order in which they will be used by Intel Authenticate.
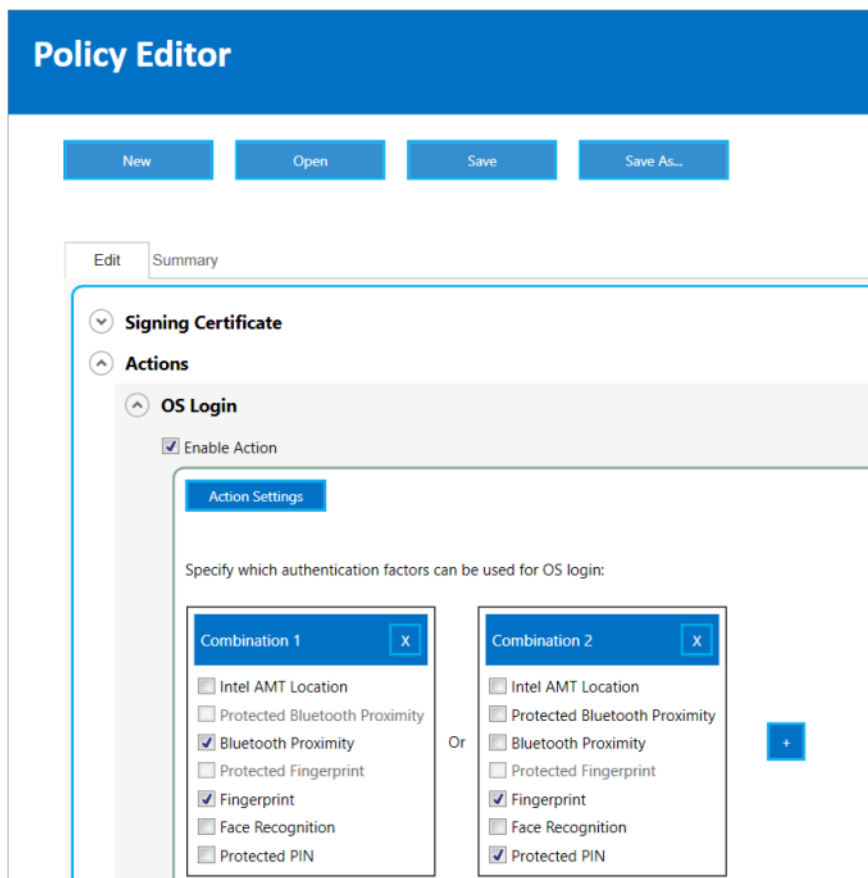
> 📝 **Note:**
>
> Version 3.5 of Microsoft .NET Framework must be installed on the computer where you want to run the Policy Editor.

2.10 New Simplified Microsoft* SCCM Integration

In previous versions, deployment via Microsoft SCCM was unnecessarily complicated and relied on several components of Intel® Setup and Configuration Software (Intel® SCS).

Note:
If you installed the Intel Authenticate plugin from an earlier version, it is recommended to uninstall it before installing the new Add-on. (And delete the old collections, deployments, packages, and task sequences.)

These are the major improvements in version 3.5:

- All dependency on Intel SCS components has been removed (no Intel SCS components are used). This means that all aspects of integration with SCCM are much simpler and focused totally on Intel Authenticate.

- Integration with SCCM is now done using a new Intel® Authenticate Add-on for Microsoft* SCCM (referred to in this document as the "Add-on"). The new Add-on is a very simple installer that creates the collections, deployments, packages, and task sequences that you will need to deploy Intel Authenticate.

- The number of collections, deployments, packages, and task sequences, used in integration is much lower than previous versions. The collections also split the platforms into more logical groups based on their current status. This makes it much easier to track the status of platforms and run the relevant task sequences until all platforms are fully deployed.

- The new "Intel Authenticate: Discover" task sequence runs the Check tool with the new /SCCM flag (see New Check Tool Data Gathering Options on page 1). After you have run this task sequence, and hardware inventory is collected, the data will be available in your SCCM database. You can then create reports in SCCM based on this data. You can also view the data for each platform using the Resource Explorer option of SCCM.

- A new "Auto Deployment" option is now available. When this option is used, deployment of Intel Authenticate on the client platforms occurs automatically. First, the "Discovery" task sequence identifies status of the platforms. On platforms that are ready to install, Intel Authenticate is automatically installed and the policy is then automatically enforced.

2.11 New User Console Permissions in McAfee* ePO

New permissions for Intel Authenticate were added to the McAfee ePO console. Access to certain functionality in the McAfee ePO console is controlled via permissions. By default, users with admin permissions are granted all permissions. For all other console users you must make sure that they have the necessary permissions for the tasks that they need to perform.

Permission	Description
Intel® Authenticate Policy	Defines what users can do in the Policy Catalog regarding Intel Authenticate policies. Valid values: • **No permissions** - Users cannot view or edit policies • **View policy** - Users can only view policies • **View and change policy** - Users can view and edit policies. Users without admin permissions can only edit policies that they created. **Note:** The "My Default" policy is always read only for users without admin permissions
Intel® Authenticate Recovery	Defines what users can do in the Intel Authenticate "Recovery" page. Valid values: • **No permissions** - Users cannot see or access the Recovery page • **View recovery screen and execute commands** - Users can see and access the Recovery page and perform all reset commands • **View recovery screen only** - Users can only view the information in the Recovery page but cannot perform any reset commands

2.12 New Look and Feel for Protected PIN

The GUI displayed to the end user when using the Protected PIN factor has been updated to look more modern and easier to use.
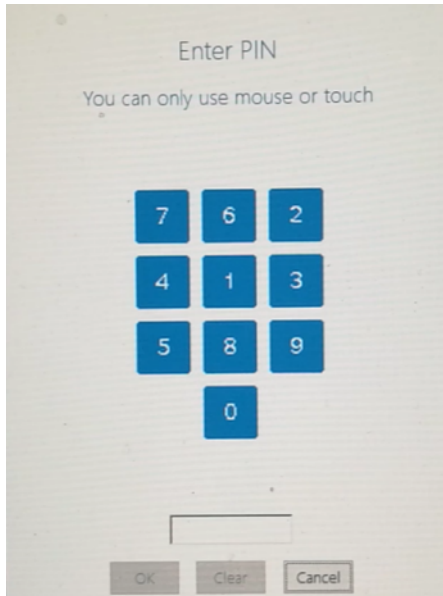
> 📝 **Note:**
>
> This screenshot is of low quality because it was taken using a camera. (A screenshot taken using screen capture software would display a black box instead of the keypad. This is part of the built-in protection of Protected PIN.)

3 Known Limitations

This table describes known limitations with Intel Authenticate and other components on which it depends.

Description	Workaround
When using iPhones* with Windows 10, the Bluetooth® Proximity factor can sometimes stop working because the Bluetooth LE Generic Attribute Services in Device Manager have "disappeared". This issue only affects the "Protected" security level of the Bluetooth Proximity factor, and usually occurs after power state changes on the computer. **Note:** We recommend to use version 20.0.0.11 of the Intel® Wireless Bluetooth® driver. We have found that this issue rarely occurs when using this version.	The cause of the disappearance of the BLE services is under investigation with Microsoft. For information how to detect and solve this issue, refer to this section of the integration guide: "Missing Bluetooth LE Generic Attribute Services (Windows 10)".
When using iPhones with Windows 10, the "Protected" security level of Bluetooth Proximity can sometimes take longer than expected to authenticate. This can occur if additional Bluetooth devices are paired to the computer, and especially if connection to one of the devices fails.	None
Users with Intel Authenticate enabled systems will not be able to see any other credential provider on the Windows login screen. When enabled, Intel Authenticate replaces any other credential provider in the system (Biometric, Password reset tool, etc.). Intel Authenticate is not compatible with software solutions that replace or prevent access to the Microsoft Credential Provider. Many Single Sign On (SSO) solutions provide their own Credential Providers that either replace or prevent access to the Microsoft Credential Provider. Checkpoint PBA*, OmniPass*, Lenovo* Fingerprint Manager Pro, and HP Client Security* are examples of software solutions that are NOT compatible with Intel Authenticate for this reason. If you are using a SSO solution in your network, check with the software vendor if they allow other software to access the Microsoft Credential Provider.	None

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

Description	Workaround
If a user defines and activates a Microsoft account for login, Intel Authenticate will not be available for that user. They will only be able to login using the Microsoft account.	Intel Authenticate is not compatible with Microsoft Accounts. Before installing Intel Authenticate, make sure that you disable Microsoft Accounts on the computer. You can do this in Group Policy by selecting the **Users can't add or log on with Microsoft accounts** option. (The option is located in Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Accounts: Block Microsoft accounts).
Many of the latest HP platforms come with these pre-installed components: • HP Client Security Manager • HP Device Access Manager If they exist, before you install Intel Authenticate, you must make sure that they are both completely removed.	None
Intel Authenticate does not support enrolling and using multiple user accounts on the same computer. (Only one active user account is supported.)	None
For the OS Login option to work, Intel Authenticate requires the user details to be displayed in the login screen. Therefore, any options that hide or prevent the user details from being displayed must not be enabled. For example, these settings in Group Policy Settings are NOT supported: • Interactive Login: Do not display last signed-in • Interactive Login: Display user information when the session is locked (when enabled with "Do not display user information" or "User display name only")	Do NOT enable these settings or any settings like them that hide the user details on the login screen. These settings are located in the Group Policy Editor here: Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.
Locking the computer during unenrollment of an authentication factor can cause unenrollment to fail. This can occur if you lock the computer before you authenticate (unenrollment requires you to authenticate before you can continue). Also, because the unenrollment process was interrupted, it can take up to 45 seconds to log back into the computer.	If you want to unenroll an authentication factor, do not lock the computer until unenrollment of the factor has completed. If you did lock the computer by mistake, simply log in and start the unenrollment process again
Replacing fingerprint reader hardware on a system where the Protected fingerprint factor was enrolled will not automatically work with Intel Authenticate. Enrollment and authentication will fail.	Intel Authenticate must be removed and reinstalled by the administrator

Description	Workaround
After enrollment of the Face or Fingerprint factors, Intel Authenticate cannot detect if the user removes their fingerprint or face registration from Windows Hello. When this occurs, the Factor Management application will show that the Face / Fingerprint factor is still enrolled (even though authentication cannot succeed).	1. Reenroll the factor (Face / Fingerprint) in Windows Hello. 2. Open the Factor Management application and reenroll the factor again. During reenrollment, you will need to authenticate with other factors that were defined for the OS Login action (or the VPN Login action). If no other factors were defined in the policy, then you will need to reset Intel Authenticate and set the policy again.
After restarting the computer, it can take approximately five seconds for the computer to establish a wireless connection. If after restarting the computer, the user logs in before the WiFi connection is established, Intel AMT Location will incorrectly return a status of false.	When using Intel AMT location and WiFi profiles, after restarting the computer wait until WiFi connection is established before trying to log in
Remote enrollment and enrollment of a non active user is not supported.	Only the active local user can enroll factors
If there is an error during Bluetooth Proximity enrollment the error is only displayed on the computer and not on the Intel Authenticate app on the phone.	If you see an error on the computer, an phone status is "Waiting for a signal from your PC/laptop", try enrollment again on the computer. If the 'Waiting for a signal..' screen is not displayed because the connection timed out, press **Start Again**.
On Windows 10, if external monitors are connected to a USB replicator, the display is sometimes corrupted. This can occur when the Protected PIN keypad is displayed (during enrollment or authentication).	Disconnect from the USB replicator to complete enrollment / authentication.

4 Resolved Issues

This table describes the issues which were resolved in version 3.5.2 of Intel Authenticate

ID	Description
DE12449	In certain conditions, upgrade of the Intel ME Firmware caused the policy settings to become invalid. This could occur even though the data migration option was enabled.
DE12350	In certain conditions, after the computer returns from sleep or hibernation, authentication was failing immediately without trying to authenticate any factors. Repeated attempts to login continued to fail with the message "Try Again". To recover from this situation required a reboot of the computer.

This table describes the issues which were resolved in version 3.5 of Intel Authenticate.

ID	Description
DE12068	"Protected" Fingerprint sensors with this hardware ID did not work with Intel Authenticate: "VID_138A&PID_00AB". This type of sensor is included in several HP platforms, including: • HP EliteBook 830 G5 • HP EliteBook 850 G5
DE12057	A specific combination of two GPO settings prevented login to the computer (using Intel Authenticate or Windows password). This only occurred if both these settings were defined with these values: 1. Interactive logon: Don't display last signed-in ==> Enabled 2. Interactive Logon: Do not require CTRL+ALT+DEL ==> Disabled **Note:** • Setting #1 must always be set as "Disabled" or "Not Defined". If it is set to "Enabled", login using Intel Authenticate will not be available. • These settings are located in the Group Policy Editor here: Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.
DE11995 DE11994	If Bluetooth is turned off on the iPhone, or the Intel Authenticate app is closed, the phone status indicator incorrectly switched between "Searching For Phone" and "Phone Found".
DE10825	When the Smartcard option was enabled, sometimes when opening an application a "Windows Security" prompt was shown asking for the user's credentials.

This table describes the issues which were resolved in prerequisite components used by Intel Authenticate.

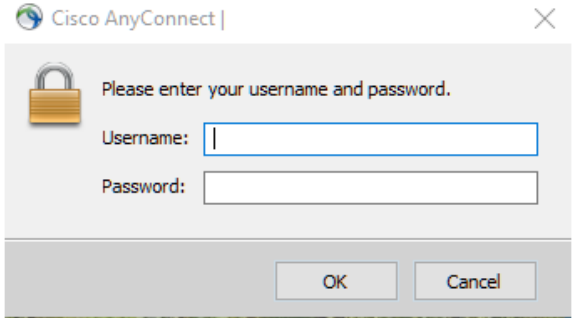| ID	Description
DE11472	Upgrading or uninstalling some versions of the Intel Graphics driver can cause Intel IPT with PTD to stop working. The main Intel Graphics driver versions affected are from 22.20.16.4814 to 22.20.16.4849. If this occurs, it will not be possible to enroll or use the Protected PIN factor or to enroll the Bluetooth Proximity factor ("Protected" security level). You can detect this issue by running the Check tool with the /F /V flags and looking at the status of the Protected PIN factor. This issue was fixed from version 23.20.16.4901 and higher.
DE11183	On some computer models, authentication using the "Soft" fingerprint factor was always failing. The fingerprint GUI was displayed, but the result shown was always "failure to match the fingerprint". This could occur on these platforms: • Dell XPS 13 9360 • Dell XPS 13 9365 2-in-1 • Dell XPS 15 9560 The method used by Intel Authenticate to query the fingerprint reader was changed to overcome errors received from some fingerprint readers when using the old method.
DE11350	When using Bluetooth Proximity with iPhones on Windows 10, if you have a Bluetooth Mouse, the mouse can sometimes stop working. To make the mouse work again it is necessary to got to Settings > Devices and toggle Bluetooth to "Off" an then back to "On" again. Sometimes it is necessary to do this several times, or even restart the computer. This issue was fixed from Intel Wireless Bluetooth driver version 20.20 and higher.
	The fingerprint driver installers released with these HP platforms do not install a required fingerprint GUI DLL file: • HP Elite x2 1012 G2 • HP EliteBook x360 1030 G2 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 of the Synaptics VFS7552 WBF Touch Fingerprint Sensor Driver installer.
DE10285	When using the VPN Login option, the Protected PIN factor does not work with Cisco AnyConnect version 4.3.05017. During login, the keypad fails to display. In addition, after this failure occurs, the Protected PIN factor will also stop working for OS Login (until you log out and log back in to the PC). This issue was fixed from Intel ME Software 11.7.0.1010 and higher.
DE10214	When using an external monitor, depending on the resolution settings, the Protected PIN keypad is sometimes not displayed in the correct position. This makes it impossible to enter the PIN and log in. This issue was fixed from Intel ME Software 11.7.0.1010 and higher.

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

ID	Description
DE10132	Sometimes, when using Intel Protected Transaction Display, the entire screen is blacked out for up to 60 seconds. This can occur during enrollment of Protected PIN or when using OS Login (if Protected PIN is used for authentication).
	This issue only occurs with certain versions of the Intel Graphics driver (from version 21.20.16.4534 to version 21.20.16.4542). The issue was fixed from version 21.20.16.4550 and higher.

5 Known Issues

This table describes the current known issues with Intel Authenticate.

ID	Description	Solution / Workaround
DE12359	During installation, if a smart card reader from another application already exists in the first slot in Device Manager it is replaced by the "Intel IPT Reader".	If you need to use the smart card reader from the other application, re-install it after installing Intel Authenticate.
DE12341	In rare cases, after upgrade, Intel Authenticate might stop working and the Factor Management application displays a message: "No Factors To Manage".	Set the policy again
DE12267	When authenticating using the "Soft" fingerprint factor, the fingerprint GUI is displayed but does not respond when the user places their finger on the sensor. (This issue does NOT occur when using the "Soft" fingerprint factor for OS Login.)	This occurs because the fingerprint GUI is opened without active focus. Click the fingerprint GUI to give the GUI focus and then place your finger on the fingerprint sensor.
DE11858	On some Android phone models, Bluetooth Proximity can sometimes stop working because the phone has closed the Intel Authenticate app service. This issue has been seen on the "OnePlus* 3" and "LG* G3" phone models.	On the phone, open the Intel Authenticate app and bring it to the foreground. If this does not fix the issue, then restart the phone (and make sure that the Intel Authenticate app has restarted).
DE11548	In the ePO Console running "Queries & Reports" on the ePO database will return incorrect or invalid data about the client platforms. This is because some database fields are either not updated, or updated with invalid values. The affected fields include "Attempt count", "Last Intel Authenticate", and "User Type".	None
DE11500	When using Microsoft VPN, authentication of the VPN Login factors only starts approximately 20 seconds clicking the button to connect to VPN. This causes a delay in the time it takes to authenticate and log in to the VPN.	None
DE11492	On rare occasions, during OS Login the Protected PIN keypad numbers are not displayed.	Click **Cancel** and try to log in again.

ID	Description	Solution / Workaround
DE11432	In certain conditions, the Factor Management application shows the Fingerprint factor as not supported. This can occur if all these conditions are true: 1. The platform has a Protected Fingerprint reader. 2. Intel Authenticate was installed before the correct fingerprint driver was installed. 3. The policy set on the platform contains the Protected Fingerprint factor. 4. The correct fingerprint driver was then installed (this adds required DLLs and registry keys).	Reset Intel Authenticate and then set the policy again.
DE11364	Sometimes, an additional login screen is displayed before the Intel Authenticate login screen is displayed. Usually it disappears on its own and login continues. But sometimes it prevents the "One Click" login (until you click the link). 	If the screen does not close, click the link or press Enter to log in.
DE11165	OS Login takes longer than expected if Bluetooth is turned off on the phone.	None
DE10989 DE10473	In certain conditions, OS Login takes longer than expected to display the next factor after the first factor fails. This can occur if the first factor is Face Recognition or Fingerprint and the user did not complete authentication before the Windows curtain falls. After pressing Enter to raise the curtain, the next factor takes longer than usual to display.	Wait for approximately a minute and then try to login again

ID	Description	Solution / Workaround
DE10878	Sometimes, when enrolling an unpaired phone, after pairing completes the enrollment fails before the enrollment code is even displayed on the computer.	Start enrollment again.
DE10877	Sometimes, when enrolling an unpaired phone, the pairing step fails to pair the phone with the computer.	Start enrollment again. If the pairing step continues to fail, try pairing the phone via Windows first (as described in the enrollment guide.)
DE10692	If a new VPN connection starts before you are logged in, VPN Login will fail and the default username and password screen is shown. Cisco AnyConnect | ✕ Please enter your username and password. Username: | Password: OK Cancel	Click **Cancel** in this window. Then make sure that the correct VPN connection option defined for Intel Authenticate is selected, and log in to VPN using Intel Authenticate.
DE10688	When switching users, and then returning to the first user, the password field is not displayed (on the "other options" login screen).	Go back to the other user and then re-select the first user to refresh the display.
DE10190	On Windows 7, during login using the Protected PIN factor, a black screen is sometimes displayed for a few seconds just before the PIN keypad is displayed.	Ignore the black screen.
DE8926	A power failure during data storage might return system errors and block the ability to log in with Intel Authenticate. This can also occur if the computer suddenly shuts down because the computer battery has reached 0%.	Reset Intel Authenticate and set the policy again.

ID	Description	Solution / Workaround
DE8873 DE8872	In some cases the status of the mobile app and the Factor Manager application are not immediately in sync. This can lead to issues and errors if the user proceeds with further actions before both devices are in sync. For example, a PIN mismatch error on the mobile device is not yet registered on the Factor Manager application yet the user attempts to enter another PIN.	Ensure that an action on one side is matched by an action on the other side and that both applications are on the same base page, and not still on the previous action, when performing an action. For example, unenrolling on user platform side must be matched by clearing enrollment data on the mobile side. If an unenroll fails on one side, bring both applications back to the start for an enrollment action.
DE8696	When making changes to a policy, the new settings will not overwrite existing factor settings. For example, changing the PIN requirement from 4 digits to 6 digits will not required enrolled users to update their PIN.	To change the Protected Pin criteria, create and apply a new policy with the new criteria and then enroll the Protected Pin with the new criteria.