Intel® Authenticate

Release Notes

Version 3.7

Document Release Date: 6 December, 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 **1**

2 Changes and New Features **1**

2.1 Support for Windows* 10 Version 1809 1
2.2 New Physical Smartcard Factor 1
2.3 New OS Login GUI 2
2.4 Support for Interactive Logon Settings 3
2.5 New Event Viewer IDs 3
2.6 Changes to the Factor Management Application 6
2.7 Support for New Phone Operating System Versions 7
2.8 Check Tool is now Installed 7
2.9 Check Tool Results Added to the Support Tool Logs 7
2.10 New Reset Factors Option in SCCM 7
2.11 Support for Windows 10 High Contrast Mode 8
2.12 Support for New Languages 8
2.13 Support for Microsoft* Azure 8
2.14 New Attestation Utility 8

3 Known Limitations **9**

4 Resolved Issues **11**

5 Known Issues **13**

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

1 Introduction

This document describes new features and changes made in version 3.7 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 3.7.

2.1 Support for Windows* 10 Version 1809

Intel Authenticate version 3.7 adds support for Windows 10 version 1809 (from build 10.0.17763.55).

2.2 New Physical Smartcard Factor

On platforms with a supported Smartcard reader, you can now define a Physical Smartcard factor.

The Physical Smartcard factor has these specific prerequisites:

- Windows 10.0.14933.222 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

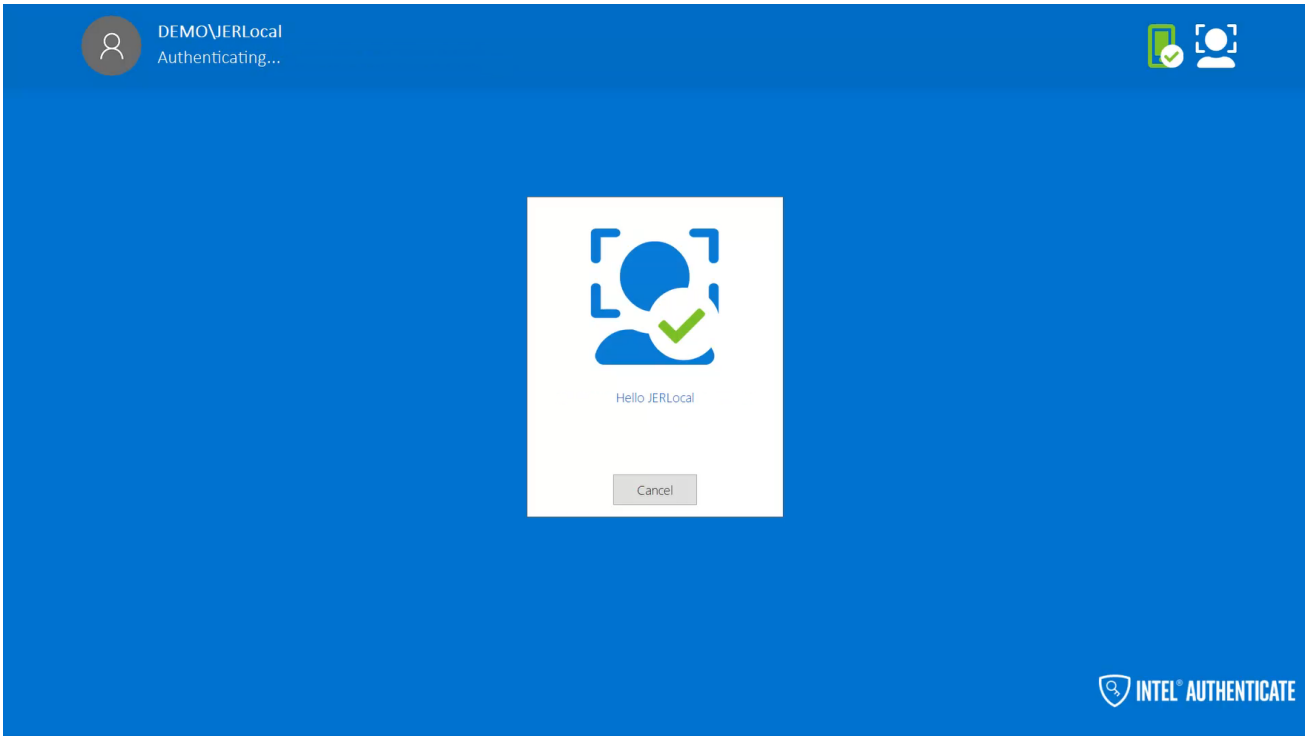
When defining the Physical Smartcard factor in the Intel Authenticate policy, you can define these settings:

- **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 the Smartcard PIN 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 OIDs that are configured in the Smartcard. When this field contains OIDs, only Smartcards that have at least one of these OIDs configured are accepted by Intel Authenticate.
- **Reader Name (partial)** – The name of the Smartcard as it appears in "Device Manager > Smart card readers". When this field contains text, only Smartcards 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.

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

2.3 New OS Login GUI

The Intel Authenticate login screen has been improved to give the user a better visual indication of the login process. In the top right corner, an icon is shown for each factor that needs to be authenticated (according to the policy settings).



These are the meanings of the colors and symbols of the factor icons:

- The icon is white – Authentication of the factor is either in progress or will start soon
- The icon is green and has a green check mark – Authentication of the factor has succeeded
- The icon is white with a red exclamation mark – Authentication of the factor has failed

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

2.4 Support for Interactive Logon Settings

In previous versions, for the OS Login option to work, Intel Authenticate required the user details to be displayed in the login screen. Therefore, any options that hid or prevented the user details from being displayed could not be enabled. This restriction has now been lifted. This means that these options in Group Policy Settings are now supported with whichever value you want to configure.

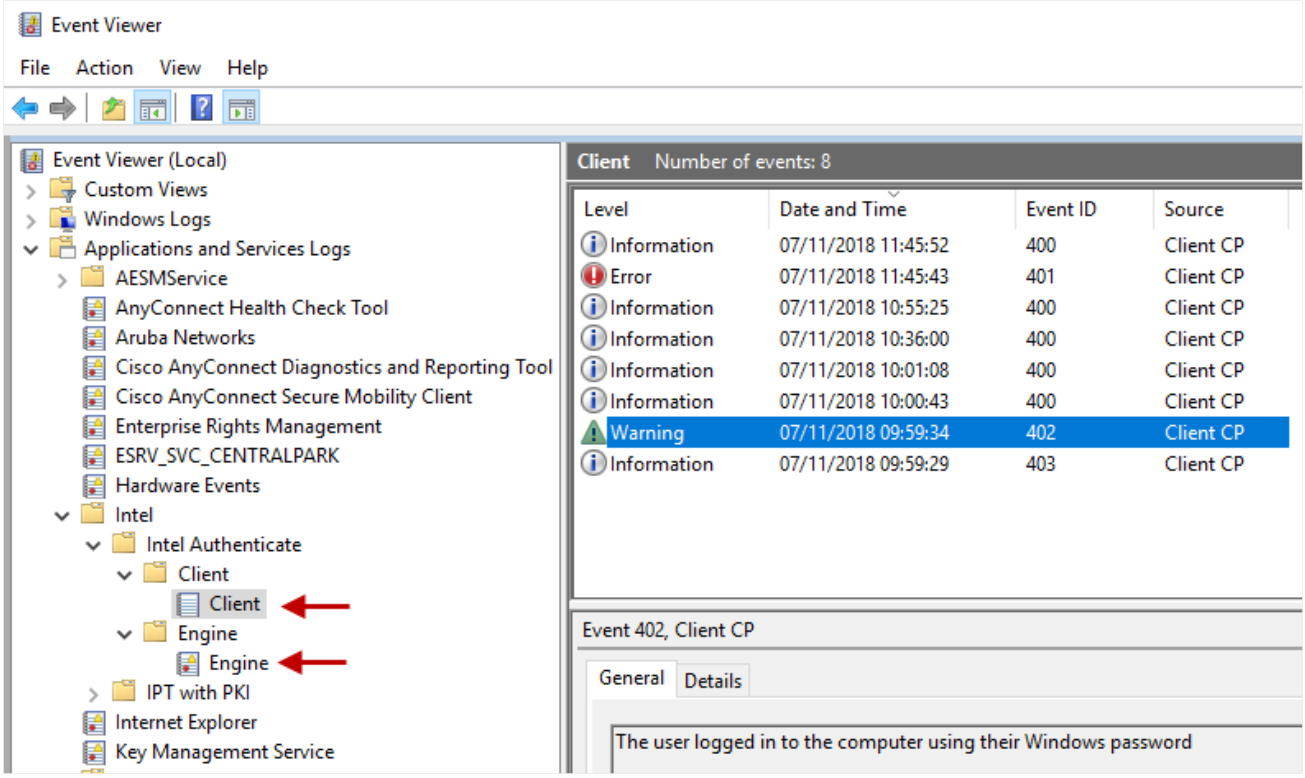
Name in Policy Editor	Registry Key
Interactive logon: Display user information when the session is locked	`DontDisplayLockedUserId`
Interactive logon: Do not require CTRL+ALT+DEL	`DisableCAD`
Interactive logon: Don't display last signed-in	`DontDisplayLastUserName`
Interactive logon: Don't display username at sign-in	`DontDisplayUsername`

For more information about these options, refer to the Microsoft* documentation.

2.5 New Event Viewer IDs

Intel Authenticate now 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



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

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
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

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

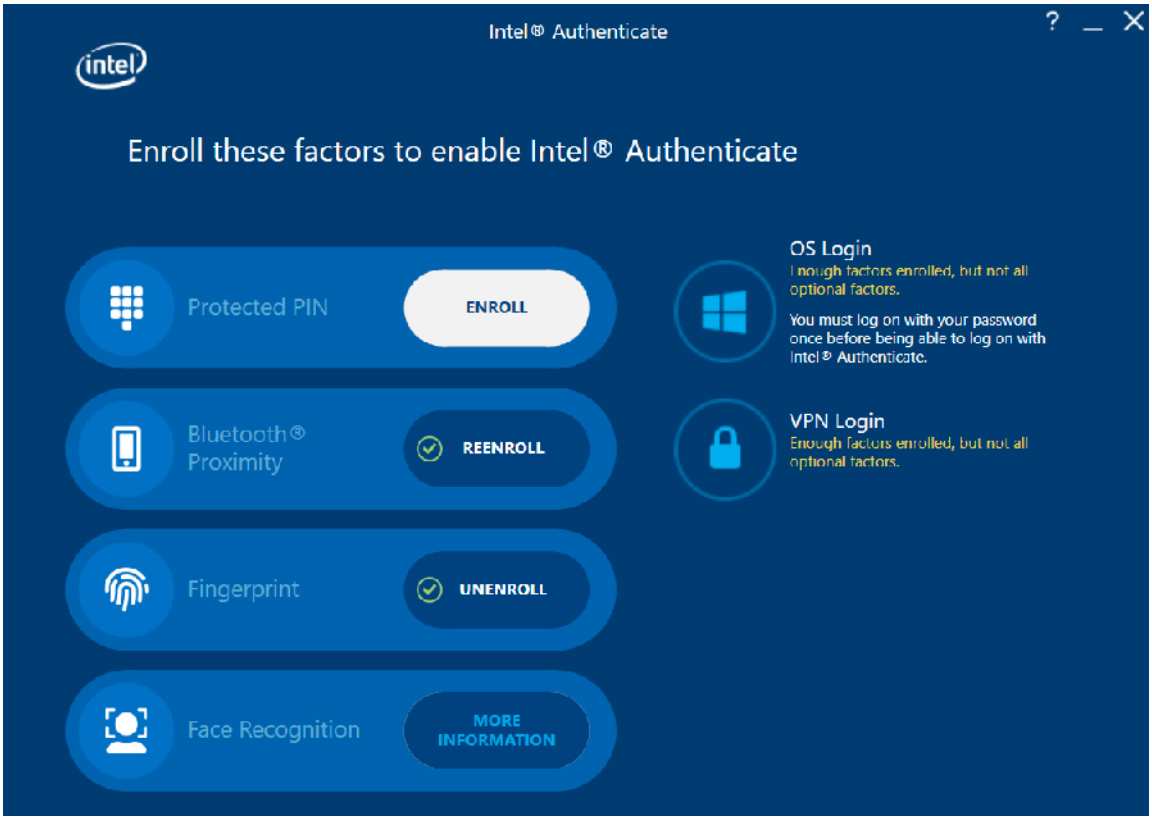
Event ID	Description	Event Type
161	Bluetooth Proximity factor unenrolled successfully (Protected)	Informational
162	Protected PIN factor unenrolled successfully	Informational
163	Face Recognition factor unenrolled successfully	Informational
164	Fingerprint factor unenrolled successfully (Soft)	Informational
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
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

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

Event ID	Description	Event Type
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

2.6 Changes to the Factor Management Application

Some small changes were made to the Factor Management application.



- When a factor is not enrolled, the color of the button is now white. After a factor is enrolled, a green check box is shown and the button color changes to blue.
- The display order of the factors is now dynamic. After a user has enrolled a factor, that factor is moved down in the list of factors so that the non enrolled factors appear at the top of the list. Any factors that the user cannot enroll (and have a status of "More Information") are displayed at the bottom of the list.
- After the user has enrolled their factors, the introductory pages are no longer displayed. When the user opens the application it will automatically open on the factor enrollment page.

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

2.7 Support for New Phone Operating System Versions

Intel Authenticate version 3.7 adds support for these phone operating system versions:

- iOS version 12.0 and 12.1
- Android version 9.0

2.8 Check Tool is now Installed

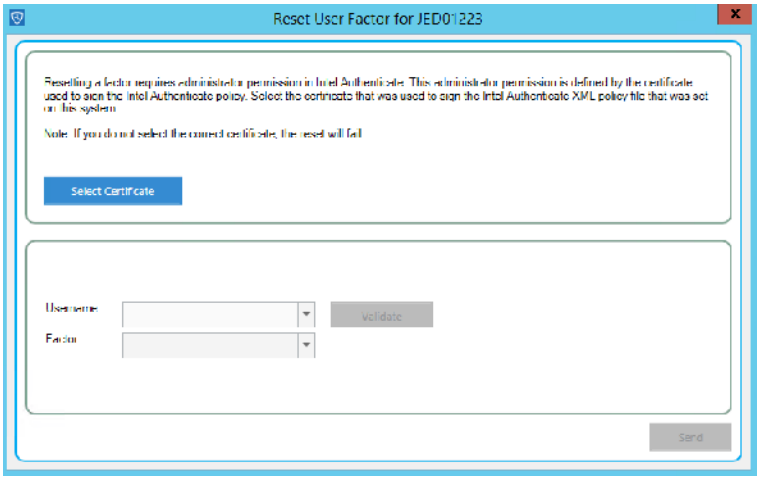
During installation of Intel Authenticate, the Check tool is now installed in this location on the client platforms: `C:\ProgramData\Intel\Intel Authenticate\Engine\CheckTool`

2.9 Check Tool Results Added to the Support Tool Logs

The Support Tool `/CollectLogs` flag now also automatically runs the Check tool and collects the results into the log zip file. The results are located in a file named `CheckToolResults.log`. This file includes the results of the Prerequisites Test (`/P`) and the Factors Test (`/F /V`). The `CheckToolResults.log` file can help you identify if a configuration change or problem with one of the factors is causing the issue that you are troubleshooting.

2.10 New Reset Factors Option in SCCM

Version 3.7 of the Intel® Authenticate Add-on for Microsoft* SCCM adds a new "Intel Authenticate Recovery" option to the SCCM console menu. This option enables you to remotely reset individual factor enrollments when the user cannot fix the problem themselves. To use this option, right-click the platform where you want to reset the factor and select **Intel Authenticate Recovery** > **Reset Factor**.



For more information, refer to the "Resetting Factors" section of the SCCM integration guide.

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

2.11 Support for Windows 10 High Contrast Mode

Intel Authenticate now supports Windows 10 High Contrast Mode.

2.12 Support for New Languages

Intel Authenticate has been translated into two additional languages:

- Chinese Simplified
- Brazilian Portuguese

2.13 Support for Microsoft* Azure

When using Microsoft Azure and supporting utilities, you can setup and configure "Hybrid Environments". In a Hybrid Environment, users are able to log in to Azure cloud-based functionality based on their on-premises Active Directory login. We have ensured that the OS Login feature of Intel Authenticate (password-based and certificate-based) does not adversely affect the expected login functionality in these Hybrid Environments.

Note:

Hybrid Environments are enabled via Microsoft utilities and system functionality. The setting up and configuration of the Hybrid Environment is not related to Intel Authenticate and must be done independently by the IT administrator.

2.14 New Attestation Utility

The SCCM and GPO integration packages now include a new "Attestation Utility". You can use this utility to verify that a platform was not compromised before initial configuration of Intel Authenticate. For more information, refer to the `Intel(R)_Authenticate_Attestation.pdf` in the `Tools` > `Attestation` folder.

Note:

The Attestation Utility is not supported when deployment is performed via McAfee* ePO.

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

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.	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)".
Pairing of multiple Bluetooth devices with the computer can affect performance of the Bluetooth Proximity factor. This is because the operating system requires time to contact each paired device. This can cause a delay if the number of paired devices is large, or if some of the devices are not in close proximity. This delay can cause authentication using the Bluetooth Proximity factor to take longer than expected or to fail. **Note:** On computers with multiple users this issue can occur more frequently because each user could potentially have several paired devices.	It is highly recommended to make sure that only required Bluetooth devices are paired with the computer. Remove all paired devices that are no longer being used.
When using Android Phones, installing and using multiple instances of the Intel Authenticate app on the same phone is not supported. This means that you must not use the Android "Dual Apps" feature, or any software that enables multiple instances of the same app.	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 (for example, Windows Hello). 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
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
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
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
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.

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

4 Resolved Issues

This table describes the issues which were resolved in version 3.7 of Intel Authenticate

ID	Description
DE12341	In rare cases, after upgrade, Intel Authenticate stopped working and the Factor Management application displayed a message: "No Factors To Manage".
DE11858	On some Android phone models, Bluetooth Proximity sometimes stopped working because the phone closed the Intel Authenticate app service. This issue was seen on the "OnePlus* 3" and "LG* G3" phone models. This issue was fixed in the latest version of the Intel Authenticate mobile app.

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

ID	Description
DE12918	On Windows 7, when using some versions of the Intel ME Software, the JHI service fails to initialize. This causes test #8 of the Check Tool Prerequisites Test to fail, and also blocks installation. This issue occurred only from Intel ME Software version 1824.12.0.1140. The issue has been fixed in Intel ME Software version 1847.12.0.1183 and higher.
DE12585	After resuming from sleep or hibernate, authentication could fail because the Intel DAL service failed to initialize due to a bug in the Intel ME Firmware. This failure only occurred when using Intel ME Software versions higher than 1752.12.0.1089. This issue was fixed in Intel ME Firmware version 11.8.60.3555 and higher.
DE12488	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)
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.

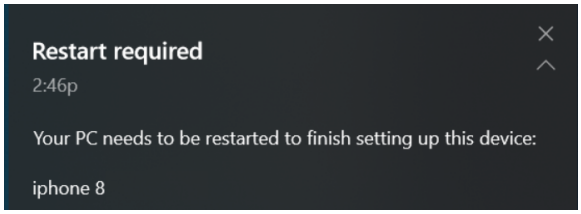
* Other names and brands may be claimed as the property of others

ID	Description
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.
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.

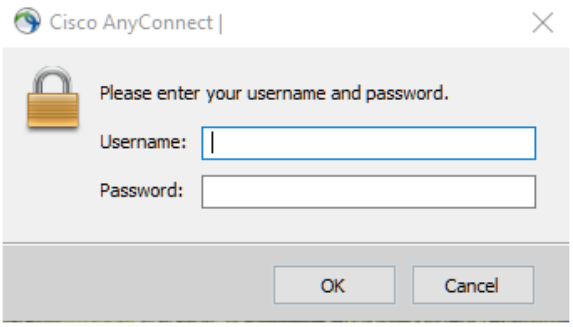
* Other names and brands may be claimed as the property of others

5 Known Issues

This table describes the current known issues with Intel Authenticate.

ID	Description	Solution / Workaround
DE12799 DE12749 DE12600	On Windows 10 versions 1803 and 1809, enrollment of an iPhone can sometimes fail. This issue only affects the "Protected" security level of the Bluetooth Proximity factor. **Note:** The occurrence of iPhone enrollment failures on versions 1803 and 1809 is higher than earlier versions of Windows 10. The cause of these failures is because the BLE stack on these versions is not responding as expected. These issues have been reported to Microsoft.	If repeated attempts to enroll the iPhone fail: 1. On the computer, manually unpair all instances of the phone. 2. On the iPhone, open Bluetooth Settings and "forget" the computer. (Make sure that you close the Bluetooth Settings page before continuing.) 3. Restart the computer.
DE12789	When using iPhones, the Bluetooth Proximity factor can sometimes stop working for no apparent reason. This issue only affects the "Protected" security level of the Bluetooth Proximity factor. **Note:** The cause of this failure is that the BLE stack is not responding as expected. This issue has been reported to Microsoft.	Try restarting the computer. If the problem continues, try running the Bluetooth troubleshooter (located in `Settings` > `Troubleshoot` > `Bluetooth`).
DE12407	When using the Bluetooth Proximity factor with multiple users, a Windows notification is sometimes shown stating that a restart is required to finish setting up the users phone.  	Ignore the message.
DE11492	On rare occasions, during OS Login the Protected PIN keypad numbers are not displayed.	Click **Cancel** and try to log in again.

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

ID	Description	Solution / Workaround
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.
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. 	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 or hard shutdown 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.
DE8696	When making changes to a policy, the new Protected PIN 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.

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