INTEL® ONLINE CONNECT

RELEASE NOTES

V1.4.35.0

Legal

Table of Contents

1 Terminology

Term	Description
API	Application Programming Interface
CUP	China Union Pay
IOC	Intel(R) Online Connect
FIDO	Fast Identity Online
IOCA	Intel(R) Online Connect Access
UAF	Universal Authenticator Framework
U2F	Universal 2nd Factor

2 Intel(R) Online Connect 1.4.35.0 – May 28th 2018

This release has undergone Intel's KBL-R BKC validation.

It has also been tested on the following additional systems with Windows 10 RS3:

- Lenovo Yoga 910 (Consumer)
- Lenovo Thinkpad (Consumer)
- Intel KBL, KBL-R CFL Test Platforms.

2.1 Updates

- Updated with RS4 WHQL certified HID and Network filter drivers. The IOC stack continues to work with both RS3 and RS4.
- The Intel® online Connect is updated with to use latest SGX libraries. The latest version for SGX is 1.9
- Extension INF supporting the hardware ID's for CFL and ICL.
- Update for IOC to work with all versions of Mozilla firefox.
- Fix for Conformance related errors.
- Update for iCLS INF based installation.
- CUP flow update to work with both 11.6 and 11.8 firmware.

2.2 Known Issues

- IOC stack will not be executed immediately after installation. It might take some time (in-consistent). Installer will be queued and executed later as mentioned in MSDN site.
- If same version has to be installed in the same system, the version key from HKLM\Software\Microsoft\Windows\CurrentVersion\Device Setup\Device Software\UpgradeISA_IOC\Version is to be deleted.

3 Intel(R) Online Connect 1.4.22.0 – Mar 7th 2018

This release has undergone Intel's KBL-R BKC validation.

It has also been tested on the following additional systems with Windows 10 RS3:

- Lenovo Yoga 910 (Consumer)
- Lenovo Thinkpad (Consumer)
- Intel KBL and KBL-R Test Platforms.

3.1 Updates

- UWD compliance - extension and component INF based installation.
- Extension INF associated with Intel ME IDs
- Included Windows 10 RS3 certified Intel(R) Online Connect Access driver
- Included Windows 10 RS3 certified U2F HID driver
- HID and Component ID's are updated as per Intel standard.
- The Intel® online Connect is updated with to use latest SGX libraries. The latest version for SGX is 1.9
- Fix for the NDIS filter driver causing blue screen. In certain situations when NULL buffers are passed in, the driver crashes, and a blue screen is observed. This network filter driver is included within the Intel® Online Connect installer. No loss of sensitive data is expected due to this issue.

3.2 Known Issues

- IOC stack will not be executed immediately after installation. It might take some time (in-consistent). Installer will be queued and executed later as mentioned in MSDN site.
- If same version has to be installed in the same system, the version key from HKLM\Software\Microsoft\Windows\CurrentVersion\Device Setup\Device Software\SetupIOC\Version is to be deleted.
- FireFox browser issue: Intel(R) Online Connect Access work with Firefox (v57) and below version only.

4 Intel(R) Online Connect 1.4.10.0 – Nov 2nd 2017

This release has undergone Intel's KBL-R BKC validation.

It has also been tested on the following additional systems:

- Lenovo Yoga 910 (Consumer)
- Lenovo Thinkpad (Consumer)
- Intel KBL and KBL-R Test Platforms.

4.1 Updates

- UWD compliance - extension and component INF based installation.
- Extension INF associated with Intel ME IDs
- Included Windows 10 RS3 certified Intel(R) Online Connect Access driver
- Included Windows 10 RS3 certified U2F HID driver
- Fixed an issue for Silent Authentication user-consent toaster form on RS3 with modification to desktop application.
- Fixed an issue where the Intel(R) Online Connect U2F applet for handle RTC reset in coinless design.

4.2 Known Issues

- SetupIOC.exe will not be executed immediately after installation. It might take time (in-consistent) depend on system. - Installer will be queued and execute later.

5 Intel(R) Online Connect 1.3.6.0 – June 21st 2017

This release has undergone Intel's KBL-R BKC validation and is also released with KBL-R BKC releases.

It has also been tested on the following additional systems:

- Lenovo Yoga 910 (Consumer)
- Lenovo Thinkpad (Consumer)
- Dell Precision 3520 (Consumer)
- Lenovo Yoga 360 (Enterprise)
- Intel KBL and KBL-R Test Platforms.

5.1 Updates

- Included Windows 10 RS2 certified Intel(R) Online Connect Access driver
- Included Windows 10 RS2 certified U2F HID driver

- Fixed an issue where the Intel(R) Online Connect authenticator applet's cached version remained in the CSME DAL service's cache after Intel(R) Online Connect uninstallation.

5.2 Known Issues

- The FIDO fingerprint authenticator *does not* have a built-in user interface. The fingerprint UI/UX is considered to be the Relying Party's responsibility. RP's will need to present the fingerprint UI to the user from the browser space at point of FIDO transaction.
- Very rarely, the system may disconnect from a WiFi network after installation of IOC. A reboot fixes the system. This is not expected to be an issue when IOC is pre-installed by OEMs.
- Very rarely, user may need to either log out and log back in, or, reboot the system after creation of a new Windows user account in order to use the IOC FIDO UAF authenticators from browsers. This will be fixed in a future release.
- Running the IOC installer with the 'Repair' option may leave the IOC service stopped after completion of the repair operation. A reboot will restart the IOC service. This will be fixed in a future release.
- There may be a very small number of relying parties (RPs) that may currently not process the registration response from IOC U2F successfully. This is likely due to the fact that IOC U2F uses a 3096 bit RSA key to attest the registration response; U2F RPs must be capable of handling this attestation

6 Intel(R) Online Connect 1.3.1.0 – June 1st 2017

6.1 Updates

- This version of Intel(R) Online Connect is tested on enterprise version of Windows 10 RS2 and with enterprise ME FW (AMT enabled).
- Tested with Intel Authenticate v for coexistence – Client v2.1.0.75, Engine v2.1.0.200.
- Resolved an issue with concurrent invocation of the UAF processUafOperation() from multiple browser tabs where the 2nd invocation can sometimes cancel the first invocation. With this fix only one processUafOperation invocation is allowed until completion of that operation.
- Resolved an issue with UAF notifyUafResults() API was not always processed correctly resulting in errors reported from server not removing invalid KeyIds. This has now been fixed.

6.2 Known Issues

- The FIDO fingerprint authenticator *does not* have a built-in user interface. The fingerprint UI/UX is considered to be the Relying Party's responsibility. RP's will need to present the fingerprint UI to the user from the browser space at point of FIDO transaction.
- Very rarely, the system may disconnect from a WiFi network after installation of IOC. A reboot fixes the system. This is not expected to be an issue when IOC is pre-installed by OEMs.

- Very rarely, user may need to either log out and log back in, or, reboot the system after creation of a new Windows user account in order to use the IOC FIDO UAF authenticators from browsers. This will be fixed in a future release.
- Running the IOC installer with the ‘Repair’ option may leave the IOC service stopped after completion of the repair operation. A reboot will restart the IOC service. This will be fixed in a future release.
- There may be a very small number of relying parties (RPs) that may currently not process the registration response from IOC U2F successfully. This is likely due to the fact that IOC U2F uses a 3096 bit RSA key to attest the registration response; U2F RPs must be capable of handling this attestation.

7 Intel(R) Online Connect 1.2.32.0 – May 11th 2017

7.1 Updates

- The Intel(R) Online Connect installer now supports additional flags to disable the UAF Silent Authenticator and built-in U2F Authenticator.
    - Pre-existing installer flags to enable China UnionPay support and disable FIDO altogether are still supported as is.
    - Default upgrade, as implemented by the Intel(R) Online Connect Software Asset Manager updater, will retain the feature set that was enabled during OEM/ODM pre-installation.
    - OEMs will have the means to update the feature set in deployed systems by deploying Intel(R) Online Connect through their own update mechanisms and executing the Intel(R) Online Connect installer with the appropriate flags.
- Updated the U2F authenticator to initialize irrespective of the version check command which some Relying Parties do not make. The authenticator now initializes on first invocation of any U2F command.
- Fixed a race condition issue where calling the UAF ProcessUafOperation JS API too quickly after the Discover API could result in an error. This issue is now resolved to remove any timing dependency on ProcessUafOperation with any other UAF API call.
- Updated the Intel(R) Online Connect Access self-signed SSL certificate to add a SubjectAltName field. Latest versions of Chrome (v58+) and Firefox (v53+) are requiring this field to accept SSL certs from web servers.

7.2 Known Issues

- The FIDO fingerprint authenticator *does not* have a built-in user interface. The fingerprint UI/UX is considered to be the Relying Party’s responsibility. RP’s will need to present the fingerprint UI to the user from the browser space at point of FIDO transaction.
- Very rarely, the system may disconnect from a WiFi network after installation of IOC. A reboot fixes the system. This is not expected to be an issue when IOC is pre-installed by OEMs.

- Very rarely, user may need to either log out and log back in, or, reboot the system after creation of a new Windows user account in order to use the IOC FIDO UAF authenticators from browsers. This will be fixed in a future release.
- Running the IOC installer with the ‘Repair’ option may leave the IOC service stopped after completion of the repair operation. A reboot will restart the IOC service. This will be fixed in a future release.
- There may be a very small number of relying parties (RPs) that may currently not process the registration response from IOC U2F successfully. This is likely due to the fact that IOC U2F uses a 3096 bit RSA key to attest the registration response; U2F RPs must be capable of handling this attestation.

8 Intel(R) Online Connect 1.2.23.0 – April 19th 2017

8.1 Updates

- Updated the licenses.txt file to add source code link for the Mozilla NSS component used in Intel(R) Online Connect Access. This is to fulfill a requirement of the Mozilla Public License NSS is distributed under.
- Updated the FIDO and Auth Assertion (CUP SecurePay) enclaves with an updated XML parser for better efficiency and security reasons.
- Updated the Auth Assertion enclave to no longer accept enclave-enclave communication from trusted (whitelisted) fingerprint enclaves that have the debug configuration enabled. Untrusted enclaves were anyway rejected.

8.2 Known Issues

- The FIDO fingerprint authenticator *does not* have a built-in user interface. The fingerprint UI/UX is considered to be the Relying Party’s responsibility. RP’s will need to present the fingerprint UI to the user from the browser space at point of FIDO transaction.
- Very rarely, the system may disconnect from a WiFi network after installation of IOC. A reboot fixes the system. This is not expected to be an issue when IOC is pre-installed by OEMs.
- Very rarely, user may need to either log out and log back in, or, reboot the system after creation of a new Windows user account in order to use the IOC FIDO UAF authenticators from browsers. This will be fixed in a future release.
- Running the IOC installer with the ‘Repair’ option may leave the IOC service stopped after completion of the repair operation. A reboot will restart the IOC service. This will be fixed in a future release.
- IOC U2F Test of User Presence check may sporadically result in a blank screen on current Windows 10 versions. If the display blankout happens the screen will repaint in a few seconds. This has been resolved in RS2.

- There may be a very small number of relying parties (RPs) that may currently not process the registration response from IOC U2F successfully. This is likely due to the fact that IOC U2F uses a 3096 bit RSA key to attest the registration response; U2F RPs must be capable of handling this attestation. This has been noticed with only 1 RP so far.

9 IOC 1.2.16.0 – Mar 24th 2017

9.1 Updates

- Built-in FIDO certified U2F Authenticator with Protected Transaction Display (PTD) used as the Test of User Presence. U2F authenticator is compliant with existing U2F Clients in Chrome and Opera browsers and is interoperable with FIDO certified U2F Relying Parties.
- The IOC FIDO Client now automatically cancels pending UAF Registrations and Authentication requests if the user locks the screen or logs out. This will release the fingerprint sensor if the user decides to do those actions while the authenticator is awaiting a fingerprint match response.
- Updated IOC-Access FIDO and SecurePay endpoint registration logic with a retry mechanism in case initial registration fails. This fixes the issue where in rare occasions the IOC endpoints were not available after a system boot.

9.2 Known Issues

- The FIDO fingerprint authenticator *does not* have a built-in user interface. The fingerprint UI/UX is considered to be the Relying Party's responsibility. RP's will need to present the fingerprint UI to the user from the browser space at point of FIDO transaction.
- Very rarely, the system may disconnect from a WiFi network after installation of IOC. A reboot fixes the system. This is not expected to be an issue when IOC is pre-installed by OEMs.
- Very rarely, user may need to either log out and log back in, or, reboot the system after creation of a new Windows user account in order to use the IOC FIDO UAF authenticators from browsers. This will be fixed in a future release.
- Running the IOC installer with the 'Repair' option may leave the IOC service stopped after completion of the repair operation. A reboot will restart the IOC service. This will be fixed in a future release.
- IOC U2F Test of User Presence check may sporadically result in a blank screen on current Windows 10 versions. If the display blankout happens the screen will repaint in a few seconds. This has been resolved in RS2.
- There may be a very small number of relying parties (RPs) that may currently not process the registration response from IOC U2F successfully. This is likely due to the fact that IOC U2F uses a 3096 bit RSA key to attest the registration response; U2F RPs must be capable of handling this attestation. This has been noticed with only 1 RP so far.

10IOC 1.1.18.0 – Feb 9th 2017

10.1 Updates

- Updated IOC installer icons to fix resolution issue with the miniaturized icons.
- Lowered IOC startup time to within 2 seconds of user login from 5 seconds. Lowers time to CPU idle state improving ADK results. Also makes IOC available quicker to the user.
- Fixed installer rollback issues in case of sub-component failure in installer bundle. Fixes rollback instability issues.
- Added support to SetpupIoc.exe installer for removing feature specific binaries for feature sets that are disabled with IOC installer flags.
- Fixed a co-existence issue between the FIDO and SecurePay (China UnionPay) Authenticators where registering with a FIDO authenticator could have prevented use of the SecurePay Authenticators. Both FIDO and SecurePay authenticators are now supported together on all IOC compliant platforms.
- Updated SecurePay authenticator to always return the hashed SID of the current logged in user instead of the matched user. Also updated SecurePay GetDeviceInfo() to return the hashed SID of logged-on user. This fulfils the CUP change request for SecurePay API changes.
- Fixed an issue in the IOC FIDO Client where a corrupt database would prevent future registrations. The FIDO Client can now recover from corrupt database scenarios by initializing a new one.
- Cleaned up extraneous logging messages.

10.2 Known Issues

- The FIDO fingerprint authenticator *does not* have a built-in user interface. It is possible to enable the Windows Hello UI using instructions in the install guide but that is for demo purposes only. For this release the fingerprint UI/UX is considered to be the Relying Party's responsibility. RP's will need to present the fingerprint UI to the user from the browser space at point of FIDO transaction.
- Very rarely, the FIDO browser endpoints may not get registered after installing IOC, resulting in the IOC javascript APIs not being able to discover the IOC FIDO authenticators. A reboot fixes this issue. This issue is seen following installation only and is not expected to affect regular reboots after IOC has been installed.

11IOC 1.1.9.0 – Dec 23rd 2016

11.1 Updates

- IOC FIDO client and authenticators updated to meet 100% UAF DOM API conformance test suite pass rate. This includes Authenticators 8086#5016 (SGX Fingerprint), 8086#5006 (SGX Silent Auth) and 8086#5002 (CSME Silent Auth).

- IOC FIDO Client and authenticators have passed FIDO interoperability testing. This includes the same 3 authenticators listed above.
- IOC UAF Javascript DOM APIs updated to meet UAF DOM API requirements as specified in the FIDO UAF Application API and Transport Binding Specification. The updated javascript file is called IocFidoUaf.js.
  The legacy IntelClientManager.js is still supported and will be deprecated in future releases.
- Updated to IOC Updater 3.4.2216 with Python 2.7.12, curl 7.51.0 and openssl 1.0.2h.This release also removed the module that referenced the asyncore.pyc module associated with CVE-20-10-3492.
- Updated to IOC-Access 1.9.11.162 to resolve a battery life issue that was being caused by unnecessary modification of the system time resolution. The system timer is no longer modified.
- Open source components used by IOC-Access have been updated to latest known stable versions to resolve known CVEs.
- All executable binaries (dll-s, exe-s) in the Intel® Online Connect install folders, including NotificationsExtensions.Win10.dll, FidoEnclave64.dll and iha64.dll, are code signed by Intel.
- Unnecessary debug logging have been removed from the release build.
- setup.cmd script has been updated to consolidate all log files into one overall install log file. See installation guide for details.
- A version of the SetupIoc.exe installer is now available that *does not* add an entry in the Control Panel ‘Programs and Features’ list. A version of the installer that does add the Control Panel entry is also included in the release package.
- IOC logo in install GUI has been updated to meet high resolution display requirements.
- Updated IOC installer to allow installation flags for feature specific installs. By default – no install flags - only the FIDO protocol is enabled.
- Added licence.txt file for all open source components used in the product.

11.2 Known Issues

- The FIDO fingerprint authenticator *does not* have a built-in user interface. It is possible to enable the Windows Hello UI using instructions in the install guide but that is for demo purposes only. For this release the fingerprint UI/UX is considered to be the Relying Party’s responsibility. RP’s will need to present the fingerprint UI to the user from the browser space at point of FIDO transaction.
- This release is provisioning against the Intel pre-production provisioning server that provisions a pre-production FIDO Attestation Private Key (APK). Will update to provision with the Intel production provisioning server with the PV release. Metadata for pre-prod and prod remain the same with the exception of the root certificate public key.
- Upgrading to a higher version of IOC from this version may require a system reboot.
  A future upgrade version of IOC may be able to work around this issue.

- On rare occasions the FIDO browser endpoints may not get registered resulting in the IOC javascript APIs not being able to discover the IOC FIDO authenticators. A reboot will fix this issue. This will be fixed in the PV release.

12 IOC 1.1.4.0 – Nov 4th 2016

12.1 Updates

- Added full SGX based fingerprint authenticator support
- Added EULA prompted displayed during software first usage
- The Silent Authenticator User Consent notification is hooked to the FIDO Client. Registration is only allowed to proceed after the user clicks/taps on 'Accept'. The timeout is 30 seconds.

12.2 Known Issues:

- Provisioning of applet and SGX token will occasionally fail. Issue can be fixed by restarting IOC service.
- Deregistration does not work with multiple authenticators.

13 IOC 1.1.1.0 – October 7th 2016

13.1 Updates

- Added initial support for SGX based Silent Authenticator - AAID 8086#5006
- Added support for SGX based Fingerprint Authenticator - AAID 8086#5016
- Added support for User Consent notification during Silent Authenticator registration flow.
- Fixed issue with notifyUafResult deregistering keyids for positive status codes.
- Added support for ignoring unknown extensions.

13.2 Known Issues

- On some systems it is possible that when the 3rd and 4th windows user attempts to register using enrolled fingerprint, the fingerprint authentication may fail. This seems to be a Windows or Fingerprint driver related issue.
- The Silent Authenticator User Consent notification is only for display purposes in this release. The accept notification is not hooked to the FIDO Client. The FIDO Client imposes a 5 second wait period during a Silent Authenticator registration flow before proceeding with the FIDO signing operation. This will be updated in a future release to allow the registratio to proceed only after the user clicks/taps on 'Accept'. The timeout will be 30 seconds.
- FIDO Fingerprint registration will fail under the following circumstances:
    - if no fingerprint reader is attached
    - if no user is enrolled or
    - if fingerprint did not match

Open the Windows 10 Hello settings page and enroll a fingerprint to enable the fingerprint authenticator.

14IOC1.0.14.0 – Dec 14th 2016

14.1 Updates

- Added setup.cmd that will install IOC with CUP only option and delete FIDO related binaries
- Update payment applet so fingerprint match result can be returned normally after system power loss and system does not have CMOS battery

14.2 Known issue

- Rarely after reboot browser communication to the underlying middleware stack fails (1 out of 50 times on specific system tested)

15IOC 10.13.0 – Dec 5th 2016

15.1 Updates

- IOC installer that supports installer flag to install IOC in a CUP-only options.
- Updated IOC services to select specific feature sets: FIDO, FIDO/CUP or CUP-only as desired by OEM.
- Update ITA to regenerate web server certificate 3 months before expiration for uninterrupted IOC access from browser.
- Fixed an ITA issue to prevent IOC browser access from being disabled when IOC code signing certificate expires.

15.2 Known issues

- Failed to get fingerprint match results after system power loss due to CMOS battery issue
- BSOD after IOC is installed and get deviceinfo – this is likely related to the BSOD we have seen with the FPC driver version 3.21.1.0; further integration testing with FPC’s latest driver and production signed enclave will verify if this issue still exists
- Rarely after reboot browser communication to the underlying middleware stack fails (1 out of 50 times)

16IOC 1.0.12.0 – November 14th 2016

16.1 Updates

- Remove logic that starting service requires system reboot after installation.
- Reduced IOC service start time to 30 seconds from 90 seconds.

- Fixed issue -- IOC Service throws null reference exception during shutdown
- Fixed an issue in ITA that caused battery life reduction due to changing system timer resolution. System timer resolution is now maintained in default value.
- Updated IOCUpdater to use the latest version of openssl and python.

17IOC 1.0.9.0 – October 4th 2016

17.1 Updates

IOC service is now pointing to IOC production server.

18 IOC 1.0.6.0 – October 3rd 2016

18.1 Updates

Fixed an issue with installing VS 2015 redist package with IOC installer. It now handles scenarios when VS2015 redist package is installed on the system

19 IOC 1.0.3.0 – September 27th 2016

This is the Release Candidate for Intel(R) Online Connect (IOC).
This package is not for production deployment.
Please treat it as an early release version of the production package that may be used for early validation and security checks.

Please refer to the IOC_1.0_OEM_Installation_Guide pdf for instructions on installing and enabling IOC.

19.1 Updates

1. Enabled China Union Pay compliant secure payments protocol support.
   This version is now fully compliant with the China Union Pay production backend.
2. Enabled support to display EULA window to user at first registration with China Union Pay or FIDO Relying Party. EULA is only displayed once and once user accepts stays hidden.
3. Added support for Intel(R) Online Connect auto updater. Updater silently updates IOC every 15 days if an update is available in the Intel managed update backend server.
4. FIDO – fixed issue with notifyUafResult deregistering for positive status codes.

20 IOC 1.0.2.0 – August 22nd 2016

20.1 Updates

1) Includes signed Silent Authenticator applet. This eliminates the need to use the DAL emulator on SkyLake (SKL) and KabyLake (KBL) systems.
   If the DAL SDK is installed on the SKL or KBL test/dev system it should be uninstalled when this version of IOC is installed.
2) Fixed an issue in the FIDO Client where it did not omit default HTTPS port in facetID generation. This allows the Silent Authenticator's resgistration/authentication responses to work correctly with a NNL FIDO server.

20.2 Known Issues:

1) FIDO - Setting an unknown extension in the MatchCriteria with a value of fail_if_unkown=false returns NO_SUITABLE_AUTHENTICATOR instead of succeeding.
   Workaround: Please avoid sending unknwon extensions in the MatchCriteria. Only extensions supported by IOC Authenticators, as specified in the IOC EPC specification, are supported.
   This will be fixed in a later release so unknown extensions are simply ignored.

2) notifyUafResult deregisters for positive status codes.
   Workaround: Do not call notifyUafResult at the end of registration or authentication flows.
   This will be fixed in a later release.