Virtual Smartcard

Installation Guide

isosec.co.uk
0161 376 3570

Quay West, Media City
Manchester, M17 1HH

Contents

1. Prerequisites

This document covers the technical installation of Isosec software for the purposes of issuing Virtual Smartcard from an RA workstation and also an end user device for authentication with a Virtual Smartcard.

It is important to understand that the installation of Isosec software is not intended to be done in a standalone manner by an end user organisation. It is a guided install that MUST be done by the Isosec deployment team together with your technical team to troubleshoot any environment issues.

Furthermore, neither end users such as RA or clinical users should be involved in the installation of Isosec software.

As a prerequisite to the installation of the RA software, the RA workstation must be capable of issuing physical smartcards. The first step of the guided installation process will be to confirm this by issuing a physical card. Unless this passes, the guided installation will be stopped until this issue is resolved by you.

Before installing the Isosec Identity Agent, we recommend your environment has the following prerequisites setup. To note, in most cases, your machine/infrastructure will already be in place due to using the NHS Identity Agent.

- Networking requirements as described in this document (Section 2)
- Java (JRE) is already installed - This is a requirement of Clinical Applications such as the the NHS Portal, CIS and SCR.
- For users of physical smartcards, a card reader should be available.
- Middleware is installed on the machine - Install Gemalto Classic Client Toolbox and/or Oberthur

*It is important to ensure that the environment is clean before installing iO and that various other components are installed in the correct order. Failure to do so will result in problems, either with iO operating incorrectly or applications failing to authenticate.

2. Networking Requirements

For users to be able to authenticate, the following URLs will need to be accessible from both the RA workstation and end user machines. Please note that we cannot provide IP addresses as the Virtual Smartcard service is cloud based and IP addresses may change.

URLs to be Whitelisted by your Organisation

- https://vsc.isosec.co.uk
- https://ar1.isosec.co.uk
- https://ar2.isosec.co.uk
- https://ar3.isosec.co.uk
- https://test-ar1.isosec.co.uk
- https://licensing.isosec.co.uk
- https://logging.isosec.co.uk

Ports: 80 & 443

For both the RA workstation and end user machines, you must route the traffic to our cloud service via the N3/HSCN network and provide us with the CIDR range for the N3/HSCN network; your network provider should be able to assist you with this.

If a cloud VDI solution is being used and you are unable to route all the internet traffic through a N3/HSCN VPN setup, you must set up a proxy with a static IP address and route the traffic from your VDI to our service through this proxy. This static IP address will need to be provided to Isosec so it can be whitelisted on our cloud service.

3. RA Workstation Installation

To move forward with your RA workstation set up, Isosec requires you to demonstrate the RA workstation is capable of issuing a physical smartcard.

If this has been confirmed, only then should the below steps be carried out.

3.1 Installation Preparation

Once the issuance of a physical smartcard has been established, the following steps will be performed.

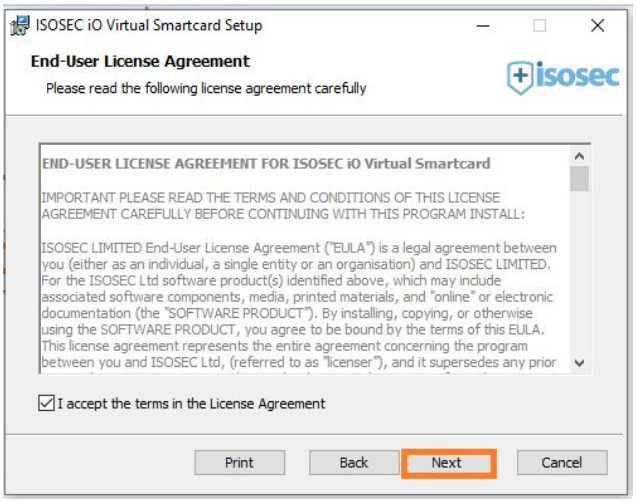
1. Uninstall the NHS Identity Agent to prevent any conflicts
2. Restart the Machine
3. Install Microsoft's Visual Studio C++ 2017 Redistributable package - https://isosec.co.uk/iO/VC_redist.x86.zip.

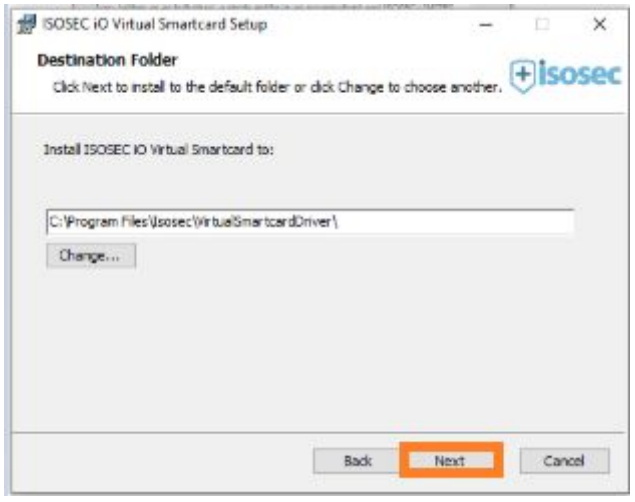
3.2 Virtual Smartcard Reader Driver

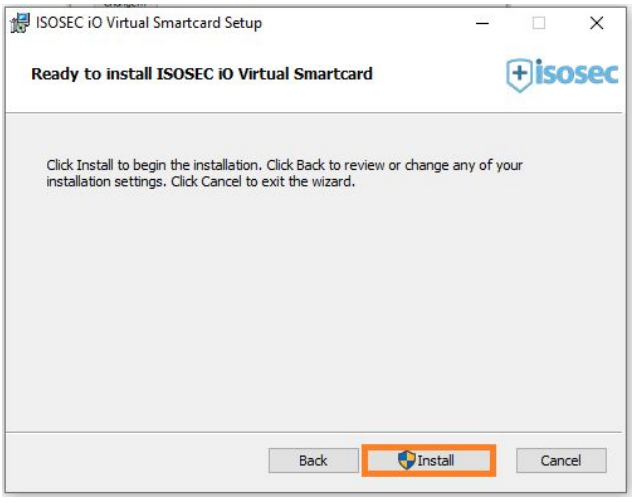
Each RA machine being set up to issue Virtual Smartcards will need to have the Virtual Smartcard Reader Driver installed. This should be installed before the Isosec Identity Agent and will follow on from any additional prerequisites highlighted from Section 3.1.

The Virtual Smartcard Reader Driver will have been sent to you in your onboarding email. This will need to be installed as an administrator (or admin rights delegated to the end-user).

1. Double click the Virtual Smartcard Reader Driver Installer and follow the steps as shown below:







2. When prompted, click to install the Driver and complete the installation. The iO Identity Agent can now be installed following the steps in Section 3.3

3.3 Standard iO installation

The Isosec iO Identity Agent must always be installed last (after any JRE & Gemalto installs) due to it also applying the following environment changes.

1. Installation of the latest NHS Root and Sub CA Certificates (if not already present)
2. Appends the Internet Options trusted sites for the NHS Portal and NHS Terms and Conditions sites

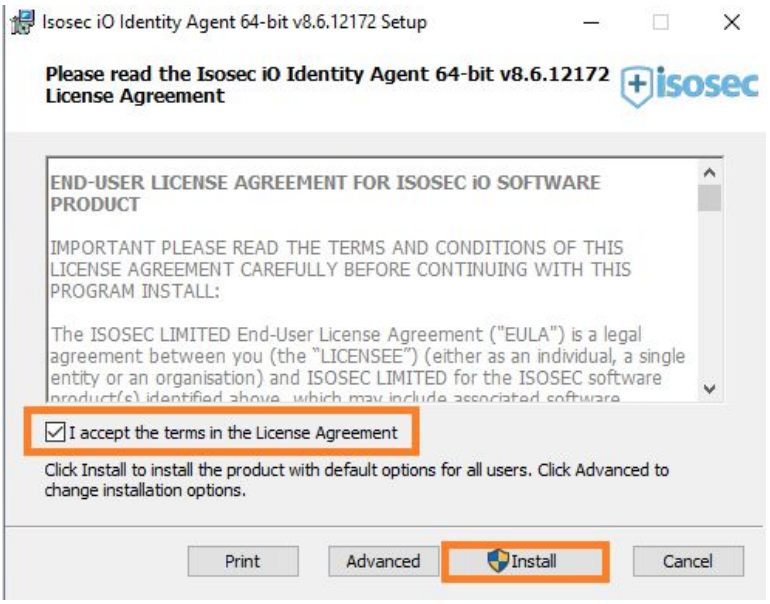
   The standard installation should ONLY be used for Registration Authorities or when the following applications are NOT used by Virtual Smartcard users.

   SystmOne
   EMIS
   Lorenzo
   Adastra

Installation Process:

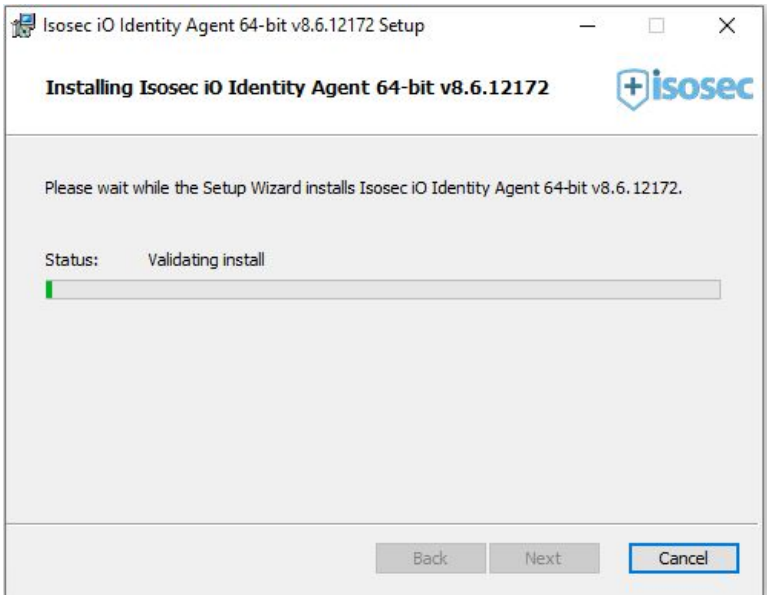
1. Ensure the HSCIC Identity Agent has been uninstalled

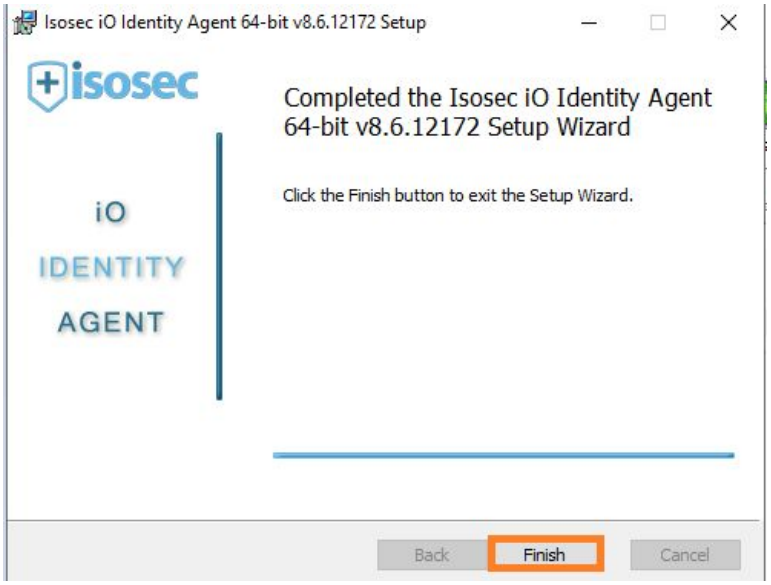
2. Double click the Isosec iO setup file which is provided within your Onboarding email. Accept the terms of the licence agreement and select Install



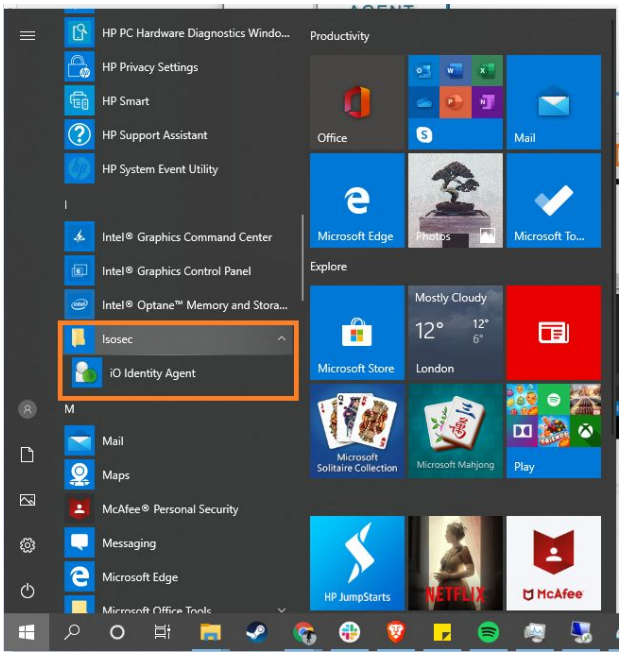
If prompted, close any applications needed for the installation.

3. The install will begin, once complete, select Finish





4. The Isosec Identity Agent can be found from the Windows Program Menu as shown below:



5. Follow the steps in Section 5 of this document to work through applying your licences.

4. End User User Machine Installation

4.1 Standard Installation

Any user who has been issued with a Virtual Smartcard will need to authenticate using the Isosec's iO Identity Agent.

As such, the NHS Identity Agent must be uninstalled from the user's machine before the Isosec's iO Identity Agent is installed on their machine.

Follow the steps in Section 3.3 of this document on how to install iO for a standard user. An End-user does not need to have the Virtual Smartcard Reader Driver installed.

If EMIS, Lorenzo or Adastra are to be used with a Virtual Smartcard, please ensure one of the Advanced iO Installation methods are used as per Sections 4.2 & 4.3.

4.2 Advanced iO Installation - P11 Tools & Local WinSCard

The Isosec Identity Agent must always be installed last due to it also applying the following environment changes.

1. Installation of the latest NHS Root and Sub CA Certificates (if not already present)

2. Appends the Internet Options trusted sites for the NHS Portal and NHS Terms and Conditions sites

The advanced installation should be followed if your organisation is planning on using the below applications and EPS with Virtual Smartcard. This method would only be installed for Virtual Smartcard users and not Registration Authorities.

EMIS
Lorenzo
Adastra
Medway

This method will install Isosec's gclib.dll file into the Gemalto directory (32bit & 64bit) ONLY. This should be used when a Trust has issues with system level placement of the WinSCard or has conflicts within their environment. The WinSCard.dll file will be automatically placed into the local application folder

using configuration items within the ISOSEC.properties as detailed within this section.

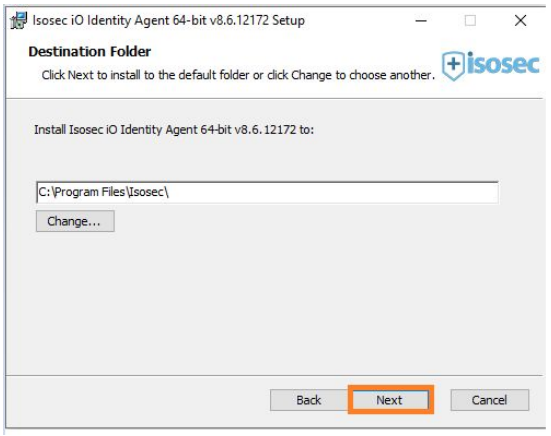
Installation Process:

1. Ensure the HSCIC Identity Agent has been uninstalled

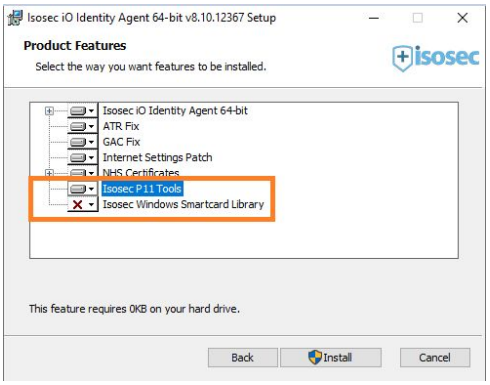
2. Double click the Isosec iO setup file as provided as part of your Onboarding email. Accept the terms of the licence agreement and select “Advanced”

   If prompted, close any applications needed for the installation.

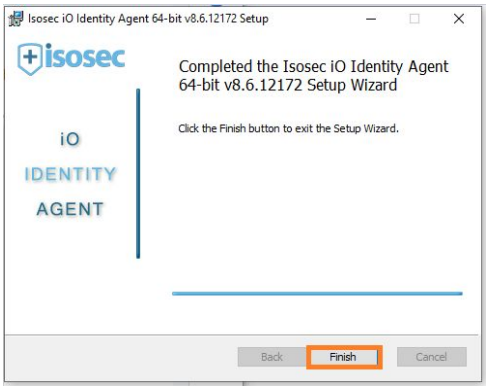
3. Click Next to install iO to the default Program Files location.



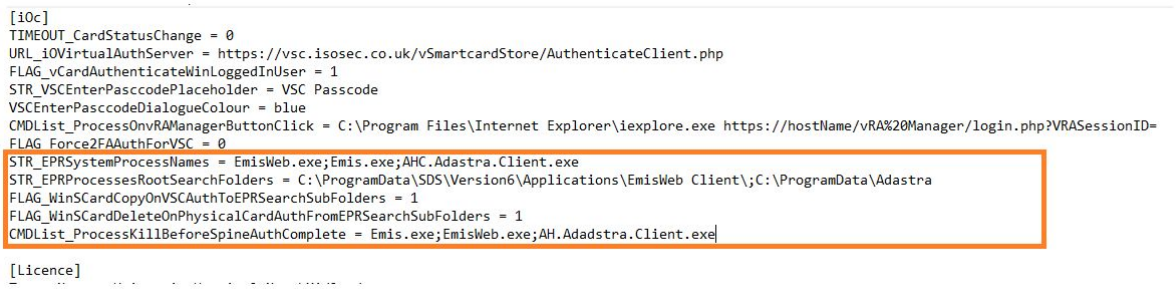
4. Select the P11 Tools ONLY as highlighted. Click Install to continue.



5. The installation process will run through quite quickly. Once complete, select Finish.



6. Open your ISOSEC.properties file and amend the top section of your licence to include the following configuration items. These items should be adjusted where necessary based on your clinical applications.



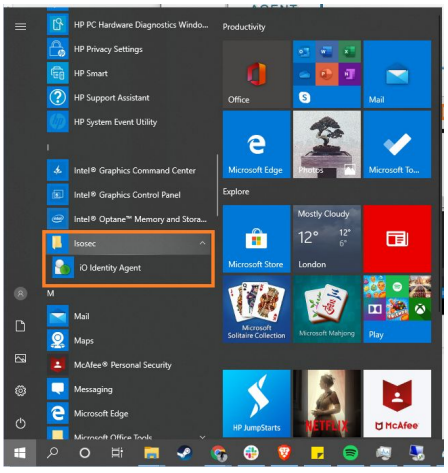
```
[iOc]
TIMEOUT_CardStatusChange = 0
URL_iOVirtualAuthServer = https://vsc.isosec.co.uk/vSmartcardStore/AuthenticateClient.php
FLAG_vCardAuthenticateWinLoggedInUser = 1
STR_VSCEnterPasccodePlaceholder = VSC Passcode
VSCEnterPasccodeDialogueColour = blue
CMDList_ProcessOnvRAManagerButtonClick = C:\Program Files\Internet Explorer\iexplore.exe https://hostName/vRA%20Manager/login.php?VRASessionID=
FLAG_Force2FAAuthForVSC = 0
STR_EPRSystemProcessNames = EmisWeb.exe;Emis.exe;AHC.Adastra.Client.exe
STR_EPRProcessesRootSearchFolders = C:\ProgramData\SDS\Version6\Applications\EmisWeb Client\;C:\ProgramData\Adastra
FLAG_WinSCardCopyOnVSCAuthToEPRSearchSubFolders = 1
FLAG_WinSCardDeleteOnPhysicalCardAuthFromEPRSearchSubFolders = 1
CMDList_ProcessKillBeforeSpineAuthComplete = Emis.exe;EmisWeb.exe;AH.Adadstra.Client.exe

[Licence]
```

Property	Example Value	Meaning
STR_EPRSystemProcessNames	EmisWeb.exe;Emis.exe;AHC.Adastra.Client.exe	A semi-colon separated list of process names that iO should search for in sub-folders specified by the 'STR_EPRProcesessesRootSearchFolders' configuration item. The configuration items will need to be used together to ensure that Isosec's WinSCard can be copied to/deleted from any folders in which these processes are found.
STR_EPRProcessesRootSearchFolders	C:\ProgramData\SDS\Version6\Applications\EMISWeb Client\;C:\ProgramData\Adastra\	A semi-colon separated list of search folders in which iO should search for the EPR processes specified by their name by 'STR_EPRSystemProcessNames' config item.
FLAG_WinSCardCopyOnVSCAuthToEPRSearchSubFolders	1	Enables copying Isosec's WinSCard dll into folders (sub-folders of folders specified in 'STR_EPRProcessesRootSearchFolders') in which the EPR processes (specified by 'STR_EPRSystemProcessNames') are found. The 'copy' operation happens upon the Virtual Smartcard passcode prompt being displayed
FLAG_WinSCardDeleteOnPhysicalCardAuthFromEPRSearchSubFolders	1	Deletes Isosec's WinSCard.dll from folders (sub-folders of folders specified in 'STR_EPRProcessesRootSearchFolders') in which the EPR processes (specified by 'STR_EPRSystemProcessNames') are found. The 'delete' operation happens upon the Physical Smartcard passcode prompt being displayed.
CMDList_ProcessKillOnCardPresence	AHC.Adastra.Client.exe;Emis.exe;EmisWeb.exe	A semi-colon separated list of process names that iO should kill when a Smartcard is presented and the user has not yet authenticated. This configuration items ensures that the clinical system is not running before Isosec's WinSCard.dll is copied into the directories listed within STR_EPRProcessesRootSearchFolders

7. Save the new licence changes. Follow the steps in Section 5 of this document to work through applying your licences.

8. The Isosec Identity Agent can be found from the Windows Program Menu as shown below:



4.4 Silent Install Instructions

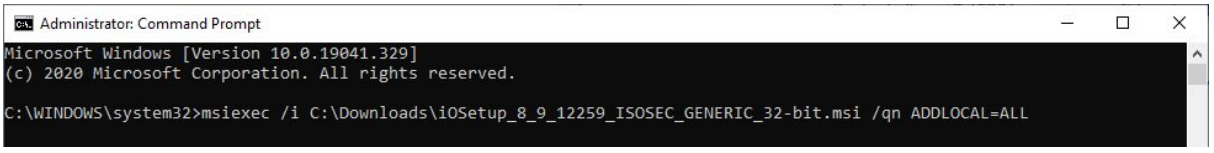
The iO Identity Agent can be installed silently via the command prompt or a script.

The iO Identity Agent MSI installer can be run with additional parameters through the msiexec utility. For this installation method to work, the command line must be run as an administrator.

Using a combination of ADDDEFAULT, ADDLOCAL, and REMOVE, you can choose which features to install.

1. Installing standard iO (not used for EPS) - msiexec /i [msi path] /qn
2. Installing Advanced iO (EPS) System Level - msiexec /i [msi path] /qn ADDLOCAL=ALL
3. Installing Advanced iO (EPS) P11 Only - msiexec /i [msi path] /qn ADDLOCAL=ALL REMOVE=IsosecWindowsSmartcardLibrary

For example, a silent install with method 2 would look like this -

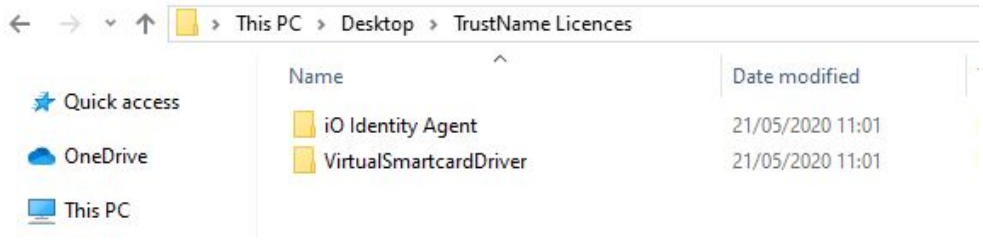


The installation can alternatively be managed by SCCM removing any required scripts and the like.

5. Applying Your Licences

Your Isosec licences will be distributed to your Organisation via email. These files should NOT be shared outside of your organisation, doing so will result in you exceeding your licence limit which may lead to additional charges.

The zip file received via e-mail will contain 2 unique ISOSEC.properties product licences as shown below.



These licences will need to be placed into the corresponding install directories. This will be dependent on what software the user has installed (Registration Authority or Standard User) and will need to overwrite the existing generic ISOSEC.properties file.

Isosec recommends that a GPO is used to distribute your licences across your device estate.

The ISOSEC.properties file in the iO Identity Agent folder should be copied into - C:\Program Files\Isosec\iO Identity Agent

The ISOSEC.properties file within the VirtualSmartcardDriver folder should be copied into - C:\Program Files\Isosec\VirtualSmartcardDriver *(Installed for RAs ONLY as highlighted in the above documentation)*

6. Uninstalling the Isosec Identity Agent

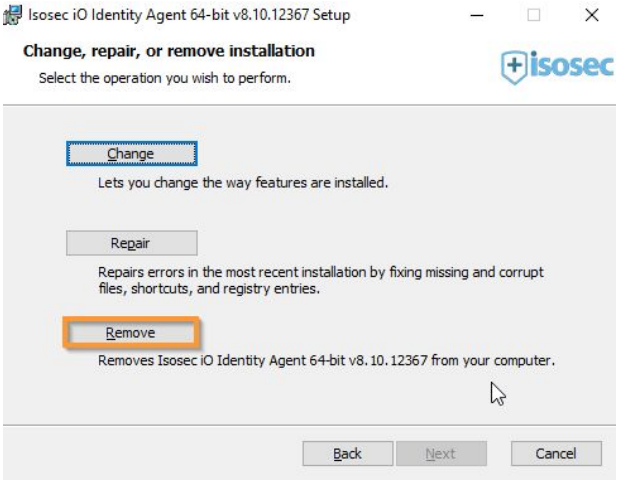
6.1 Manual Uninstall

The iO Identity Agent and/or the Virtual Smartcard Reader driver can easily be removed via the "Add or Remove Programs" or by double clicking the MSI file and working through the uninstall wizard - Administrator rights will be required.

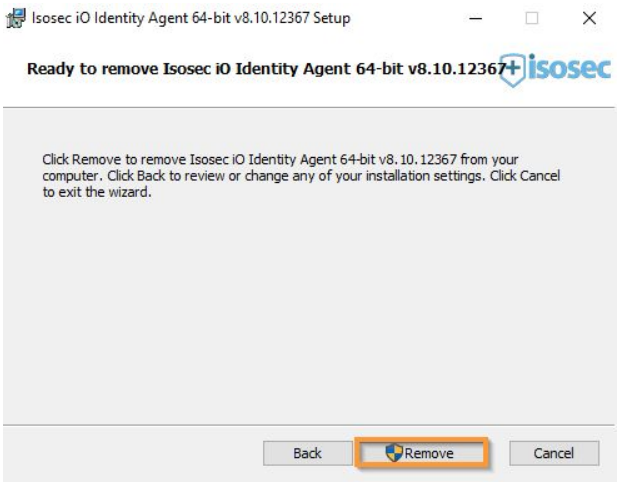
This process will remove the Identity Agent and any additional configuration required for AdES - The licence file within the C:\Program Files\Isosec\iO Identity Agent directory with the AdES configuration will also be removed.

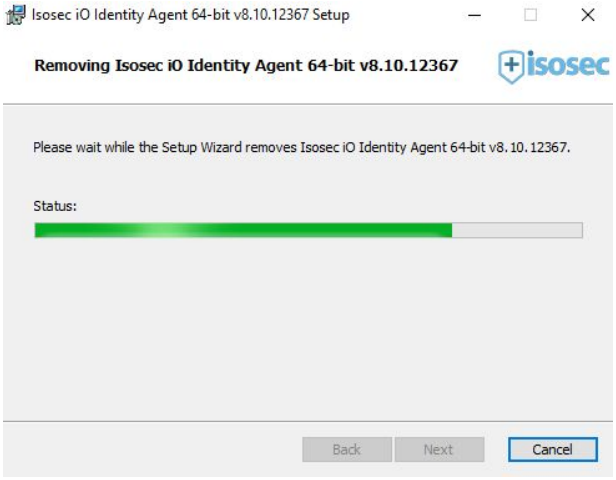
When prompted, select "Next"

Select the "Remove" option

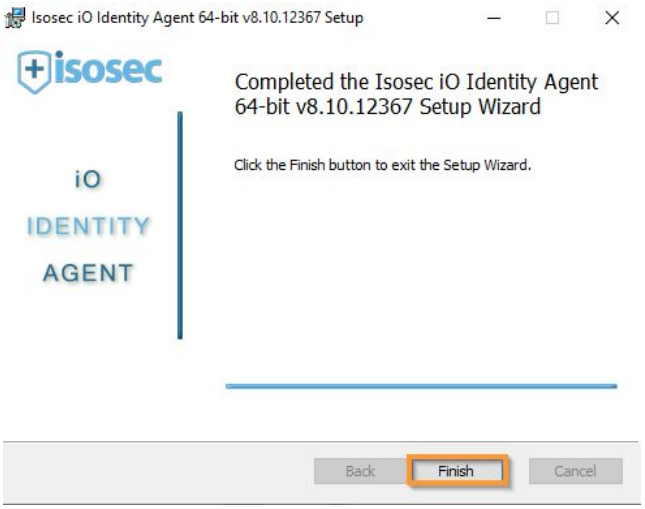


To confirm the removal, hit “Remove” - If this process was not initiated by an administrator, the uninstaller will prompt for administrator credentials.





After the process has run through, simply click “Finish” - A restart is recommended before proceeding to install an alternative Identity Agent



6.2 Scripted Uninstall

The iO Identity Agent can be uninstalled via the command prompt or a script.

Each MSI installer can be run with additional parameters through the msiexec utility. For this installation method to work, the command line must be run as an administrator.

Using a combination of ADDDEFAULT, ADDLOCAL, and REMOVE, you can choose which features to uninstall.

1. Uninstall standard iO & Virtual Smartcard Reader Driver (not used for EPS) - msiexec /x [msi path]

2. Uninstalling Advanced iO (EPS) System Level - msiexec /x [msi path] ADDLOCAL=ALL

3. Uninstall Advanced iO (EPS) P11 Only - msiexec /i [msi path] ADDLOCAL=ALL REMOVE=IsosecWindowsSmartcardLibrary

A package GUID can also be used for the removal instead of referencing the MSI path. /qn and /passive along with other sub commands can be used to silently remove the application, with or without a UI.

The uninstallation can alternatively be managed by SCCM removing any required scripts and the like.

7. Licence Configuration

The Identity Agent installation folder (default directory - *C:\Program Files\Isosec\iO Identity Agent)* contains an ISOSEC.properties file which includes information about your licence and a number of settings which control the behaviour of the iO Identity Agent.

Your licence will include a FLAG_Enable1FAForVSC = 0, forcing Two Factor Authentication by default. This can not be amended by an organisation, doing so will invalidate the licence.

AdES Virtual Smartcards are Two Factor enabled by default and can not be changed by an organisation.

7.1 iO Properties

The following table includes optional properties (with examples and explanations) which can be added to iO, these must be set anywhere under the [iOc] header in the ISOSEC.properties file as shown below:

Property	Example Value	Explanation
CMD_Browser	C:\Program Files (x86)\Internet Explorer\iexplore.exe	Location of browser executable, used for LaunchURI and Auth State URLs
CMDList_ProcessOnCardPresence	C:\Program Files\Gemalto\Classic Client\BIN\RegTool.exe	A semi-colon separated list of executable locations to launch on Card Presence

CMDList_ProcessOnCardRemoval	tsdiscon.exe	A semi-colon separated list of executable locations to launch on Card Removal
CMDList_ProcessOnPostAuthentication	C:\Program Files\Internet Explorer (x86)\iexplore.exe https://portal.national.ncrs.nhs.uk	A semi-colon separated list of executable locations to launch on Authentication
CMDList_ProcessOnReconnect	C:\Program Files\Gemalto\Classic Client\BIN\RegTool.exe	A semi-colon separated list of executable locations to launch on Reconnect
CMDList_ProcessOnStart	C:\Program Files\Gemalto\Classic Client\BIN\RegTool.exe	A semi-colon separated list of executable locations to launch on Start
CMDList_ProcessKillOnCardRemoval	iexplore.exe;RegTool.exe	A semi-colon separated list of process names to kill on card removal
CMDList_ProcessKillOnDisconnect	RegTool.exe	A semi-colon separated list of process names to kill on disconnect
CMDList_ProcessKillOnExit	notepad.exe;calc.exe;cmd.exe	A semi-colon separated list of process names to kill on Exit
CMDList_ProcessKillOnPostDeauth	iexplore.exe	A semi-colon separated list of process names to kill on de-authentication
CMDList_ProcessKillOnCardPresence	iexplore.exe	A semi-colon separated list of process names that iO should kill when a Smartcard is presented and user has not yet authenticated.

STR_Cert_Issuer_Pattern	NHS Level 1A;SubCA02; TSPINE_SubCA;NIS4_SubCA	A semi-colon separated list of Certificate Issuer Patterns that match the certificate issuer present on user smart cards
STR_Cert_Issuer_Removal_Pattern	NHS Level 1A;NHS Level 1B; SubCA02;NIS1_SUBCACC; TSPINE_SubCA;TSPINE_Sub CACC; NIS4_SubCA;NIS4_SubCACC	A semi-colon separated list of Certificate Issuer Patterns that match the certificate issuer present in the user's personal cert store to be removed on authentication, so that only the current user's smart card certificates are present
STR_SharedFolderLocation	\\Permanent-Share-Location\SharedFolder_iO\	Location where the shared licence is housed. The licence can be updated remotely from Isosec and all other clients read from this licence.
STR_Reader_Pattern_Ignore_List	OMNIKEY;Dell Keyboard Reader	A semi-colon separated list of card readers to be ignored by iO. Cards will not be detected by these readers. Case sensitive.
URL_SpineActivateRequest	https://gas.national.ncrs.nhs.uk/login/authactivate; https://gas.nis1.national.ncrs.nhs.uk/login/authactivate; https://gas.tsp.national.ncrs.nhs.uk/login/authactivate; https://gas.vn1.national.ncrs.nhs.uk/login/authactivate	A semi-colon separated list of URLs for Spine Authentication activation requests (matching STR_Cert_Issuer_Pattern semi-colon order)
URL_SpineRoleSelection	https://sbapi.national.ncrs.nhs.uk/saml/RoleSelectionGP.jsp;https://sbapi.nis1.national.ncrs.nhs.uk/saml/RoleSelectionGP.jsp;https://sbapi.tsp.national.ncrs.nhs.uk/saml/RoleSelectionGP.jsp;https://sbapi.vn1.national.ncrs.nhs.uk/saml/RoleSelectionGP.jsp	A semi-colon separated list of URLs for Role Selection (matching STR_Cert_Issuer_Pattern semi-colon order)
FLAG_BlankScreenIgnoreAuthState (introduced version 4.1)	1	Blank Screen on reconnect, regardless of auth state.

FLAG_BlankScreenOnCardRemoval	1	Blank Screen on card removal, to cover user's workspace/desktop
FLAG_DisableBlankScreenOnReconnect	1	Disable Blank Screen on reconnect, to cover the user's workspace/desktop during authenticated card verification
FLAG_DisableLaunchURIonAuthSuccess	1	Disable Launch URI returned as part of the Role Selection response. Generally used for new users to accept Spine/Portal terms and conditions
FLAG_DisableMenuItemCancelLA	1	Disable 'Cancel LA' menu item entry
FLAG_DisableMenuItemLA_Switch	1	Disable user switching of Options menu 'Local Auth' menu item entry
FLAG_DisableMenuItemLockScreen	1	Disable 'Lock Screen' menu item entry
FLAG_DisablePinReAuth (Callisto Only)	1	Disable PIN entry during authenticated user verification. Handy for allowing users to continue with their work, unprompted, if the smart card is always going to be present
FLAG_DisableRoleSelection	1	For some Spine authentications there is no response from the Role Selection URL. In such cases disabling the Role Selection is useful (e.g. in 'Choose & Book' environments)
FLAG_DisableSlotNotificationIcon	1	Disable system tray icon for active Card Reader status (card presence)

FLAG_DisableSpineSessionPersistence (Callisto Only)	1	Disable Spine Session Persistence, do not retain the spine session when the smartcard is removed
FLAG_DisconnectOnCardRemoval	1	Disconnect on card removal
FLAG_LargeDialogSize	1	Use large dialog size, if set then all dialogs are double the normal size, which is handy for tablets
FLAG_LaunchURIandProcessPostAuth	0	If FLAG_DisableLaunchURIonAuth Success is not set, and a Role Selection response URI is launched, continue with CMDList_ProcessOnPostAuthentication
FLAG_LocalAuth (LA Only)	1	Launch iO in Local Auth mode
FLAG_LockScreenOnCardRemoval	1	Lock Screen on card removal, to cover user's workspace/desktop, requiring authenticated card verification to resume
FLAG_NoAuth	1	Don't perform an authentication
FLAG_NoAuthCloseSlotSelectionDlg	1	When FLAG_NoAuth is set, close Slot Selection dialog

FLAG_ReverseRoles	1	Reverse the order of the roles in the Role Selection dialog
FLAG_SeparatePinFailDlg	1	Display a separate Pin Fail dialog after an incorrect/invalid pin has been entered
FLAG_CardCheckV5V6CardsFirst	1	Checks v5 & v6 cards using legacy methods of smartcard communication which are quicker (use if Trust has no v8 cards)
FLAG_EnableClosingSmartcardSession	1	Enables iO to forcibly close connection to smartcard after authentication. In some cases, can help with 3rd party applications accessing the card
FLAG_EnableRecognisingCardsByATR	1	If set, iO recognises smartcard type (or inserted card) by Answer to reset (ATR) as soon as the card is inserted, without having to initiate any smartcard communication to detect the smartcard type
FLAG_MapGetTicketNoAuthToGetTicket	1	By default (if the config item is omitted from iO's config file) this value is set to 0.. If the value is set to 1, it will cause that all TicketAPI calls that call GetTicketNoAuth function will effectively trigger GetTicket function *
FLAG_VerifyUserAfterWakeFromSleep	1	If turned on the user is required to enter Smartcard passcode after waking the machine from sleep
FLAG_ForceClearSmartcardDataCache	1	If enabled forces iO to read entire contents of smartcard for every time it's presented

FLAG_DisableTLSProtocolSettingForWinHttp	1	iO by default sets certain secure protocols that can be used for network connections for VSC service and other services. If this flag is set / enabled, iO will not set any specific secure protocols but instead will use default windows network connection settings for secure https connections.
STR_DefaultRoleID		Default role to select, by ID number. Useful for automating testing
STR_Passcode	Password	Change the word Passcode in dialogs to string present here
STR_ProxyUserPass		username: password colon separated pairing for proxy user validation, for auditing
TIMEOUT_Authentication	600	Timeout, in minutes, before the ticket is destroyed (automatic logout is performed)
TIMEOUT_AuthWarning	30	Timeout, in minutes.By default the user is notified with a popup about their spine ticket / session expiry 60 minutes before the spine session expires. If this configuration item is set, iO will notify the user about their spine session expiry the specified amount of minutes before its expiry.
TIMEOUT_Challenge	20	Period of time in seconds that iO requests another challenge from the spine.
TIMEOUT_MediumInactivity	60	Timeout, in seconds, before the display is blanked. Useful for privacy on tablets

TIMEOUT_LongInactivity	180	Timeout, in seconds, after TIMEOUT_MediumInactivity before validation is required to return from a blanked display. Useful for privacy/security on tablets
TIMEOUT_LogoutInactivity	120	Timeout, in seconds after TIMEOUT_MediumInactivity and TIMEOUT_LongInactivity before the user is automatically logged out. Useful for security on tablets
TIMEOUT_ReconnectPrompt	60	Timeout, in seconds, before the verification dialog that appears on reconnect is automatically cancelled. TIMEOUT refreshes on user input
TIMEOUT_CardStatusChange	0	Timeout, in milliseconds, before iO checks for a change in cards behaviour
TIMEOUT_IgnoreDisconnectOnCardRemovalIfCardPresented	2	Timeout in seconds to wait for card presence to occur before disconnect is triggered. Only works when FLAG_DisconnectOnCardRemoval is set
NUM_DefaultConnectionsWinHttpSecureProtocols	0	Numeric representation of Windows secure protocols for secure https connections that should be enforced by iO clients to be used for communication with Isosec's auditing, licensing and remote logging services. 2048 - TLS 1.2 ; 512 - TLS 1.1 ; 128 - TLS 1.0 ; 32 - SSL3 ; 8 - SSL2 Combination of multiple protocols - add up numeric representations of required protocols (e.g support for TLS 1.2 and TLS 1.1 = 2048 + 512 = 2560) Setting the number to 2048 will allow TLS 1.2 protocol only Setting the number to 0 has the same effect like setting it to 2728 (- enables all secure protocols = adds up all the numeric representations of all protocols)

DelayMilliSec_ReadCardUID	500	Delay, in milliseconds, before iO will begin to attempt to read the smartcard's UID
DelayMilliSec_BeginCardSession	100	Delay, in milliseconds, before iO will begin to attempt to start the session to the card
FLAG_ImmediateLogging	1	Disables background threading for capturing logs as well as disables a temporary memory buffer to store logs in before the logs are written in a log file. Having this item on will immediately write every single log to a log file. It will however slow down program execution to some extent.
FLAG_DisableProxyUseForSpineConnections	1	As of iO 8.9.12307, iO will now use a system proxy (if available) for spine connectivity. Should a Trust wish to disable this due to how their infrastructure is set up, this item can be added with a value of 1.
NumOnCardSignFailRetryAttempts		Number of attempts iO will try to sign an authentication challenge (with physical Smartcard only) if the challenge signing fails for whatever reason
NumOnCardSignFailRetryAttempts	10	Number of attempts iO will try to sign an authentication challenge (with physical Smartcard only) if the challenge signing fails for whatever reason

* *GetTicketNoAuth* - Gets the ticket from the identity agent if the user is authenticated. If the user is not authenticated, no ticket will be returned and the identity agent will not trigger any action

GetTicket - gets the ticket from the identity agent if the user is authenticated. If the user is not authenticated, it will prompt the user to authenticate (if the user's smartcard is not present, the user will be presented with 'Please log in with your smartcard dialogue') and must wait for the authentication to be either completed or cancelled.

Returns the ticket to the application after the user finished the authentication. If

the user cancels the authentication (by hitting a cancel button on one of the dialogues), no ticket will be returned

7.2 Licence properties

Below are the permanent Licence section properties along with the corresponding descriptions. These should NOT be adjusted, doing so will invalidate your licence file.

Property	Example Value	Meaning
Trust_Name	ISOSEC	Name of the organization which the iO Identity Agent is licenced for.
Expiry_Date	31/08/2020 15:59:00	Expiration date until when the licence is valid. When the expiration date is reached, iO will start working in a 'graceful mode' and will display pop-ups prompting the user to renew the licence, allowing the user for another up to 30 days to use iO. After 30 days of licence being expired iO will no more allow the user to authenticate.
FLAG_Audit	1	If set, iO automatically sends audits to Isosec's auditing services for authentication and de-authentication events, as well as for Windows session disconnects and reconnects.
FLAG_Callisto	1	If set, iO enables Spine session persistence which in turn allows the user to remove physical smartcard from a smartcard reader. Any opened clinical applications that don't require private key operations with the smartcard will remain open and the user will be able to use them without the smartcard being inserted.
FLAG_Eval	0	Set for evaluation versions of iO. There is absolutely no difference, software wise, between the evaluation and release versions of iO. It purely comes down to the ISOSEC.properties file used
FLAG_LA	0	Available as an optional extra, enables the following optional entries to be used: - FLAG_LocalAuth

FLAG_vCard	1	Available if Trust has purchased the Virtual Smartcard product. Allows the use of Virtual Smartcard for authentication
FLAG_Enable1FAForVSC	0	If requested by the Trust this can be enabled to allow 1 Factor Authentications for whitelisted applications using a Virtual Smartcard
FLAG_LocalVSCPasscodeCache	0	When this is set, iO will start caching the VSC passcode upon successful authentication into the AppData folder on the local device for each user on the machine

7.3 Virtual Smartcard Properties

The following are settings are for use with the Isosec Virtual Smartcard with iO:

Property	Example Value	Explanation
URL_iOVirtualAuthServer	https://vsst.isosec.co.uk/vSmartcardStore/Authenticate Client.php	Location of virtual authentication server
FLAG_DisplayQRImageOnLoginPrompt	0	Allows QR code scanning in order to authenticate using Isosec Authenticator Mobile Application (2-Factor)
TIMEOUT_QRCode	60	Timeout in seconds, before the QR code expires.
FLAG_vCardRemoteAuthentication	0	Allows iO client machines to connect to N3 without connectivity as long as Virtual Smartcard authentication server is reachable and iO is configured to use such server
FLAG_vCardAuthenticateWinLoggedInUser	1	Allow authentication using Windows Active Directory account and Virtual Smartcard

FLAG_ConnectIsosecVSCIntoVSCReaderAfterAuth	1	If turned on will emulate a card being inserted into the Virtual Smartcard Reader after authentication. Requires Isosec's VSC reader driver component to be installed
TIMEOUT_VSCPasscodeLocalCache	3600	Value in seconds that the VSC passcode can be cached for. Requires FLAG_LocalVSCPasscodeCache to be enabled to have any effect
TIMEOUT_vSCSignChallengeRequest	15	Timeout, in seconds. Default number of seconds used by iO is 5. Number of seconds for Virtual Smartcard signing network requests until they timeout. If Isosec's virtual smartcard service doesn't respond to the challenge signing request within this timeout period, the user will not be able to authenticate with their VSC.
FLAG_DisableLocalVSCPasscodeCache	1	If enabled will disable VSC passcode caching. Requires FLAG_LocalVSCPasscodeCache to be enabled to have any effect
FLAG_DisableVSCFido2DeviceSupport	1	If enabled, iO will stop watching for supported FIDO2 devices insertions / removals. By default iO watches for FIDO2 devices for 2FA authentication with Virtual smartcard
FLAG_AllowRFIDCards	1	If enabled, will allow HR cards (e.g mifare cards with required frequency levels) to be recognised by iO, possibly associated with a virtual smartcard of a user and used as a second factor for authentication with Virtual Smartcards
NUM_VSC_API_Version	1	Virtual smartcard backend API version that should be used by iO. iO clients 8.3.xxxx and above use API version 2 by default. Currently supported version numbers are 1 or 2
NUM_VSCAllowedWinHttpSecureProtocols	2048	Numeric representation of Windows secure protocols for secure https connections that should be enforced by iO client to be used for communication with Virtual smartcard service. Since 30th June 2020 Isosec's VSC service enforces /will enforce TLS 1.2 protocol only, which is represented by number 2048 2048 - TLS 1.2 ; 512 - TLS 1.1 ; 128 - TLS 1.0 ;

		32 - SSL3 ; 8 - SSL2 Combination of multiple protocols - add up numeric representations of required protocols (e.g support for TLS 1.2 and TLS 1.1 = 2048 + 512 = 2560) Setting the number to 2048 will allow TLS 1.2 protocol only
STR_VSCEnterPasccodePlaceholder	VSC passcode	Text displayed as a placeholder in Virtual Smartcard passcode field
VSCEnterPasccodeDialogueColour	blue	Set colour of Virtual Smartcard dialogue box (useful for differentiating between physical and virtual) Supported colours: yellow, orange, red, green, blue, purple
CMDList_ProcessOnvRAManagerButtonClick	start chrome "https://virtualsmartcardserver.isosec.co.uk/RAManager/login.php"	If specified authenticated users with RA role can launch RA Management tool as specified URL (required only on RA machines)
FLAG_ForceServerSpineTicketCheckForVRAManagerAccess	1	Forces iO to evaluate the user's ability to access vRA Manager based on the spine ticket obtained during authentication. Evaluation of this is enforced to be done on a Virtual smartcard server as opposed to iO client side.

7.4 Optional EPR Properties

As per this guide, the "Advanced" installation for iO should be used to enable electronic prescribing with Virtual Smartcard. Should an organisation experience any issues with the full advanced installation whereby the Isosec Windows Smartcard Libraries are installed in the System32 & SysWoW Directory, local application folder placement should be used.

An advanced installation of iO should be performed, selecting the P11 Tools ONLY. Once installed, the below configuration items will need to be added into the ISOSEC.properties file.

Property	Example Value	Meaning
STR_EPRSystemProcessNames	EmisWeb.exe;Emis.exe;AHC.Adastra.Client.exe	A semi-colon separated list of process names that iO should search for in sub-folders specified by the 'STR_EPRProcesessesRootSearchFolders' configuration item. The configuration items will need to be used together to ensure that Isosec's WinSCard can be copied to/deleted from any folders in which these processes are found.
STR_EPRProcessesRootSearchFolders	C:\ProgramData\SDS\Version6\Applications\EMISWebClient\;C:\ProgramData\Adastra\	A semi-colon separated list of search folders in which iO should search for the EPR processes specified by their name by 'STR_EPRSystemProcessNames' config item.
FLAG_WinSCardCopyOnVSCAuthToEPRSearchSubFolders	1	Enables copying Isosec's WinSCard dll into folders (sub-folders of folders specified in 'STR_EPRProcessesRootSearchFolders') in which the EPR processes (specified by 'STR_EPRSystemProcessNames') are found. The 'copy' operation happens upon the Virtual Smartcard passcode prompt being displayed
FLAG_WinSCardDeleteOnPhysicalCardAuthFromEPRSearchSubFolders	1	Deletes Isosec's WinSCard.dll from folders (sub-folders of folders specified in 'STR_EPRProcessesRootSearchFolders') in which the EPR processes (specified by 'STR_EPRSystemProcessNames') are found. The 'delete' operation happens upon the Physical Smartcard passcode prompt being displayed.
CMDList_ProcessKillOnCardPresence	AHC.Adastra.Client.exe;Emis.exe;EmisWeb.exe	A semi-colon separated list of process names that iO should kill when a Smartcard is presented and the user has not yet authenticated. This configuration items ensures that the clinical system is not running before

		Isosec's WinSCard.dll is copied into the directories listed within STR_EPRProcessesRootSearchFolders

8. Additional iO Links

For reference, Isosec changelog can be found below which includes all release notes for our iO Identity Agent.

www.isosec.co.uk/changelog/iO/
http://isosec.co.uk/changelog/Virtual%20Smartcard/

9. User Guides

A number of guides can be found on our Delivery Hub page below to assist RAs with managing/issuing Virtual Smartcard and using 2-Factor Authentication:

https://isosec.co.uk/delivery-hub/