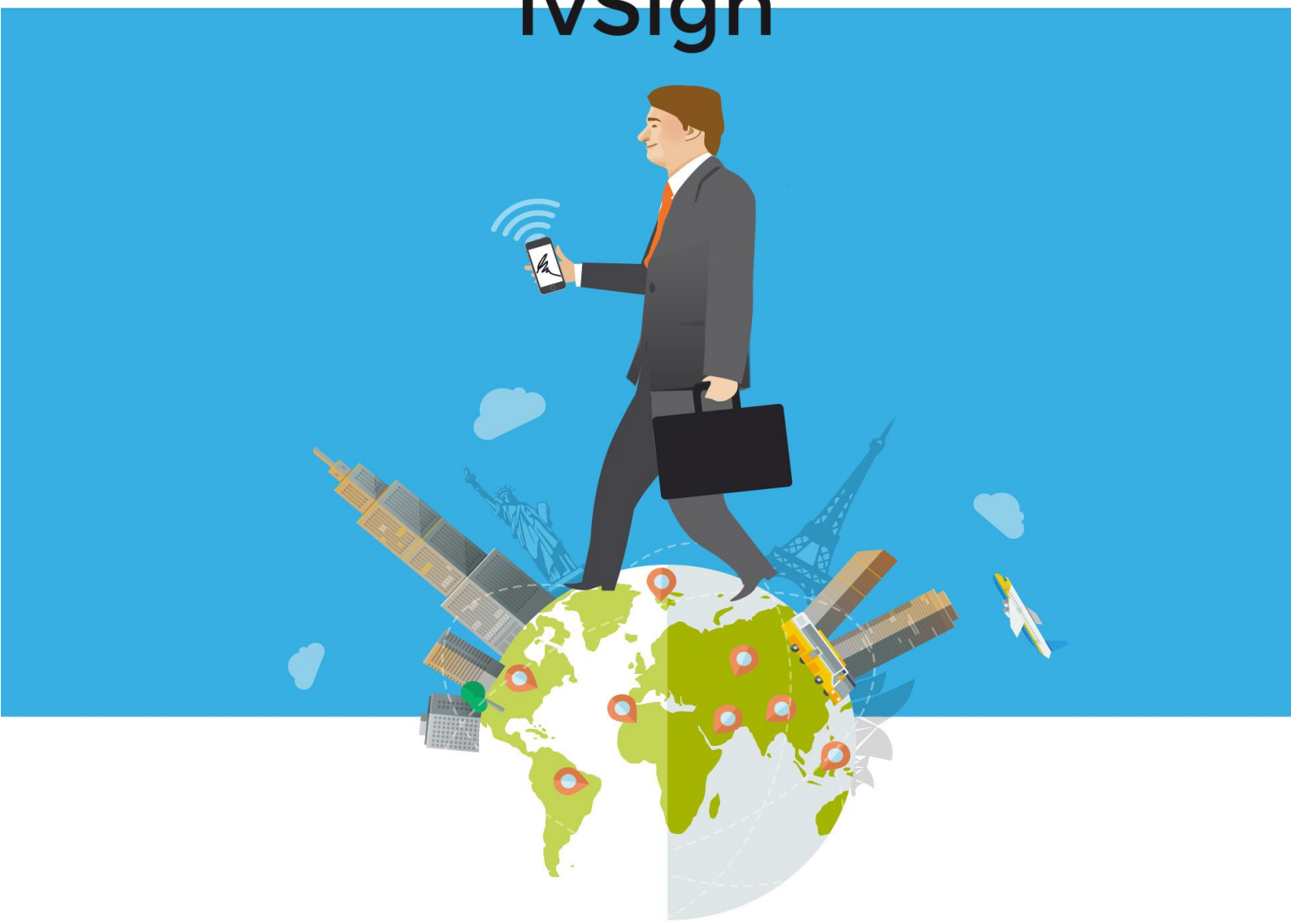
IvSign



Manual de descubrimiento y autoimportación de certificados: IvSign Sniffer Tool

ÍNDICE

1. Extensión IvSign Sniffer Tool

El módulo KeyController de IvSign dispone de una extensión que permite el inventariado y autoimportación de los certificados instalados en el equipo local para un usuario específico.

Se trata de un ejecutable que debe ser lanzado desde línea de comandos, o mediante GPO, de acuerdo con la siguiente estructura:

```
ListCertificates.exe -formato -ruta_fichero_salida [-sobreescritura]
```

La herramienta cuenta con 2 funcionalidades principales:

- Autodescubrimiento de los certificados instalados localmente en el equipo
- Autoimportación de certificados a IvSign (con posibilidad de borrado de los certificados locales)

Adicionalmente, la herramienta cuenta con un alto nivel de parametrización y configuración que ofrece la flexibilidad necesaria para que cada organización planifique y gestiones los procesos de descubrimiento e importación en base a sus necesidades y sus criterios de uso.

En los siguientes apartados se muestran ejemplos detallados sobe el funcionamiento de Ivsign Sniffer Tool y las diferentes posibilidades de parametrización disponibles para el usuario.

En caso de necesitar esta aplicación, deberá solicitar el código de licencia a su gestor de proyectos.

2. Utilización y ejemplos

Este módulo dispone de diferentes funcionalidades para la gestión de los certificados instalados localmente en un equipo.

Autodescubrimiento de certificados

Los diferentes parámetros se cumplimentan en base a los valores de la siguiente tabla:

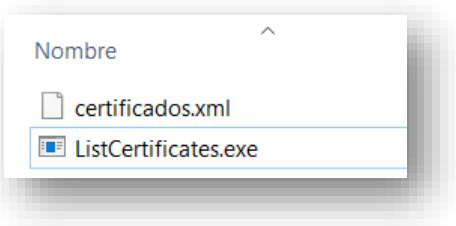
Parámetro	Descripción
licencia	**-lic:[id.licencia]** id.licencia es la licencia de la ampliación IvSign Sniffer Tool. Si no dispones de una licencia o ha expirado, contacta con tu gestor de proyectos.
ruta_fichero_salida	**-o:[archivo]:** Establece el archivo de enumeración de certificados. Debe especificarse la ruta completa del fichero de salida de los datos. Por ejemplo: **-o:C:\temp\certificados.xml** Adicionalmente, la aplicación permite incluir información sobre el equipo o el usuario en el nombre del fichero de salida de datos, utilizando los comodines {USERNAME} y {COMPUTERNAME}.
formato	Posibles valores: **-csv** : Establece el formato de salida para enumeración de certificados a CSV **-xml** : Establece el formato de salida para enumeración de certificados a XML
sobreescritura	Parámetro opcional que sobrescribe el archivo de enumeración de certificados. Valor: **-overwrite**

A continuación, se incluyen ejemplos básicos de uso de la herramienta.

EJEMPLO 01: Obtención del inventario de certificados en formato XML.

```
C:\Temp>ListCertificates.exe -lic:[id.licencia] -xml -o:C:\Temp\certificados.xml
```

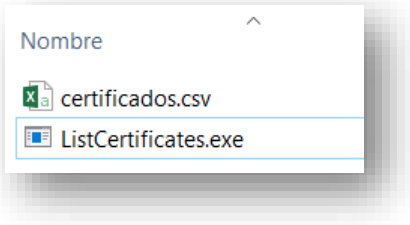
Este comando genera el fichero:



EJEMPLO 02: Obtención del inventario de certificados en formato CSV.

```
C:\Temp>ListCertificates.exe -lic:[id.licencia] -csv -o:C:\Temp\certificados.csv
```

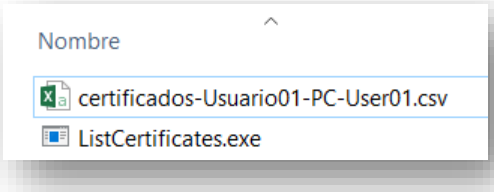
Este comando genera el fichero:



EJEMPLO 03: Obtención del inventario de certificados formateando el fichero de salida con el nombre del equipo y del usuario:

```
C:\Temp>ListCertificates.exe -lic:[id.licencia] -csv -o:C:\Temp\certificados-
{USERNAME}-{COMPUTERNAME}.csv
```

Este comando genera el fichero:



Autoimportación de certificados a IvSign

Antes de iniciar un proceso de importación de certificados a IvSign es necesario verificar los siguientes puntos:

- Disponer de una licencia válida. En caso de no disponer de una licencia consulta con tu gestor de proyectos.
- Verificar que existe conectividad entre el equipo o entorno local, y el entorno de IvSign deseado.

Operación	Descripción y parámetros
licencia	**-lic:[id.licencia]** id.licencia es la licencia de la ampliación IvSign Sniffer Tool. Si no dispones de una licencia o ha expirado, contacta con tu gestor de proyectos.
autoimportación	**-ai** : Activa la opción de autoimportación de certificados exportables instalados en local. **-aifcheck** -Comprueba que el certificado NO exista en IvSign para la autoimportación de certificados. **- aif: [Filtro1 | Filtro2 | FiltroN]** : Establece el filtro para la autoimportación de certificados. El filtro por defecto itera sobre el asunto del certificado, pero se pueden establecer otros atributos del certificado para filtrar, como: • **-aif:in=[string]** : Filtra sobre la propiedad IssuerName. • **-aif:fn=[string]** : Filtra sobre la propiedad FriendlyName. • **-aif:in=[string]|fn=[string]** : Filtra sobre ambas propiedades y lo selecciona si al menos una de ellas se cumple. **-configfile:[archivo]** : Este comando permite leer los parámetros de configuración de un fichero en lugar de incluirlos en la línea de comandos. De esta forma se pueden establecer configuraciones centralizadas y configurables sin redistribución del programa con nuevos parámetros. Para conocer el formato del fichero escriba el parámetro *-help:configFile* **-defpin:[pin]** : Permite especificar un pin específico para todos los certificados importados. Si este parámetro no se incluye, el pin por defecto de todos los certificados será *123456.* **-dai** : Elimina los certificados del almacén de Windows una vez finalizado el proceso de autoimportación a IvSign.

	-ivsignserver:[server] : Establece el servidor o entorno de IvSign sobre el que se realizará la autoimportación de certificados. • Servidor de producción: **-ivsignserver:ivsign.net** • Servidor de demo/pruebas: **-ivsignserver:demo.ivsign.net** **-l:[usuario]** : Establece el usuario para autenticarse en el servidor Ivsign. Si no se especifica, se utiliza autenticación integrada por defecto. **-p:[contraseña]** : Establece el password para autenticarse en el servidor IvSign, siempre y cuando se haya especificado previamente el parámetro -l. NOTA: Si no se introducen los parámetros -l y -p, el sistema utilizará autenticación integrada por defecto. **-logfile:[file]** : Define el archivo de salida para el log de la operación de autoimportación. Este parámetro permite la utilización de comodines como {USERNAME} o {COMPUTERNAME}. **-verbose** : Establece mayor nivel de información en el log **-testivsign** : Comprueba que la comunicación entre el equipo local y la plataforma IvSign seleccionada es correcta.
borrado	**-dc** : Activa la opción de borrado de los certificados exportables (para procesos posteriores a la autoimportación) sin password. No compatible con -ai. **-dcfcheck** -Comprueba que el certificado EXISTA en IvSign para autorizar el borrado físico. **-dcf: [Filtro1 | Filtro2 | Filtron]** : Establece el filtro para el borrado de certificados. El filtro por defecto itera sobre el asunto del certificado, pero se pueden establecer otros atributos del certificado para filtrar, como: • **-dcf:in=[string]** : Filtra sobre la propiedad IssuerName. • **-dcf:fn=[string]** : Filtra sobre la propiedad FriendlyName. • **-dcf:in=[string]|fn=[string]** : Filtra sobre ambas propiedades y lo selecciona si al menos una de ellas se cumple.

A continuación, se muestran algunos ejemplos para la autoimportación de certificados.

EJEMPLO 04: Comprobación de conectividad con autenticación **integrada**.

Autenticación **integrada**, utiliza el usuario de Windows como nombre de usuario para comprobar que hay conectividad con IvSign.

```
C:\Temp>ListCertificates.exe -lic:[id.licencia] -ivsignserver:ivsign.net -
testivsign
```

EJEMPLO 05: Comprobación de conectividad con autenticación **básica**.

Autenticación **básica**, utiliza el nombre de usuario (-l:) y la contraseña (-p:), en este caso para comprobar que hay conectividad con IvSign.

```
C:\Temp>ListCertificates.exe -lic:[id.licencia] -l:usuario1 -p:123456Abcd -
ivsignserver:ivsign.net -testivsign
```

EJEMPLO 06: Importación básica de certificados a IvSign.

El siguiente comando realiza las siguientes acciones:

- Importa los certificados instalados en local (solo aquellos que tengan la clave marcada como exportable).
- Utiliza autenticación integrada.
- Genera un documento *.txt* por cada equipo en el que se ejecuta el comando.

```
C:\Temp>ListCertificates.exe -lic:[id.licencia] -ai -logfile:C:\Temp\log-
{COMPUTERNAME}.txt -ivsignserver:ivsign.net
```

EJEMPLO 07: Importación de certificados con filtro.

El siguiente comando realiza las siguientes acciones:

- Busca el tag "TEXTO" en el campo asunto de los certificados instalados en los equipos y si lo encuentra lo importa a IvSign.
- Genera un documento *.txt* por cada equipo en el que se ejecuta el comando.

```
C:\Temp>ListCertificates.exe -lic:[id.licencia] -ai -aif:TEXTO -
logfile:C:\Temp\log-{COMPUTERNAME}.txt -ivsignserver:ivsign.net
```

EJEMPLO 08: Importación de certificados con borrado.

Una vez importados los certificados locales se procede a la eliminación de los certificados del almacén de Windows.

```
C:\Temp>ListCertificates.exe -lic:[id.licencia] -ai -dai -logfile:C:\Temp\log-
{COMPUTERNAME}.txt -ivsignserver:ivsign.net
```

EJEMPLO 09: Borrado local de certificados previamente importados con filtro con filtro (buscamos el tag "TEXTO" en el asunto de los certificados).

```
C:\Temp>ListCertificates.exe -lic:[id.licencia] -dc -dcfcheck -dcf:TEXTO -
logfile:C:\Temp\log-{COMPUTERNAME}.txt -ivsignserver:ivsign.net
```

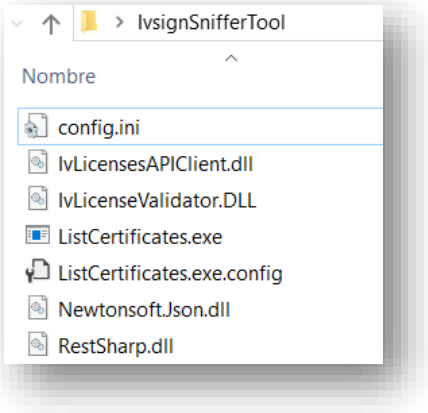
3. Distribución

Para la distribución masiva de *IvSign Sniffer Tool* dentro de la organización se recomienda utilizar Políticas de dominio.

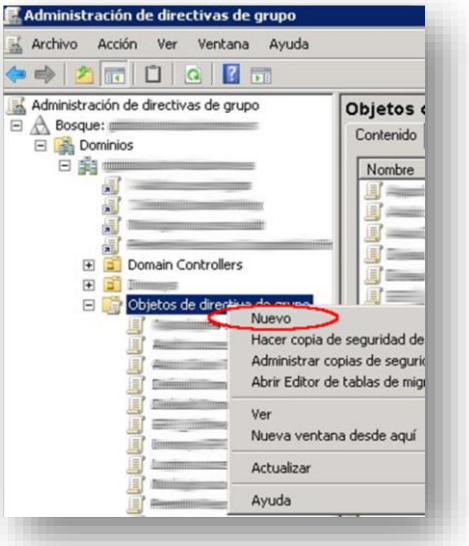
Pasos a seguir:

El primer paso consiste en habilitar un recurso compartido para permitir el almacenamiento de los ficheros obtenidos por la herramienta. Este recurso compartido debe estar accesible por todos los puestos, y con permisos para todos los usuarios.

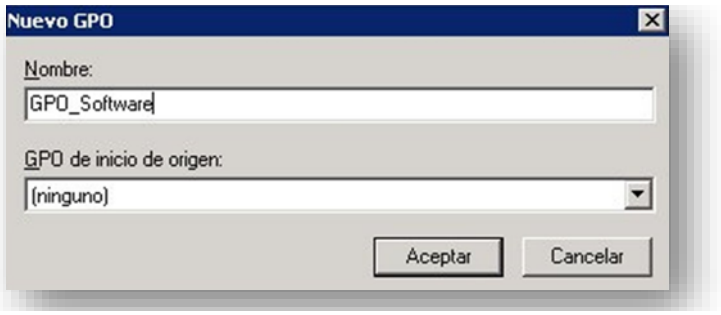
Seguidamente, crear el directorio *IvsignSnifferTool* e incluir el fichero *ListCertificates.exe*.



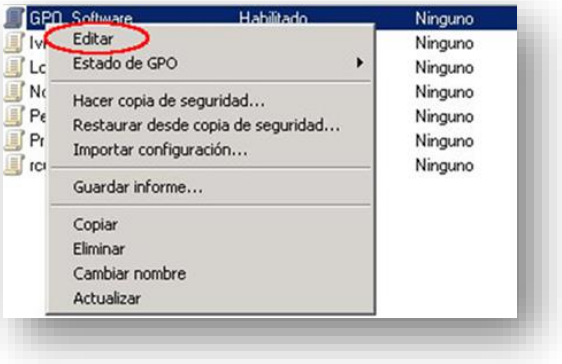
La directiva encargada de realizar la instalación desatendida se debe crear a través del Administrador de directivas de grupo. Para acceder a este panel, desde el controlador de dominio, se debe ejecutar el comando "gpmc".



Dentro de este panel, desplegando el dominio empleado, y en **Objetos de directiva de grupos**, se debe crear uno nuevo.

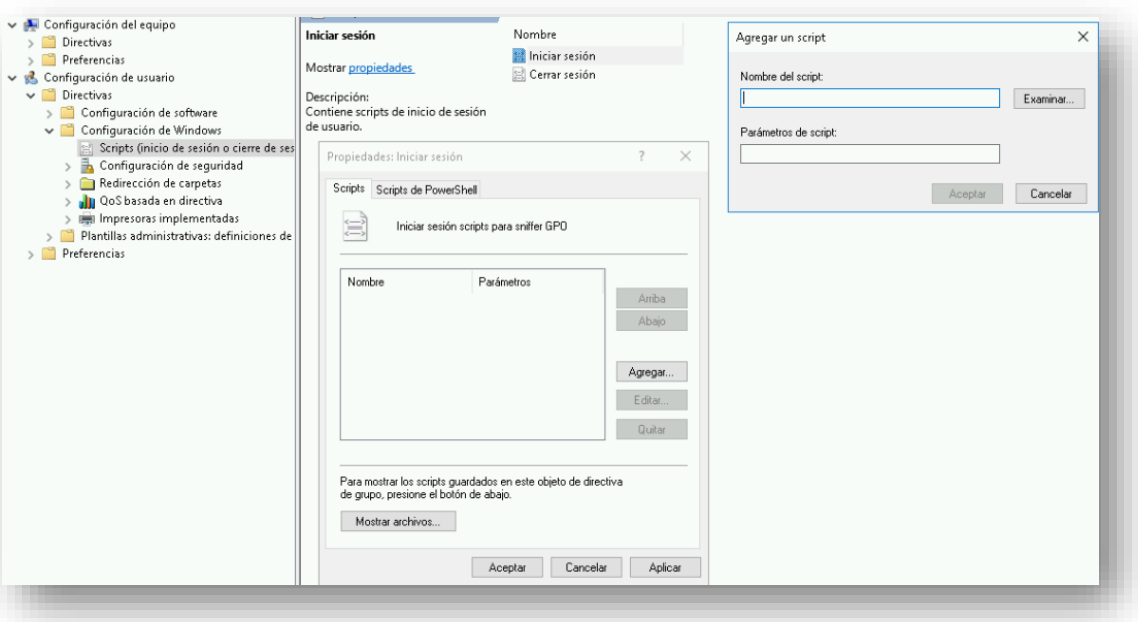


Edita la política creada.



En la nueva ventana, acceder a la siguiente ruta:

Configuración de usuario > Configuración de Windows > Scripts > Iniciar Sesión > *Agregar* un Script.



Ejemplo del script a cargar:

El script hace referencia a un archivo *.bat* con el siguiente código.

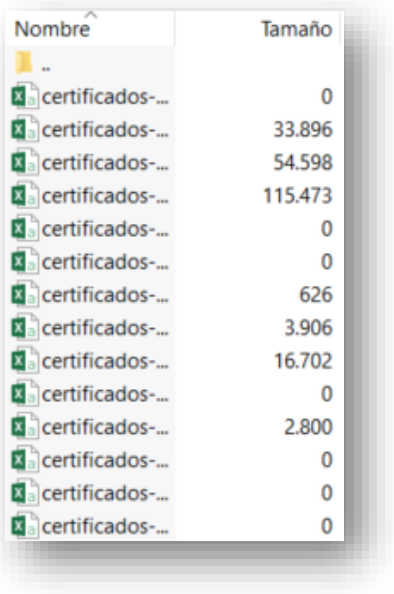
```
\\share\ListCertificates.exe -lic:[id.licencia] -csv -o:\\share\listing\certificados-
{COMPUTERNAME}-{USERNAME}.csv
```

Anotaciones:

- Las dos rutas especificadas requieren que el usuario que se utiliza para ejecutar el .exe tenga permisos de lectura y escritura sobre ellas.
- Los campos {COMPUTERNAME} y {USERNAME} se rellenan automáticamente.
- **NOTA:** Entre "–lic:" y el identificador de la licencia no tiene que haber ningún espacio. Ejemplo: -lic:xxxxxxxxxxx

Resultado esperado:

- Al ejecutar el comando en un único equipo aparecerá el siguiente mensaje que significa que se ejecutó correctamente: Código:ERR_SUCCESS
- Si el documento de salida está vacío, con solo la primera línea rellenada, dicho usuario no dispondrá de certificados instalados en el almacén local de certificados.
- El resultado final esperado comprende un conjunto de documentos (.csv), uno por cada usuario/equipo. Con dicho listado se podrá realizar un análisis de dichos certificados.



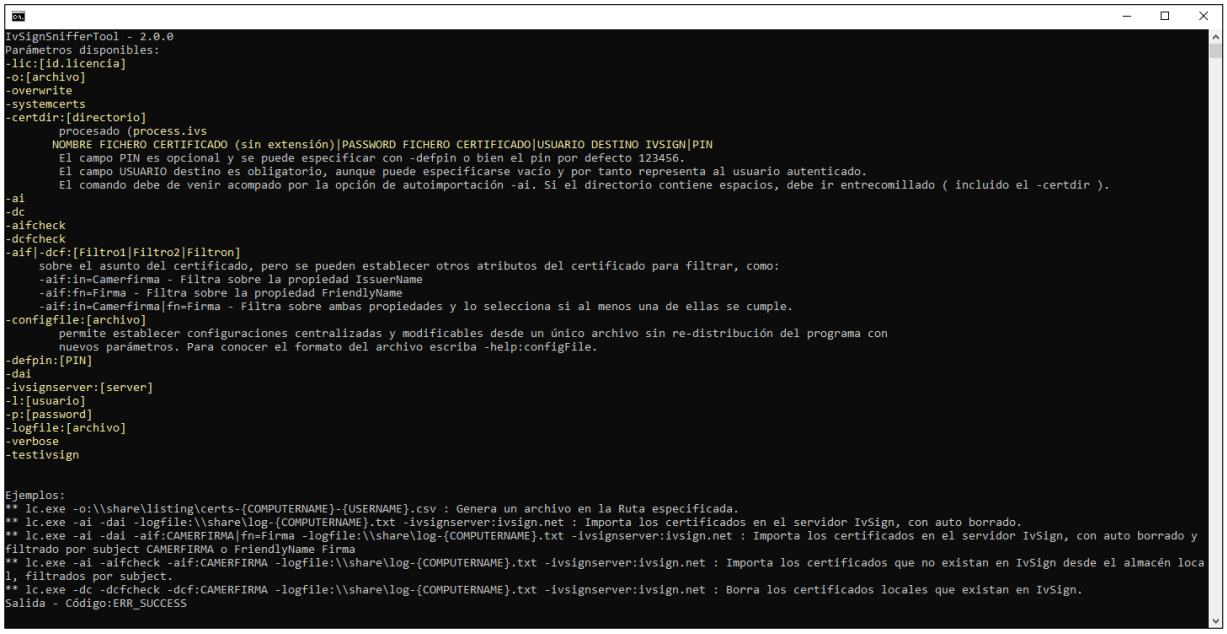
En caso de necesitar esta aplicación, deberá solicitar el código de licencia a su gestor de proyectos.

4. Consejos y ayuda

Antes de inicializar la operación de autoimportación verifique que existe conectividad entre el equipo y la plataforma de IvSign deseada, tal y como se indica en el **EJEMPLO 04**.

En caso de duda puede utilizar el comando **-help** para obtener información adicional sobre los parámetros disponibles y otros ejemplos de uso.

```
C:\Temp>ListCertificates.exe -lic:[id.licencia] -help
```



Anexo: Información de certificados detectados

El proceso de autodescubrimiento de *IvSign Sniffer Tool* permite obtener la lista de certificados instalados en un equipo cliente o puesto de trabajo, en formato CSV o XML.

A continuación, se incluye una breve descripción de los campos obtenidos por la herramienta para cada uno de los certificados.

Partimos de un ejemplo en el que se ha ejecutado la aplicación y esta ha obtenido 2 certificados, obteniendo el resultado en formato XML.

```
<?xml version=”2.0”?>
  <CertData>
    <CertGUID>c7dafc6d-55ee-41e0-ab99-2a49735427b9</CertGUID>
    <SN>055ª8C81F33195</SN>
    <Emisor>Tester User CA -</Emisor>
    <ValidoHasta>2029-02-16T10:05:10+00:00</ValidoHasta>
    <ValidoDesde>2019-02-17T10:05:10+00:00</ValidoDesde>
    <CN>prueba 2</CN>
    <IdNIFNIE>28254125V</IdNIFNIE>
    <O>Test S.L.</O>
    <OU>Ciudadanos</OU>
    <T />
    <Descripcion />
    <Huella>C88D4165900ACAF8FCEE7949D4CA0EAEBC73D257</Huella>
    <ClavePrivada>true</ClavePrivada>
    <Almacen>CurrentUser</Almacen>
    <CSPInfo>
        <CertGUID>c7dafc6d-55ee-41e0-ab99-2a49735427b9</CertGUID>
        <Proveedor>Microsoft Enhanced Cryptographic Provider v1.0</Proveedor>
        <Exportable>false</Exportable>
        <Protegido>false</Protegido>
        <Expulsable>false</Expulsable>
        <Hardware>false</Hardware>
    </CSPInfo>
    <UserInfo>
      <CertGUID>c7dafc6d-55ee-41e0-ab99-2a49735427b9</CertGUID>
      <NombrePC>EQUIPOPRUEBA-PC</NombrePC>
      <PlataformaPC>Win32NT</PlataformaPC>
      <PCOS>Microsoft Windows 10 Pro</PCOS>
      <NombreUsuario />
    </UserInfo>
  </CertData>
```

En base a la captura anterior, la información obtenida consiste en:

Información interna del certificado	
CertGUID	Código identificador cuando el certificado se instala en un equipo. En cada equipo que se instale el certificado varia dicho valor.
SN *(Serial number)*	Código interno generado por la Entidad emisora para identificar el certificado. Este código es único para los certificados emitidos por una misma CA.
Emisor	Nombre de la entidad emisora del certificado (o Autoridad de certificación).
ValidoHasta	Indica la fecha de caducidad del certificado.
ValidoDesde	Fecha de inicio de la validez del certificado.
CN *(Common Name)*	Nombre común o nombre distintivo del certificado. Se utiliza para aportar información adicional sobre la persona u organización para los que se emite el certificado.
IdNIFNIE	DNI del usuario.
O	Organización / Entidad / Compañía.
OU (*Organization Unit*)	Suele utilizarse para especificar la Unidad organizativa, Área o Departamento.
T	Suele utilizarse para especificar un cargo o función específica.
Descripcion	Descripción del certificado. Se utiliza para identificar fácilmente el tipo de certificado y su uso.
Huella	*String* o código correspondiente a la huella digital del certificado.
ClavePrivada	Clave privada del certificado.
Almacen	
Campos adicionales	
L (*Location*)	Localidad.
C (*Country*)	País.
Datos del CSP (Crypto Service Provider)	
Proveedor	Sistema que aprovisiona el certificado.
Exportable	Indica si el certificado está configurado como exportable.
Protegido	Indica si el certificado está protegido por un pin.
Expulsable	Se utiliza para certificados en formato Hardware (como DNI electrónico), para indicar si son extraíbles o no.
Hardware	Indica si el certificado está identificado como formato Hardware o no.
Información sobre el equipo y el usuario	
NombrePC	Nombre del equipo (puesto de trabajo).
PlataformaPC	Versión de la plataforma.
PCOS	Sistema operativo.
NombreUsuario	Usuario.