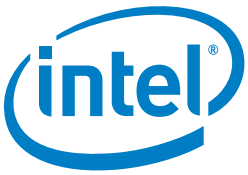


Intel® Authenticate

Guía de integración para Microsoft* System Center Configuration Manager (SCCM)

Versión 3.1

Fecha de publicación del documento: 27 de marzo de 2018

Renuncias de responsabilidad y avisos legales

El usuario no debe utilizar ni facilitar el uso de este documento en relación con ninguna infracción u otro análisis legal relativo a los productos Intel que se describen. El usuario acepta conceder a Intel una licencia no exclusiva libre de regalías a cualquier reivindicación de patente que se derive como borrador que incluya la materia que se da a conocer en el presente documento.

El presente documento no concede ninguna licencia (ni explícita ni implícita, por impedimento legal o por otro motivo) a ningún derecho de propiedad intelectual.

Los productos que se describen en él pueden contener defectos de diseño u errores conocidos como errores de dirección que pueden provocar que el producto difiera de las especificaciones publicadas. Los errores de dirección existentes están disponibles bajo petición.

Intel declina cualquier garantía, explícita o implícita, incluidas, entre otras, las garantías implícitas de comerciabilidad, idoneidad para un determinado fin y ausencia de infracción, así como cualquier garantía que se derive del rendimiento, la gestión o el uso comerciales.

Las funciones y ventajas de las tecnologías Intel dependen de la configuración del sistema y pueden requerir la habilitación de hardware o software o la activación de servicios. El rendimiento variará en función de la configuración del sistema. No hay ningún sistema informático que sea completamente seguro. Consulte con el vendedor o fabricante de su sistema o visite intel.es para más información.

Intel, Intel vPro, Intel Core, Xeon y el logotipo de Intel son marcas comerciales de Intel Corporation o de sus subsidiarias en Estados Unidos y/o en otros países.

*Otros nombres comerciales y marcas pueden ser reclamados como propiedad de terceros.

Microsoft, Windows y el logotipo de Windows son marcas comerciales o marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

Java es una marca registrada de Oracle y/o de sus empresas afiliadas.

La palabra Bluetooth® y sus logotipos son marcas registradas de Bluetooth SIG, Inc. y cualquier uso de estas marcas por parte de Intel se realiza bajo licencia.

Índice de contenido

1 Introducción

En este documento se describe cómo integrar y utilizar Intel® Authenticate con Microsoft System Center Configuration Manager (SCCM).

Nota:

Intel Authenticate también cuenta con paquetes de integración separados para utilizar al realizar la integración con:

- McAfee* ePolicy Orchestrator (ePO)
- Objetos directiva de grupo (GPO) de Active Directory

Para obtener información sobre cómo realizar la integración y el despliegue con ePO o GPO, consulte la documentación incluida en el paquete de integración correspondiente.

1.1 ¿Qué es Intel® Authenticate?

Intel Authenticate es una verdadera solución de autenticación de factores múltiples que admite tres categorías de factores de autenticación:

- Algo que el usuario sabe, como un número de identificación personal (código PIN)
- Algo que el usuario tiene, como un smartphone
- Algo único del usuario, como su huella digital

La frecuencia de los ataques en entornos empresariales está creciendo a un ritmo alarmante. El punto de partida para muchas infracciones de seguridad son unas credenciales de inicio de sesión peligrosas. Estos ataques tienen éxito porque la mayoría de los sistemas de autenticación almacenan y procesas los datos de autenticación en la capa de software. El proceso de comparación de los datos enviados por el usuario con los originales guardados puede ser vulnerable a ataques, modificaciones o supervisión cuando se realiza en el entorno del sistema operativo.

Intel Authenticate mejora la seguridad de los servicios y aplicaciones empresariales al reforzar los flujos y los factores de autenticación. Intel Authenticate admite factores de autenticación con distintos niveles de seguridad; los factores con el nivel más alto están "reforzados" y protegidos en el hardware de la plataforma Intel. De este modo, es más difícil que el malware y los atacantes accedan a sus datos de autenticación confidenciales o los manipulen.

Para cada acción permitida (consulte Acciones en la página 7), puede definir una combinación de factores de autenticación (consulte Factores de autenticación en la página siguiente) que puedan utilizar los usuarios finales.

Nota:

En sistemas que no sean Intel vPro, los conjuntos de factores están limitados a dos factores por conjunto. Por ejemplo, este conjunto de factores no está permitido: {Fingerprint AND Protected PIN AND Face Recognition}. La aplicación de una directiva que contenga más de dos factores en un conjunto de factores fallará en sistemas que no sean Intel vPro. Esta restricción no se aplica a sistemas Intel vPro. En sistemas Intel vPro, puede definir tantos factores por conjunto de factores como desee.

1.2 Factores de autenticación

En esta sección se describen los factores de autenticación que admite Intel Authenticate.

1.2.1 Proximidad® Bluetooth

Este factor permite al usuario registrar su smartphone personal o de empresa y utilizarlo como factor de autenticación. Todo el proceso de autenticación con el factor de Proximidad Bluetooth es automático y el usuario no debe hacer nada. Lo único que debe hacer es tener consigo el teléfono registrado cuando realice la acción.

Este factor tiene requisitos previos específicos (consulte Requisitos previos para la Proximidad Bluetooth en la página 21).

El nivel de seguridad de este factor depende del teléfono del usuario y la versión de Windows*.

Teléfono	Windows 7	Windows 10 versión 1607	Windows 10 versión 1703 y posteriores
Android*	Protegido	Protegido	Protegido
iPhone*	Protegido	Débil	Protegido (valor predeterminado) o Débil* **Nota:** En la versión 1703 o posteriores de Windows, puede que no resulte fácil configurar el nivel de seguridad "Protegido" con un iPhone. Para hacer esta combinación, deberá encontrar el equilibrio entre seguridad y facilidad de uso más adecuado para su organización.

Así es como funcionan los distintos niveles de seguridad:

- **Protegido**: el teléfono se registra en la plataforma del usuario utilizando un código secreto que solo comparten el teléfono y la plataforma. El código compartido se procesa y protege mediante el hardware de la plataforma Intel. Cuando el usuario realice una acción para la que se haya definido la Proximidad Bluetooth como factor de autenticación, Intel Authenticate enviará una comprobación de autenticación al teléfono. Si el teléfono está cerca, la comprobación se realizará correctamente y se aceptará el factor Proximidad Bluetooth. Este nivel de seguridad requiere que el usuario instale una pequeña aplicación en el teléfono (consulte Aplicación Intel Authenticate en la página 12).
- **Débil**: el teléfono se registra utilizando solo el emparejamiento de Bluetooth de Windows. Siempre y cuando el sistema operativo informe de que el teléfono está "Conectado", se aceptará el factor Proximidad de Bluetooth. Este nivel de seguridad no utiliza ninguna aplicación en el teléfono.

La directiva contiene dos entradas para este factor (solo necesita utilizar una).

- **Proximidad Bluetooth protegida**: seleccionar este factor implica que solo se podrá utilizar el nivel de seguridad "Protegido". Es decir, los usuarios con la versión 1607 de Windows 10 NO podrán registrar ni utilizar un iPhone con el factor de Proximidad Bluetooth.
- **Proximidad Bluetooth**: este factor permite los niveles de seguridad "Protegido" y "Débil" en todas las combinaciones de teléfono/sistema operativo del equipo (enumeradas en la tabla anterior). Para las versiones 1703 y posteriores de Windows 10, el valor predeterminado para los usuarios de iPhone es el nivel de seguridad "Protegido". Aun así, podrá cambiar el ajuste en la directiva para que el nivel de seguridad "Débil" sea el que esté activado en estas versiones de Windows cuando se utilice un iPhone.

Durante el registro, Intel Authenticate determina automáticamente qué nivel de seguridad se debe aplicar (en función de la configuración de las directivas que haya definido), así como el teléfono del usuario y el sistema operativo del equipo. A continuación, se guía al usuario a través de los pasos de registro necesarios.

Cambio del nivel de seguridad después del registro

En la versión 1703 y posteriores de Windows 10, se puede cambiar el nivel de seguridad del factor de Proximidad Bluetooth después de que el usuario haya registrado su teléfono. Para ello, deberá aplicar una nueva directiva con el nivel de seguridad requerido. Una vez aplicada la nueva directiva, la autenticación fallará cuando el usuario intente iniciar sesión en su teléfono. El usuario deberá iniciar sesión con un conjunto de factores alternativo o con su contraseña de Windows. Unos minutos después de iniciar sesión, se abrirá la aplicación de gestión de factores que mostrará un mensaje que indica que el usuario tiene que volver a registrar el teléfono. Después de hacerlo, la autenticación volverá a funcionar con el teléfono.

1.2.2 Reconocimiento facial

Este factor permite al usuario registrar su rostro y utilizarlo como factor de autenticación.

Este factor tiene requisitos previos específicos (consulte Requisitos previos para el reconocimiento facial en la página 23).

Nota:

Este factor no es un factor "endurecido" porque los datos biométricos del usuario suelen protegerse únicamente en el software. El nivel de protección depende del mecanismo de seguridad suministrado por el proveedor de la cámara.

1.2.3 Huella digital

Este factor permite al usuario registrar sus huellas digitales y utilizarlas como factor de autenticación.

Intel Authenticate admite dos tipos de lectores de huellas digitales.

- **Lectores de huellas digitales protegidas**: este tipo de lector de huellas digitales está diseñado para ser completamente independiente mediante la tecnología conocida como "Match on Chip". Los datos biométricos (la huella digital del usuario) se protegen y procesan en el chip del lector de huellas digitales. De este modo, es más difícil que los atacantes accedan a los datos de huella digital del usuario o los roben.
- **Lectores de huellas digitales ligeras**: este tipo de lector de huellas digitales es menos seguro porque los datos biométricos del usuario se suelen proteger únicamente en el software. El nivel de protección depende del mecanismo de seguridad suministrado por el proveedor del lector de huellas digitales. Este tipo de lector de huellas digitales no puede proporcionar el mismo nivel de protección que un lector de huellas digitales protegidas.

Este factor tiene requisitos previos específicos (véase Requisitos previos para Huella digital en la página 22).

1.2.4 Código PIN protegido

Este factor permite al usuario crear un número de identificación personal (código PIN) que utilizar como factor de autenticación. El código PIN se crea utilizando un teclado numérico protegido que se muestra mediante Intel® Identity Protection Technology con Protected Transaction Display (Intel IPT® con PTD). Estas son las principales funciones de seguridad de Intel IPT con PTD:

- El raspado de pantalla basado en software o los ataques de malware que tratan de realizar una captura de pantalla del teclado numérico no pueden ver la disposición del código PIN. Todo el teclado numérico está oculto.
- Cada vez que se muestra la ventana del teclado numérico, cambia el teclado numérico. Esto significa que las ubicaciones donde se hace clic con el ratón para introducir el código PIN cambian cada vez. No es posible capturar el patrón de clics del ratón para introducir el código PIN posteriormente.
- Los clics del ratón para la introducción del código PIN se traducen y utilizan en el hardware protector. El valor del código PIN real no se expone fuera del hardware.
- Un "mecanismo de regulación de códigos PIN" rastrea el número de intentos de introducción de código PIN incorrectos y en intervalos específicos rechazará los intentos de código PIN adicionales durante un periodo de tiempo específico. Esta función minimiza los ataques por fuerza bruta en el código PIN (consulte Mecanismo de regulación de códigos PIN en la página siguiente).
- No se permite introducir el código PIN con el teclado. Esta función minimiza los ataques mediante registro del teclado.

Nota:

Si se utilizan varios monitores, algunas configuraciones del sistema harán que el teclado numérico solo se muestre en uno de ellos y esté oculto en el resto. Con otras configuraciones, el teclado se muestra en todos los monitores. Esto no es un error, sino el comportamiento previsto.

1.2.4.1 Configuración del código PIN protegido

La configuración del código PIN protegido le permite definir los requisitos de complejidad para un código PIN válido. Al definir el factor de código PIN protegido en la directiva, puede definir estas opciones para el código PIN:

- **Longitud mínima del código PIN**: el número mínimo de dígitos que el usuario tiene que definir para su código PIN. Valores válidos: 4 – 10. El número de números secuenciales ascendentes que el usuario puede emplear en su código PIN está limitado a uno menos que el valor de esta opción. Por ejemplo, con un valor de 5, un código PIN de "12345" no es válido, pero un PIN de "12349" es válido.
- **Mínimo de dígitos exclusivos**: el número mínimo de dígitos exclusivos que el usuario tiene que definir para su código PIN. Valores válidos: 3 – 10. (El valor no puede ser superior al valor de Longitud mínima del código PIN).

1.2.4.2 Mecanismo de regulación de códigos PIN

El factor de autenticación de código PIN protegido tiene un mecanismo de regulación de códigos PIN integrado. Esto significa que cuando un usuario introduce un código PIN no válido, se inicia un contador de códigos PIN no válidos. Después de introducir un código PIN no válido una serie de veces, el sistema entrará en un modo en el que estará bloqueada la introducción de códigos PIN durante un periodo de tiempo específico. Cuando esté bloqueada, el usuario no podrá completar temporalmente ninguna acción para la que el factor de autenticación de código PIN protegido sea obligatorio. Esta función limita la eficacia de los ataques por fuerza bruta contra el código PIN de un usuario. Cuantos más intentos de código PIN no válido se realicen, mayor será el periodo de bloqueo de introducción de códigos PIN.

Número de intentos de código PIN incorrectos	Tiempo (en minutos) antes del próximo intento de código PIN
1 – 4	0
5 – 7	1
8 – 11	10
12 +	30

El contador de códigos PIN no válidos se restablecerá a cero una vez transcurridos 60 minutos desde el último intento de código PIN no válido.

Nota:

- El mecanismo de regulación de códigos PIN no admite contadores de códigos PIN no válidos separados para cada usuario. El mecanismo de regulación, cuando está activado, lo está para todos los usuarios. (Esto significa que todos los usuarios de la plataforma tendrán que esperar el tiempo requerido antes de poder introducir su código PIN).
- Al introducir un código PIN válido no se restablece el contador de códigos PIN a cero. Si el contador ya tenía un valor elevado (debido a varias introducciones de códigos PIN no válidos), las futuras introducciones de códigos PIN no válidos activarán el mecanismo antes de lo necesario.

1.2.5 Ubicación de Intel® AMT

Este factor utiliza la función Detección de entorno de la Tecnología de gestión activa Intel® (Intel® AMT). Las plataformas móviles normalmente funcionan en dos entornos de red distintos:

- Dentro de la red de la organización
- Fuera de la red de la organización; por ejemplo, utilizando puntos de acceso públicos y redes domésticas

La función Detección de entorno se utiliza para descubrir en qué tipo de red se está utilizando la plataforma. La función se activa configurando los nombres de sufijo de DNS de "dominios de inicio" en Intel AMT. Estos dominios de inicio son redes que se considera que son una parte de confianza de la red de la organización.

El factor de autenticación Ubicación de Intel AMT utiliza Detección de entorno para permitirle definir distintas directivas de autenticación en función de la ubicación de la plataforma. Normalmente, definirá que las acciones requieran un mayor número de factores de autenticación o factores más estrictos cuando la plataforma se encuentre fuera de la red de la organización.

Por ejemplo, puede definir una combinación de factores de autenticación como esta:

Ubicación de Intel AMT **Y** Proximidad Bluetooth

O

Código PIN protegido **Y** Proximidad Bluetooth

Esta combinación significa que cuando la plataforma funciona dentro de uno de los dominios de inicio, el único factor de autenticación requerido es el de proximidad Bluetooth. Pero cuando funciona fuera de los dominios de inicio, el usuario también tendrá que autenticarse utilizando el factor de código PIN protegido.

Este factor no requiere ninguna entrada por parte del usuario, pero sí que requiere algunos preparativos de configuración en la plataforma antes de poder utilizarse. Para obtener más información, consulte Requisitos previos para Ubicación de Intel AMT en la página 23.

Nota:

- Si la plataforma está conectada mediante WLAN pero no hay perfiles WLAN establecidos, el registro del factor Ubicación de Intel AMT siempre fallará.
- Normalmente, utilizará este factor junto con otros factores. Utilizar este factor como factor de autenticación único realmente significa que el flujo de autenticación solo será posible si la plataforma está ubicada dentro de la red de su organización.
- Si el usuario se conecta a la red de la organización mediante una conexión VPN, el factor Ubicación de Intel AMT considerará que la plataforma se encuentra fuera de la red de la organización.

1.3 Acciones

En esta sección se describen las acciones que admite Intel Authenticate.

> **Nota:**
>
> Para la mayoría de las acciones, es posible definir múltiples factores de autenticación. Más factores implican más seguridad, pero normalmente reducen la capacidad de uso de los usuarios finales. Al definir el número y el tipo de factores de cada acción, debe equilibrar los requisitos de seguridad de la organización con la experiencia del usuario.

1.3.1 Inicio de sesión de SO

Esta acción permite a los usuarios iniciar sesión en el sistema operativo Windows utilizando Intel Authenticate en lugar de su contraseña de Windows. Durante el inicio de sesión, se muestra una indicación visual en la pantalla de inicio de sesión de Windows que advierte al usuario de que puede utilizarse Intel Authenticate para iniciar sesión. A continuación, el usuario puede pulsar Entrar para iniciar sesión en Windows utilizando los factores de autenticación definidos. No se pedirá al usuario que proporcione su contraseña de Windows.

> **Nota:**
>
> NO se admite la opción "No mostrar el último nombre de usuario" en la configuración de directiva de grupo. NO active esta opción de configuración.

Durante el inicio de sesión, se verifican los factores de Intel Authenticate definidos para el inicio de sesión en el SO. Si son correctos, Intel Authenticate emite las credenciales para completar el proceso de inicio de sesión en Windows. Si la plataforma está conectada a un dominio, el usuario también iniciará sesión automáticamente en el dominio. Windows se encarga de la conexión con el dominio, incluidos los servicios conectados, tales como Autenticación de Windows integrada (IWA) y Servicios de federación de Active Directory (ADFS).

Puede definir el tipo de credenciales que Intel Authenticate emite para Windows.

- **Contraseña de Windows del usuario**: es el tipo predeterminado.
- **Una tarjeta inteligente virtual**: cuando se activa esta opción, el proceso de inicio de sesión se lleva a cabo mediante un certificado. El certificado se genera y protege en el hardware de la plataforma Intel utilizando Intel® Identity Protection Technology con infraestructura de clave pública (Intel® IPT con PKI). Si la autenticación de los factores es correcta, Intel Authenticate desbloquea el certificado para que Windows complete el proceso de inicio de sesión. El uso de esta opción puede reducir la utilización de contraseñas de Windows en su entorno al mínimo. Esta opción requiere configuración adicional (consulte Configuración del inicio de sesión con tarjeta inteligente en la página 35).

Al activar con contraseña la acción de inicio de sesión en SO, Intel Authenticate debe guardar la contraseña de Windows del usuario. Esto significa que, cuando no se utiliza la opción de tarjeta inteligente, el primer inicio de sesión después del registro se debe realizar utilizando la contraseña de Windows. A continuación, el usuario puede empezar a iniciar sesión utilizando Intel Authenticate.

1.3.1.1 Bloqueo de la contraseña de Windows*

Para reducir las posibilidades de que los usuarios intenten evitar los requisitos establecidos para iniciar sesión en el SO con Intel Authenticate, dispone de tres opciones diferentes. (Implemente solo una opción).

Nota:

En las opciones 1 y 2, tras completar la autenticación, la contraseña de Windows es la que se sigue enviando a Windows para completar el proceso de inicio de sesión.

Opción 1: Aumentar la complejidad de la contraseña de Windows

Para disuadir a los usuarios del uso de su contraseña de Windows, puede aumentar la complejidad de los requisitos de la contraseña de Windows. Cuando los usuarios deban recordar e introducir una contraseña larga y compleja, la mayoría simplemente optará por utilizar Intel Authenticate para iniciar sesión.

Opción 2: Bloquear la contraseña en la directiva

Esta opción obliga al usuario a iniciar sesión usando los factores de Intel Authenticate que se han definido en la directiva. Para activar esta opción, en la directiva de Intel Authenticate, seleccione la opción: **Impedir que el usuario utilice su contraseña de Windows para iniciar sesión**.

Si selecciona esta opción, cuando un usuario inicie sesión correctamente con Intel Authenticate, se desactivará la opción para iniciar sesión con su contraseña de Windows. En su lugar, se mostrará un mensaje informando al usuario de que el departamento de TI ha desactivado el inicio de sesión mediante la contraseña de Windows.

Nota:

En determinadas condiciones, Intel Authenticate seguirá permitiendo que el usuario inicie sesión con su contraseña de Windows:

- Si Intel Authenticate detecta que hay un error en el sistema o algún otro problema que impida al usuario iniciar sesión con Intel Authenticate.
- Si Intel Authenticate detecta que no posee la contraseña de Windows del usuario guardada en el almacén de datos seguro. (Por ejemplo, el usuario ha cambiado su contraseña o la contraseña ha caducado).

Opción 3: Utilizar la opción de tarjeta inteligente y bloquear la contraseña en Active Directory

Esta es la opción más segura. Si esta opción está totalmente activada, la contraseña de Windows no se utilizará nunca. Para activar esta opción:

1. Active la opción de tarjeta inteligente de inicio de sesión de SO (consulte Configuración del inicio de sesión con tarjeta inteligente en la página 35).
2. Asegúrese de que los usuarios hayan registrado correctamente sus factores y puedan iniciar sesión con Intel Authenticate y un certificado de tarjeta inteligente.
3. En las propiedades de la cuenta de usuario de Active Directory, seleccione la opción: **Se necesita una tarjeta inteligente para un inicio de sesión interactivo**.

Nota:

Si esta opción está activada, el usuario seguirá viendo la opción de iniciar sesión con una contraseña de Windows. Pero, si intenta iniciar sesión con una contraseña, se muestra un mensaje de error como este: **Debe utilizar una tarjeta inteligente para iniciar sesión**.

1.3.2 Inicio de sesión en VPN

Esta acción permite a los usuarios iniciar sesión en la red privada virtual (VPN) de su organización utilizando los factores de autenticación admitidos por Intel Authenticate. Debe configurar el cliente VPN para que utilice un certificado para la autenticación, en lugar de una contraseña. El certificado se genera y protege en el hardware de la plataforma Intel utilizando Intel® Identity Protection Technology con infraestructura de clave pública (Intel® IPT con PKI). Durante el inicio de sesión, se verifican los factores de Intel Authenticate definidos para el inicio de sesión en VPN. Si la verificación se completa correctamente, Intel Authenticate desbloquea el certificado y lo transmite al cliente VPN para iniciar sesión en la VPN.

Antes de poder utilizar esta acción, tiene que configurar los sistemas cliente y el punto de acceso VPN. Para obtener más información, consulte Configuración del inicio de sesión en VPN en la página 26.

1.3.3 Bloqueo por distancia

Cuando esta función está activada y el teléfono registrado no está cerca (es decir, el usuario "se ha ido" con su teléfono), la estación de trabajo se bloquea automáticamente. Cuando el usuario vuelve a su estación de trabajo, será necesario volver a iniciar la sesión utilizando Intel Authenticate. Cuando define el bloqueo por distancia, también define un periodo de gracia durante el cual no se produce el bloqueo si el usuario vuelve a su estación de trabajo.

Esta función depende de la precisión con la que el teléfono o el sistema operativo informen de que el teléfono ha salido del rango. El nivel de precisión puede diferir entre los distintos modelos de teléfono. Además, puede haber bloqueos erróneos en función de donde esté el teléfono (por ejemplo, si lo lleva en el bolsillo el usuario). Para minimizar los bloqueos erróneos, antes de bloquear el equipo todas las pantallas se atenúan durante 7 segundos. Si el usuario mueve el ratón o utiliza el teclado durante esos 7 segundos, la pantalla no se bloquea y el bloqueo por distancia se desactiva temporalmente. Cuando se restablece la conexión con el teléfono, el bloqueo por distancia se vuelve a activar.

Nota:

- El bloqueo por distancia no sustituye el bloqueo de estaciones de trabajo inactivas tras un período de tiempo mediante directivas de TI.
- El bloqueo por distancia se activa mediante el factor Proximidad Bluetooth (véase Proximidad® Bluetooth en la página 2).
- El bloqueo por distancia solo está disponible si las acciones "inicio de sesión de SO" o "inicio de sesión de VPN" están activadas en la directiva.

1.4 Componentes de Intel Authenticate

En esta sección se describen los componentes principales que utiliza Intel Authenticate.

1.4.1 Client y Engine

El software de Intel Authenticate se instala en estas ubicaciones en la plataforma cliente:

- `C:\Program Files\Intel\Intel Authenticate`
- `C:\Program Files (x86)\Intel\Intel Authenticate`

Los componentes de software en la plataforma cliente se dividen en dos niveles lógicos: "Client" (cliente) y "Engine" (motor). Cada conjunto de componentes se instala en una subcarpeta con el mismo nombre (Client y Engine).

En la plataforma cliente, Intel Authenticate utiliza dos servicios, descritos en esta tabla.

Nombre para mostrar del servicio	Descripción
Intel Authenticate: Client	Este servicio controla principalmente las tareas en el nivel del sistema operativo. Esto incluye las comunicaciones con la aplicación de gestión de factores (consulte Aplicación de gestión de factores en la página siguiente).
Intel Authenticate: Engine	Este servicio controla principalmente las tareas que requieren comunicaciones con applets de software en el firmware de la plataforma. Intel Authenticate instala y utiliza varios applets en Intel Dynamic Application Loader (Intel DAL). Además, este servicio también gestiona las conexiones Bluetooth utilizadas por Intel Authenticate.
Nota: ambos servicios deben estar en ejecución para que Intel Authenticate funcione correctamente.	

1.4.2 Directivas

Las directivas contienen la configuración de Intel Authenticate que desea implementar en la plataforma cliente. Esto incluye las acciones que desea activar y la combinación de factores de autenticación que desea definir para cada acción. El método utilizado para crear y desplegar la directiva dependerá de la opción de integración que decida utilizar (SCCM, GPO, ePO). Una vez creada la directiva, esta se despliega y se implementa en las plataformas cliente. A continuación, el usuario tiene que registrar los factores de autenticación definidos en la directiva implementada (consulte Aplicación de gestión de factores abajo).

Cada plataforma cliente solo puede tener una directiva. No obstante, puede reemplazar y volver a implementar directivas tan a menudo como sea necesario cuando sus requisitos cambien.

Nota:

Las directivas están protegidas por un certificado de firma (consulte Preparación de un certificado de firma digital). Solo puede sustituir una directiva si la nueva directiva está firmada con el mismo certificado que se usó para firmar la directiva existente en la plataforma. Si desea utilizar un certificado de firma diferente, primero debe restablecer (eliminar) la directiva existente antes de poder establecer la nueva directiva.

1.4.3 Aplicación de gestión de factores

Poco después de la implementación de la directiva, la aplicación de gestión de factores se abre automáticamente en la plataforma cliente. Esta aplicación es un asistente sencillo que guía al usuario final por el proceso de registro de los factores de autenticación. Una vez completado el registro, el usuario puede empezar a utilizar las funciones de Intel Authenticate, de acuerdo con la configuración definida en la directiva. El usuario no puede cambiar los parámetros de la directiva que se ha implementado.

Tras el registro, el usuario también puede abrir la aplicación de gestión de factores en cualquier momento y utilizarla para administrar (volver a registrar) sus factores registrados. Por ejemplo, es posible cambiar el código PIN protegido o el teléfono que se utiliza para el factor Proximidad Bluetooth. Para volver a registrar un factor, el usuario debe autenticarse primero. Por ejemplo, para cambiar su PIN, el usuario debe proporcionar su PIN original. Y para cambiar su teléfono, debe autenticarse con el teléfono actualmente registrado.

Nota:

- La aplicación de gestión de factores es dinámica y muestra pantallas e instrucciones de acuerdo con la configuración de la directiva implementada. El proceso de registro es muy sencillo y solo dura unos minutos. No obstante, se recomienda familiarizarse con el flujo antes de desplegarlo en los usuarios finales. Para comprender mejor el flujo, véase la guía de registro situada en la carpeta raíz de este paquete de instalación.
- Se necesita una resolución de pantalla mínima de 1024 x 768 para utilizar la aplicación Factor Management (las resoluciones inferiores no son compatibles).

1.4.4 Aplicación Intel Authenticate

El factor Proximidad Bluetooth requiere que el usuario instale una pequeña aplicación en el teléfono con el que se desee utilizar Intel Authenticate.

Nota:

Con el nivel de seguridad "Débil" del factor de Proximidad Bluetooth no hace falta la aplicación. Es decir, durante el registro, no se pedirá a los usuarios que instalen la aplicación ni que introduzcan un código. Para obtener más información, consulte Proximidad® Bluetooth en la página 2.

Las aplicaciones se publican en Google Play (para teléfonos Android) y en App Store (para iPhones):

- App Store: https://itunes.apple.com/app/intel-authenticate/id1171157350
- Google Play: https://play.google.com/store/apps/details?id=com.intel.auth13217

La aplicación de gestión de factores incluye botones de descarga en la página Proximidad Bluetooth. Se le pedirá al usuario que descargue e instale la aplicación Intel Authenticate directamente en su teléfono como parte de los procesos de registro. Si lo prefiere, puede enviar los vínculos anteriores a sus usuarios y pedirles que instalen la aplicación relevante en su teléfono antes del proceso de registro en sí.

Nota:

- En los teléfonos Android, la aplicación se ejecuta como servicio en segundo plano. De forma predeterminada, muchos teléfonos Android impiden que los servicios en segundo plano se inicien automáticamente. En estos teléfonos, el usuario tendrá que permitir manualmente el inicio automático de la aplicación de Intel Authenticate. (Si la aplicación no se ejecuta en segundo plano, la verificación de Proximidad Bluetooth fallará).
- En teléfonos iPhone, el usuario debe asegurarse de no cerrar la aplicación. Además, una vez que se reinicia el teléfono, será necesario abrir manualmente la aplicación.

1.5 Cómo funciona la integración con Microsoft SCCM

La integración con SCCM requiere varios componentes de Intel® Setup and Configuration Software (Intel® SCS) y dos complementos de Intel Authenticate.

Nota:

Los componentes necesarios de Intel SCS se suministran en este paquete de integración y están listos para su uso. Si aparecen nuevas versiones, estarán disponibles en el sitio web de Intel SCS.

En esta tabla se describen los componentes de Intel SCS utilizados para integrar Intel Authenticate con SCCM.

Componente	Descripción
Complemento de Intel® SCS para Microsoft* SCCM (Denominado "complemento" en esta guía)	• Nombre de archivo: `SCCMAddon.exe` • Versión admitida: 2.1.8 y posteriores • Ubicación en el paquete: `Intel_SCS_Components > IntelSCS_SCCMAddon > SCCMAddon` • Finalidad: un asistente de configuración que crea recopilaciones, despliegues, paquetes y secuencias de tareas en SCCM. Cada uno de los elementos que crea el complemento en SCCM se configura previamente de forma automática. **Nota:** • Las recopilaciones, los despliegues, los paquetes y las secuencias de tareas creadas por el complemento son un "punto de partida". Son ejemplos operativos que se pueden utilizar para integrar rápidamente Intel Authenticate en SCCM. Puede utilizar los elementos creados por el complemento en SCCM tal cual o como base a partir de la cual aprender y avanzar. Para obtener más detalles, consulte ¿Qué crea el complemento en SCCM? en la página 15 • El complemento incluye muchas opciones adicionales. Por ejemplo, puede usar el complemento para agregar compatibilidad con Intel AMT, así como para la integración con el servicio de configuración remota de Intel SCS. Dichas opciones quedan fuera del ámbito de esta guía. Para obtener información detallada sobre el complemento, consulte la documentación suministrada con él.
Utilidad Platform Discovery	• Nombre de archivo: `PlatformDiscovery.exe` • Versión admitida: 11.0.0.81 o posterior • Ubicación en el paquete: `Intel_SCS_Components > Platform_Discovery` • Finalidad: descubre los productos y las capacidades de Intel que existen en las plataformas, incluido Intel Authenticate. Al ejecutar el complemento, seleccione este componente y el complemento creará las secuencias de tareas y los paquetes utilizados para descubrir qué plataformas admiten Intel Authenticate.

Componente	Descripción
Todas las plataformas en las que no está instalado Host Solution Manager	• Nombre de archivo: `HostSolutionManagerInstaller.msi` • Versión admitida: 10.0.20 y posteriores • Ubicación en el paquete: `Intel_SCS_Components > Intel_SCS_Framework > Framework` • Finalidad: presenta una API que emplea WMI (Instrumental de administración de Windows). Esta API es el punto de acceso para el complemento de host de Intel Authenticate (véase la tabla siguiente) y se debe instalar en las plataformas cliente. Al ejecutar el complemento, seleccione este elemento y el complemento creará las secuencias de tareas y los paquetes utilizados para instalarlo.
Complemento de Profile Editor	• Nombre de archivo: `ProfileEditor.exe` • Versión admitida: 10.0.20 y posteriores • Ubicación en el paquete: `Intel_SCS_Components > Intel_SCS_Framework > Profile Editor` • Finalidad: una interfaz gráfica de usuario autónoma que permite crear y editar perfiles de configuración, así como guardarlos en archivos XML. Cuando se inicia Profile Editor, busca en la subcarpeta `Plugins` los complementos de Profile Editor. Por cada complemento encontrado (y validado), se muestra un editor de complementos.

En esta tabla se describen los complementos de Intel Authenticate.

Tipo de complemento	Detalles
Complemento de host	• Nombre de archivo: `AuthenticatePlugin.dll` • Ubicación en el paquete: `HostPluginInstaller` • Finalidad: gestiona las solicitudes de configuración y otras comunicaciones con Intel Authenticate en la plataforma cliente. Este complemento se debe instalar en las plataformas cliente. Al ejecutar el complemento, seleccione este componente y el complemento creará las secuencias de tareas y los paquetes utilizados para instalar el componente. El complemento de host se debe "registrar" con el componente Host Solution Manager (véase la tabla anterior). Host Solution Manager utiliza el Registro para buscar los complementos. El instalador msi del complemento agrega automáticamente la clave de registro durante la instalación.

Tipo de complemento	Detalles
Complemento de Profile Editor	• Nombre del archivo: `AuthenticateProfileEditor.dll` • Ubicación en el paquete: previamente instalado en la instancia de Profile Editor proporcionada en este paquete • Finalidad: se utiliza para crear los perfiles de configuración (directivas) correspondientes a Intel Authenticate. Este complemento se utiliza en el equipo donde decida ejecutar el componente Profile Editor de Intel SCS. **Nota:** El complemento incluye ayuda con información sobre las opciones de configuración disponibles en las directivas de Intel Authenticate. Para abrir la ayuda, haga clic en el icono de ayuda del complemento en Profile Editor.

1.5.1 ¿Qué crea el complemento en SCCM?

En las tablas de esta sección se describen los elementos que crea el complemento en SCCM en función del procedimiento indicado en Instalación del complemento en la página 49.

Recopilaciones

Nombre	Reglas de pertenencia
Intel SCS: Platform Discovery	Todas las plataformas con sistema operativo de Microsoft
Intel Authenticate: Exists	Todas las plataformas que satisfacen los requisitos previos de hardware y firmware necesarios para permitir la instalación de Intel Authenticate **Nota:** El complemento también crea recopilaciones "Exists" adicionales para otros productos de Intel (no se indican aquí porque no son relevantes para la integración con Intel Authenticate).
Intel SCS: Solutions Framework Not Installed	Todas las plataformas en las que no está instalado Host Solution Manager
Intel SCS: Solutions Framework Installed	Todas las plataformas en las que ya está instalado Host Solution Manager
Intel Authenticate: Plugin Not Installed.	Todas las plataformas en las que el complemento de host de Intel Authenticate no está instalado
Intel Authenticate: Plugin Available	Todas las plataformas en las que el complemento de host de Intel Authenticate ya está instalado
Intel Authenticate: Managed	Todas las plataformas en las que el complemento de host de Intel Authenticate ya está instalado y funcionando correctamente

Secuencias de tareas (y despliegues)

De forma predeterminada, las secuencias de tareas están desactivadas (consulte Activación de las secuencias de tareas (en orden) en la página 58).

Nombre	Descripción
Intel SCS: Platform Discovery	Se ejecuta en la recopilación "Intel SCS: Platform Discovery" para descubrir los productos de Intel que admite cada plataforma. Los datos se envían a la base de datos de SCCM y se emplean para rellenar las recopilaciones de tipo "Exists" de los productos compatibles. (La recopilación "Intel Authenticate: Exists" tiene interés en nuestro caso).
Intel SCS: Solutions Framework Installation	Se ejecuta en la recopilación "Intel SCS: Solutions Framework Not Installed" para instalar Host Solution Manager en las plataformas
Intel Authenticate: Installation	Se ejecuta en la recopilación "Intel Authenticate: Plugin Not Installed" para instalar el complemento de host de Intel Authenticate en las plataformas **Nota:** Esta secuencia de tareas no instala los componentes de software de Intel Authenticate. Esto significa que deberá crear una secuencia de tareas y un paquete en SCCM para instalar el software (consulte Creación de un paquete de instalación del cliente en la página 53).
Intel Authenticate: Configuration	Se ejecuta en la recopilación "Intel Authenticate: Plugin Available" para implementar la directiva de Intel Authenticate en las plataformas
Intel Authenticate: Unconfigure	Se ejecuta en la recopilación "Intel Authenticate: Managed" para eliminar la configuración de directiva de Intel Authenticate de las plataformas

Paquetes

Nombre	Descripción
Intel SCS: Platform Discovery	Utilizado por la secuencia de tareas "Intel SCS: Platform Discovery". El origen de datos es una carpeta llamada "Platform Discovery" que contiene la utilidad Platform Discovery y scripts para ejecutarla.
Intel SCS: Solutions Framework	Utilizado por la secuencia de tareas "Intel SCS: Solutions Framework Installation". El origen de datos es una carpeta llamada "Solutions Framework" que contiene el instalador de Host Solution Manager.

Nombre	Descripción
Intel Authenticate: Installation	Utilizado por la secuencia de tareas "Intel Authenticate: Installation". El origen de datos es una carpeta llamada "Intel Authenticate Installation" que contiene el instalador del complemento de host de Intel Authenticate.
Intel Authenticate: Actions	Utilizado por las secuencias de tareas "Intel Authenticate: Configuration" e "Intel Authenticate: Unconfigure". El origen de datos es una carpeta llamada "Intel Authenticate Actions" que contiene los scripts de PowerShell empleados por las secuencias de tareas.
Nota: Las carpetas que actúan como origen de datos fueron creadas automáticamente por el complemento en la carpeta principal definida en el complemento durante la instalación.	

2 Requisitos previos de la plataforma cliente

En esta sección se describen los requisitos previos para Intel Authenticate en las plataformas cliente.

Nota:

- Las versiones que se muestran en esta sección son las versiones mínimas que son compatibles. No obstante, a menos que se indique lo contrario, siempre es recomendable usar la última versión para cada requisito.
- Puede utilizar la herramienta de comprobación para determinar si una plataforma satisface los requisitos previos (consulte Utilización de la herramienta de comprobación en la página 74).

2.1 Requisitos previos para la instalación

En esta tabla se describen los requisitos mínimos para instalar Intel Authenticate en las plataformas cliente.

Requisito previo	Detalles
Procesador	La plataforma debe contar con un procesador de 6ª generación (o posterior) que pertenezca a una de estas familias de procesadores: • Intel® Core™ • Intel® Core™ M • Intel® Core™ vPro™ • Intel® Core™ M vPro™ • Intel® Xeon® E3 (versión 5 o posterior)
Firmware de Intel ME	SKU corporativo del firmware de Intel Management Engine: • Intel ME 11.8: versión 11.8.50.3399 o posterior • Intel ME 11.7 • Intel ME 11.6: versión 11.6.0.1117 o posterior • Intel ME 11.0: versión 11.0.0.1157 o posterior (la versión 11.0.0.1202 es la versión mínima para las plataformas que tienen el servicio de Sensor de Intel activado) **Nota:** • De forma predeterminada, la instalación se bloquea en cualquier Firmware de Intel ME con una versión anterior a la 11.8.50.3399 (consulte Versión mínima de Firmware de Intel ME en la página 20). • El SKU de consumidor NO es compatible.

Requisito previo	Detalles
Software Intel ME	Software de Intel Management Engine versión 11.6.0.1019 o posterior. El instalador del software Intel ME instala automáticamente varios componentes. Estos son los componentes principales necesarios y utilizados por Intel Authenticate: • Controlador de Intel Management Engine Interface (Intel MEI) • Dynamic Application Loader de Intel (Intel DAL) • El servicio Java Host Interface (JHI)

Sistema operativo	• Windows* 10, versión 1709 (64 bits):
	  • Versión mínima: 10.0.16299.125
	• Windows* 10, versión 1703 (64 bits):
	  • Versión mínima: 10.0.15063.540
	• Windows* 10, versión 1607 (64 bits):
	  • Versión mínima: 10.0.14393.222
	• Windows* 7 (32 y 64 bits)
	Nota: En el caso de Windows 7*, son necesarias las siguientes correcciones:
	• KB2921916: si no está instalada, la instalación silenciosa fallará.
	• KB3033929: si no está instalada, la opción de tarjeta inteligente no funcionará.
	• KB2863706: si no está instalada, la autenticación mediante Huella digital ligera no funcionará.

Gráficos integrados	Debe tener instalada la versión 21.20.16.4481 o posterior del controlador de Intel HD Graphics. **Nota:** algunas funciones de Intel Authenticate se basan en las prestaciones proporcionadas por Intel IPT con Protected Transaction Display. Estas prestaciones requieren una CPU Intel con gráficos integrados. En algunas plataformas que también cuentan con gráficos discretos, se puede activar una función de gráficos intercambiable. Intel Authenticate solo admite la función de gráficos intercambiables si el controlador de gráficos discretos puede transferir automáticamente la propiedad a los gráficos integrados cuando se requiere Intel IPT con PTD.
Transport Layer Security	El protocolo Transport Layer Security (TLS) debe estar activado
.NET Framework	La aplicación de gestión de factores requiere .NET Framework versión 4.5.2 o superior

2.1.1 Versión mínima de Firmware de Intel ME

De forma predeterminada, la instalación se bloquea en cualquier Firmware de Intel ME con una versión anterior a la 11.8.50.3399.

Si se instala Intel Authenticate en versiones anteriores, los datos almacenados en el Firmware de Intel ME serán potencialmente vulnerables. Esto incluye datos de registro, como son el código PIN protegido, la contraseña de Windows y las claves PKI. Para instalar Intel Authenticate en versiones anteriores de Firmware de Intel ME compatibles, necesitará utilizar un indicador de instalación especial denominado `ByPassMEFirmwareCheck`.

Nota:

- Por razones de seguridad, se recomienda actualizar las versiones anteriores del Firmware de Intel ME a la versión 11.8.50.3399 o posterior. Para obtener más información, consulte el comunicado oficial aquí.
- En equipos donde Intel Authenticate ya esté instalado, la actualización del Firmware de Intel ME a la versión 11.8.50.3399 o posterior hará que el programa se detenga. Para volver a activarlo, tendrá que restablecer Intel Authenticate y establecer la directiva de nuevo. Además, los usuarios finales tendrán que volver a registrar sus factores. (Para restablecer Intel Authenticate, utilice la secuencia de tareas `Intel Authenticate: Unconfigure`).

Esta tabla describe el indicador `ByPassMEFirmwareCheck`.

Marca	Detalles
`BypassMEFirmwareCheck`	Valores válidos: • **0**: es el valor predeterminado. Intel Authenticate solo se instalará si se detecta la versión 11.8.50.3399 o una posterior. (La actualización desde versiones anteriores de Intel Authenticate también se bloqueará en plataformas con una versión anterior a la 11.8.50.3399). • **1**: este valor indica que Intel Authenticate también se instalará o actualizará en cualquier versión de Firmware de Intel ME compatible (aunque sea menos segura).

Si desea cambiar el valor predeterminado, debe hacerlo en el archivo `Install_IA.ps1` (que se encuentra en la carpeta `AuthenticateInstallers`).

2.2 Requisitos previos para la Proximidad Bluetooth

El factor Proximidad Bluetooth requiere una tarjeta inalámbrica Intel con Bluetooth integrado en la plataforma y un smartphone. El smartphone puede ser el teléfono personal o de empresa del usuario; tanto Android como iPhone. Esta tabla describe los requisitos mínimos de Proximidad Bluetooth (y del bloqueo por distancia).

Requisito previo	Detalles
Tarjeta inalámbrica	• Intel Wireless-AC 9560 • Intel Wireless-AC 9260 • Intel Dual Band Wireless-AC 8265 • Intel Tri-Band Wireless-AC 18265 • Intel Dual Band Wireless-AC 3168 • Intel Dual Band Wireless-AC 8260 • Intel Tri-Band Wireless-AC 18260 • Intel Dual Band Wireless-AC 7265 • Intel Dual Band Wireless-AC 3165 **Nota:** Intel Authenticate solo admite estas tarjetas inalámbricas si están instaladas en una plataforma y un sistema operativo que sean totalmente compatibles con dichas tarjetas.
Controladores	Tanto el controlador del adaptador de red como el controlador de Intel® Wireless Bluetooth® de la tarjeta deben estar instalados en la plataforma. **Nota:** Solo es compatible la versión 19.00.1626.3453 o posterior del controlador de Intel® Wireless Bluetooth®.
Sistema operativo del teléfono	• En teléfonos Android: Android 4.2.2 o posterior • En teléfonos iOS: versión iOS 10.1 o posterior
Aplicación del teléfono	• En teléfonos Android: `IntelAuthenticate.apk` • En iPhone: `IntelAuthenticate.ipa` (solo nivel de seguridad "Protegido") **Nota:** Para obtener más información, consulte la Aplicación Intel Authenticate en la página 12.
Nota: Proximidad Bluetooth (y bloqueo por distancia) en iPhones: • Solo se puede usar cuando se utiliza un iPhone* 5S o posterior (los dispositivos iPhone 5 y iPhone 5C no son compatibles). • Solo se puede usar en Windows 7 si la plataforma tiene una tarjeta Intel Dual Band Wireless AC 8260.	

2.3 Requisitos previos para Huella digital

Los requisitos previos específicos para el factor Huella digital dependen del tipo de lector de huellas digitales.

Nota:

El controlador del lector de huellas digitales para el lector de huellas digitales específico se debe instalar antes de instalar Intel Authenticate. Si instala el controlador después de instalar Intel Authenticate, el usuario final no podrá registrar sus huellas digitales con Intel Authenticate. Esto se debe a que no existirían las DLL y las claves de Registro necesarias (consulte Resolución de problemas de huellas digitales en la página 70).

Lectores de huellas digitales protegidas

- Lector de huellas digitales con tecnología de coincidencia en chip (Match on Chip o MOC)
- Controlador de lector de huellas digitales instalado
- Aplicación de administración de huellas digitales (FMA) instalada. Puede ser una FMA propietaria o la FMA de Windows incluida como parte del Marco biométrico de Windows (WBF) en Windows 10.

En esta versión, el factor Huella digital protegida solo se admite en las plataformas con los siguientes requisitos previos:

- Hardware de lector de huellas digitales: sensor de huellas digitales de Synaptics Natural ID* de la serie VFS7500
- Software de lector de huellas digitales: un controlador de Synaptics WBDI compatible con la integración con Intel Authenticate (pida más detalles al proveedor de la plataforma)

Lectores de huellas digitales ligeras

- Lector de huellas digitales
- Controlador de lector de huellas digitales instalado
- Aplicación de administración de huellas digitales (FMA) instalada. Puede ser una FMA propietaria o la FMA de Windows incluida como parte del Marco biométrico de Windows (WBF) en Windows 10.
- En Windows 7, esta revisión es un requisito previo para el factor Huella digital ligera: https://support.microsoft.com/es-es/kb/2863706

Nota:

En la configuración de la directiva de Intel Authenticate, puede seleccionar específicamente qué tipo de factor de huella digital desea activar. Si la directiva contiene solo el factor Huella digital protegida, no será posible registrar el factor de huella digital en plataformas que tengan un lector de huellas digitales ligeras. Si la red contiene ordenadores con ambos tipos de lector, se recomienda definir solo el factor Huella digital ligera en la directiva. El establecimiento solo del factor Huella digital ligera en la directiva en realidad significa que desea que se registre y utilice cualquier tipo de factor. Intel Authenticate detectará y registrará automáticamente el factor de huella digital conforme al tipo de lector de huellas digitales que exista en la plataforma ("Protegido" o "Débil").

2.4 Requisitos previos para el reconocimiento facial

El factor Reconocimiento facial tiene estos requisitos previos específicos:

- Windows 10.0.14933.222 o posterior
- Una cámara compatible con Windows Hello. Las cámaras compatibles suelen ser cámaras de infrarrojos tridimensionales que pueden utilizar el Marco biométrico de Windows (WBF). Para obtener más información, consulte la documentación de Microsoft.

2.5 Requisitos previos para Ubicación de Intel AMT

El factor Ubicación de Intel AMT tiene estos requisitos previos específicos:

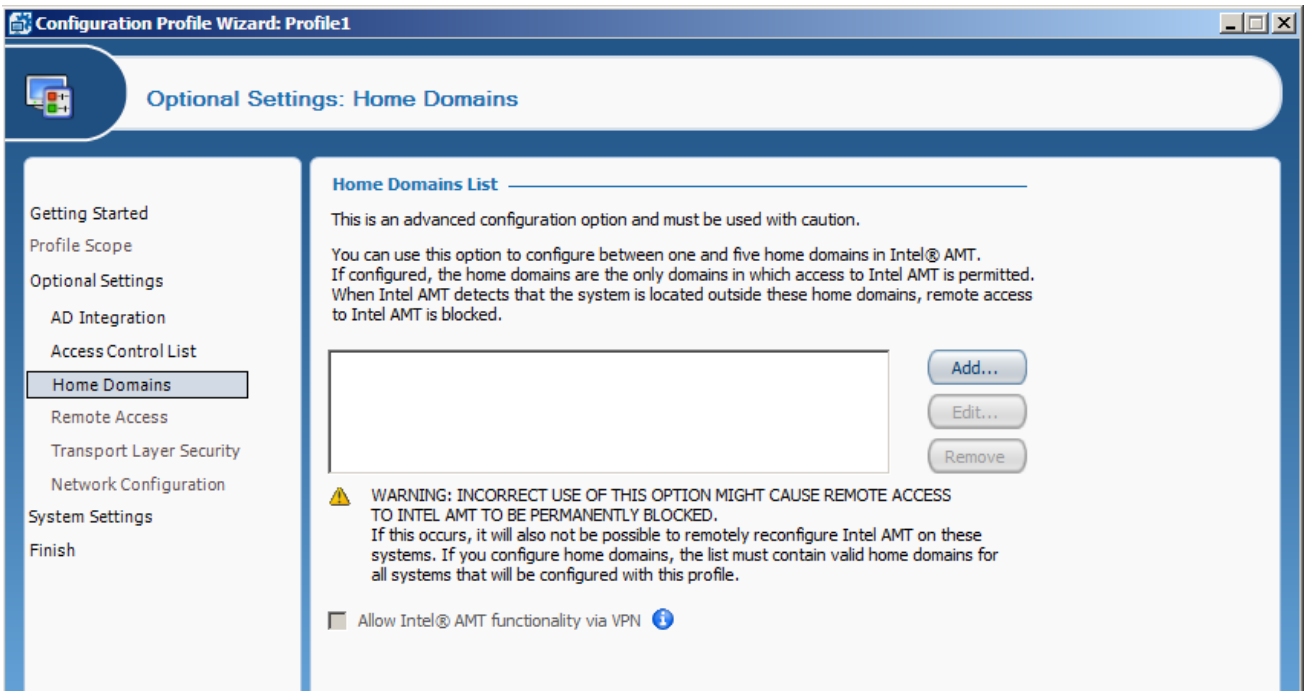
- Plataforma: sistema Intel® vPro™
- Firmware de Intel ME: versión 11.0.15.1003 o posterior
- Estado de configuración: Intel AMT debe estar configurado con dominios de inicio (si Intel AMT está configurado, pero los dominios de inicio no lo están, el registro y el uso de este factor darán error)
- Dirección IP: dirección IP dinámica (las direcciones IP estáticas NO se admiten)

Intel AMT incluye muchas opciones y métodos de configuración distintos. El único requisito para el factor Ubicación de Intel AMT es que Intel AMT se configure con dominios de inicio. Puede configurar Intel AMT mediante la configuración basada en host (método más fácil) o la configuración remota (requiere más pasos). Una vez configurados los dominios de inicio, puede utilizar el factor de autenticación Ubicación de Intel AMT.

Puede configurar Intel AMT utilizando Intel® Setup and Configuration Software (Intel® SCS) o mediante McAfee ePO Deep Command. La configuración de Intel AMT no se explica en esta guía. La información aquí presentada tiene como objetivo ayudarle a comprender la ubicación de la configuración de los dominios de inicio. Para obtener información completa sobre la configuración de Intel AMT, consulte la documentación de Intel SCS o McAfee ePO Deep Command.

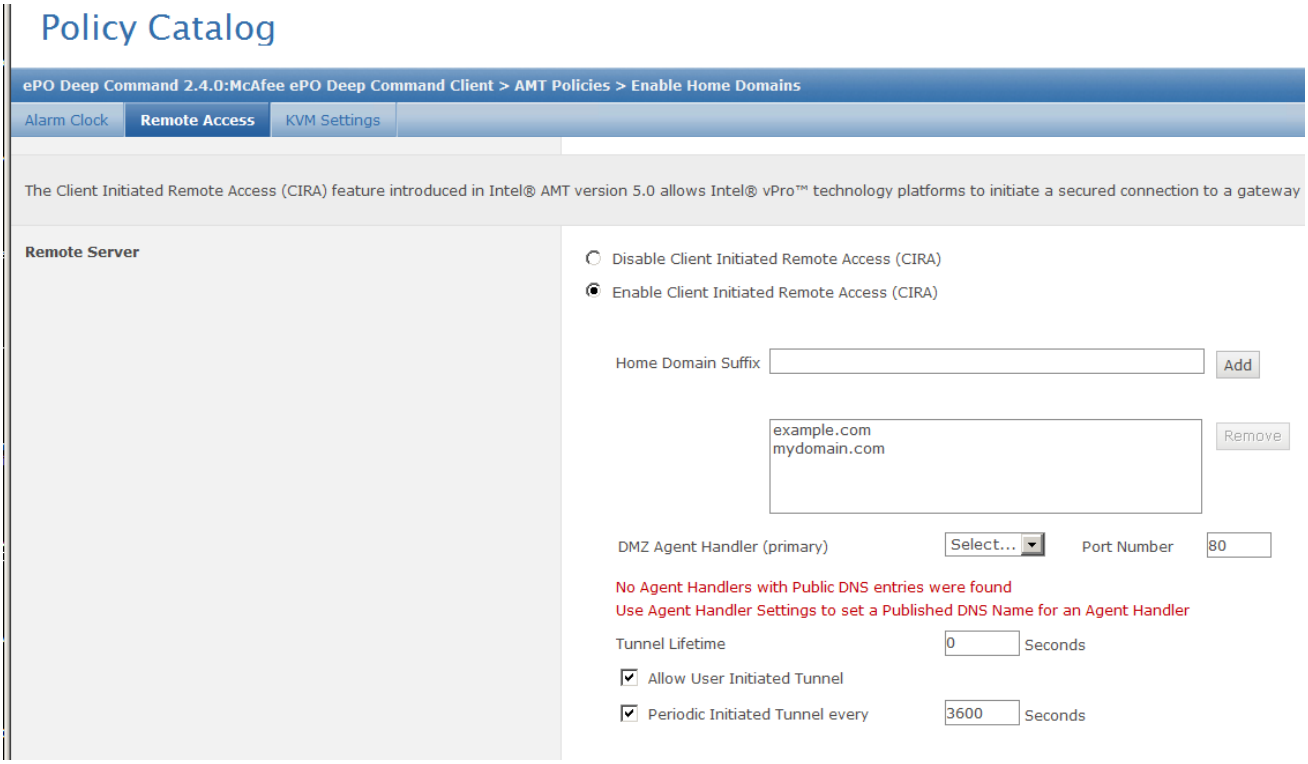
2.5.1 Configuración de los dominios de inicio con Intel SCS

Cuando se utiliza Intel SCS, la opción más rápida para configurar Intel AMT es mediante la utilidad de configuración de Intel AMT. No es necesario utilizar el componente de servicio de configuración remota (RCS) de Intel SCS. Al definir el perfil de configuración (mediante el Asistente del perfil de configuración), defina los dominios de inicio en la ventana Dominios de inicio. Puede definir entre uno y cinco dominios de inicio.



2.5.2 Configuración de los dominios de inicio con ePO Deep Command

En ePO Deep Command, la configuración de los dominios de inicio se encuentra en la pestaña Acceso remoto de la directiva. La configuración de los dominios de inicio también se utiliza para implementar la función de acceso remoto iniciado por el cliente (CIRA) de Intel AMT. Para utilizar el factor Ubicación de Intel AMT solo tiene que configurar los dominios de host. No es necesario configurar su entorno para CIRA.



2.6 Versión de PowerShell necesaria

Esta solución de integración se basa en scripts escritos en PowerShell 3.0. Para que estos scripts funcionen correctamente, debe estar instalada la versión 2.0 o posterior de PowerShell. Esto significa que debe asegurarse de que PowerShell versión 2.0 o posterior esté instalado en todas las plataformas cliente donde desee usar esta solución de integración.

Puede comprobar la versión de PowerShell mediante este comando de PowerShell: `get-host`.

3 Configuración del inicio de sesión en VPN

En esta sección se describe lo que hay que preparar para poder utilizar la acción de inicio de sesión en VPN.

3.1 Clientes de VPN compatibles

Intel Authenticate es compatible con clientes de VPN que utilicen la Microsoft Cryptographic Application Programming Interface (CAPI) estándar del Proveedor del servicio de credenciales (CSP). Los siguientes clientes de VPN han sido probados y validados para su uso con Intel Authenticate:

- Cisco*
- Microsoft*.

Intel Authenticate también funciona con otros clientes VPN, como Juniper*, pero no se han validado por completo.

3.2 Intel IPT con PKI

La acción Inicio de sesión en VPN utiliza certificados generados y protegidos en el hardware de la plataforma Intel utilizando Intel IPT con PKI. Se requieren componentes de Intel IPT con PKI:

- **En la plataforma cliente**: el instalador de Intel Authenticate instala automáticamente este componente en las plataformas cliente. (Si una plataforma admite Intel Authenticate, también admite Intel IPT con PKI). No se requiere ninguna otra acción.
- **En la CA de Microsoft**: consulte Preparación de la entidad de certificación abajo.

Nota:

Intel Authenticate requiere la versión 4.1 o posterior de Intel IPT con PKI. No se admiten versiones anteriores de Intel IPT con PKI.

3.3 Preparación de la entidad de certificación

Se necesita una entidad de certificación (CA) de Microsoft para utilizar las plantillas de CA empresariales al generar certificados para la acción de inicio de sesión en VPN. Para poder definir la plantilla, debe instalar un conjunto de "componentes de CA" para Intel IPT con PKI en el servidor donde se encuentra la CA de su organización. En esta sección se describen los requisitos previos de la CA y el procedimiento para instalar los componentes de CA.

3.3.1 Sistemas operativos de servidor compatibles

Los componentes de la CA de Intel IPT con PKI son compatibles con estos sistemas operativos de servidor:

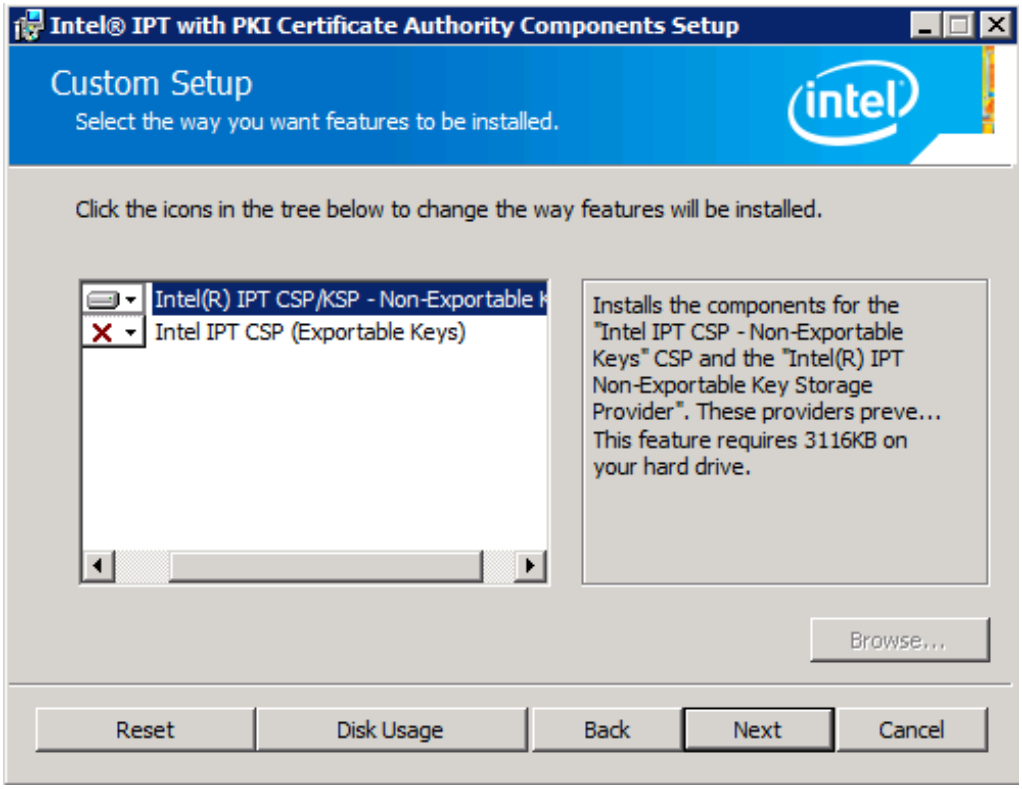
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

3.3.2 Instalación de componentes de CA

El instalador de los componentes de CA de Intel IPT con PKI se encuentra en la carpeta del `MS_CA_Installer` en la raíz de este paquete. Puede instalar Intel IPT con PKI utilizando el asistente del instalador o un comando CLI.

Para instalar los componentes de CA de Intel IPT con PKI (utilizando el asistente):

1. En el servidor de la autoridad de certificación, haga doble clic en **Intel_IPT_PKI_CA_Components_x64**. Aparecerá la pantalla de bienvenida.
2. Haga clic en **Siguiente**. Se abrirá la ventana Acuerdo de licencia de usuario final.
3. Seleccione **Acepto los términos del acuerdo de licencia** y haga clic en **Siguiente**. Se abrirá la ventana Instalación personalizada.



4. De manera predeterminada, la opción "Claves no exportables de Intel IPT CSP/KSP" está seleccionada. Esta es la única opción que tiene que instalar para activar la acción Inicio de sesión en VPN. Haga clic en **Siguiente** y, a continuación, haga clic en **Instalar** para iniciar la instalación.

Para instalar de forma inadvertida los componentes de la CA de Intel IPT con PKI:

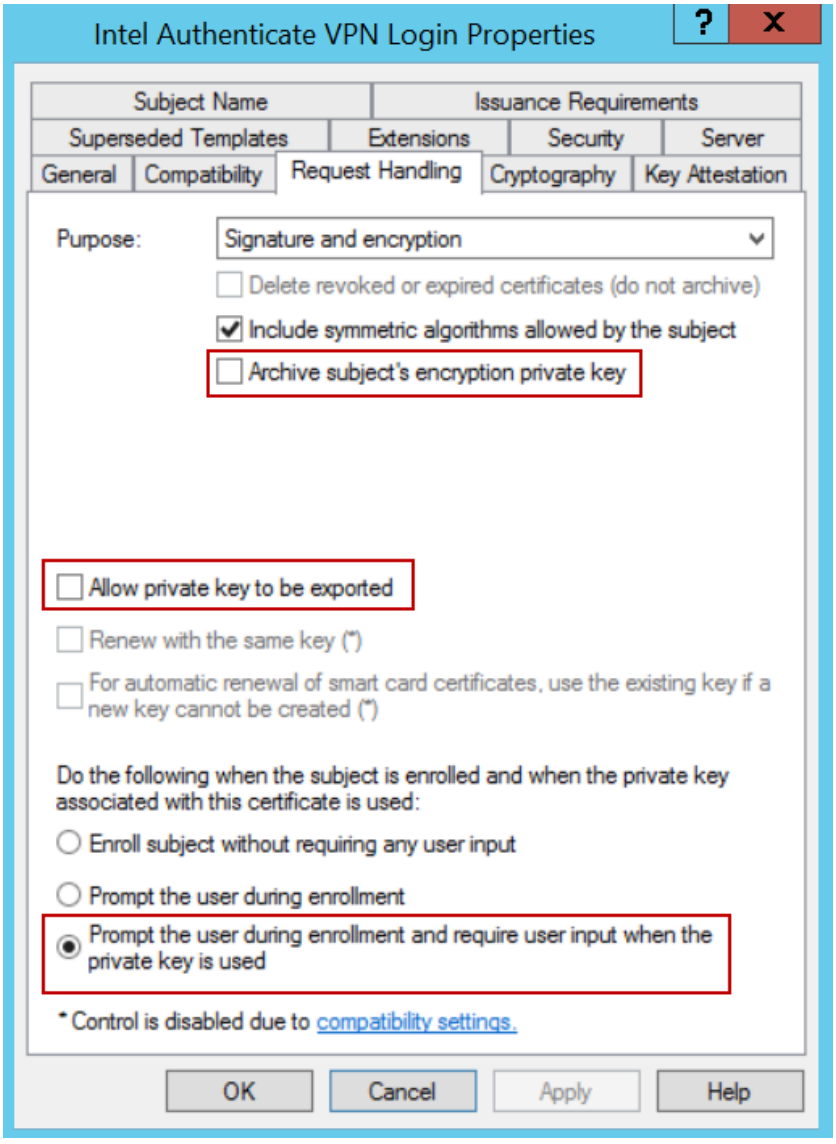
1. En el servidor donde se encuentra la CA, abra un símbolo del sistema administrativo.
2. Introduzca este comando:

```
msiexec /i [nombre_archivo_instalador].msi /qn ADDLOCAL=NonExportable
```

3.4 Definición de la plantilla de CA para el inicio de sesión en VPN

Los pasos para crear una plantilla de certificado varían según la versión del sistema operativo Windows Server. Además, el valor de muchos parámetros depende de los requisitos específicos de su organización. En esta sección se describen los parámetros de plantilla que tienen requisitos específicos para la acción de inicio de sesión en VPN.

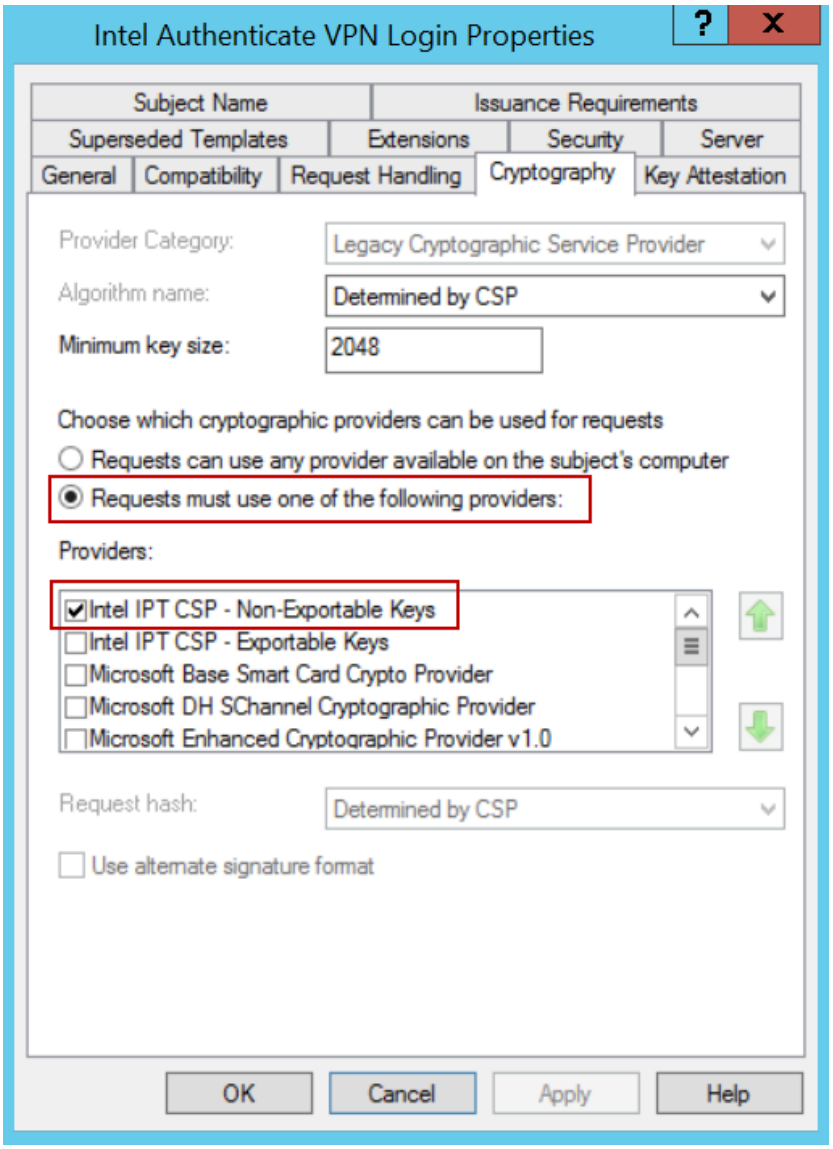
Tratamiento de la solicitud



En la ficha Tratamiento de la solicitud:

- Asegúrese de que la casilla **Archivar clave privada de cifrado de sujeto** NO esté marcada. Si se selecciona esta opción, el registro fallará y devolverá el mensaje de error "Parámetro no válido".
- Asegúrese de que la casilla **Permitir que la clave privada se pueda exportar** NO esté marcada.
- Seleccione la opción **Preguntar al usuario durante la inscripción y requerir la acción del usuario cuando se use una clave privada**.

Selección de CSP/Criptografía



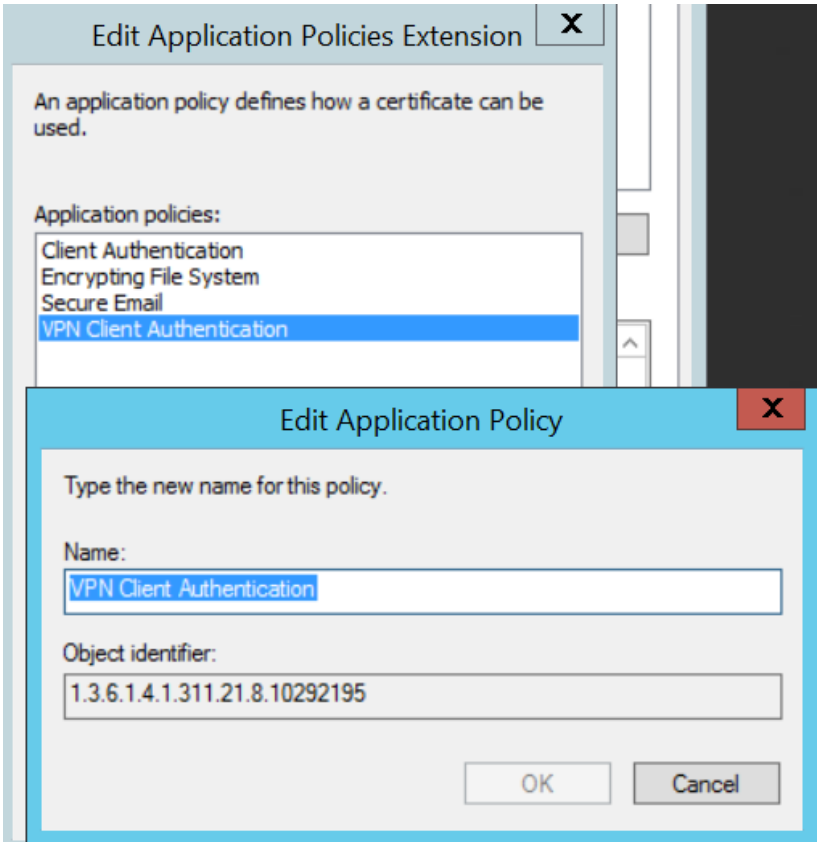
Cuando seleccione el CSP, asegúrese de que solo esté seleccionada la casilla de este CSP:

- Claves no exportables de Intel IPT CSP

Nota:

Intel IPT con PKI incluye CSP y KSP adicionales. Estos CSP y KSP no se admiten cuando se utiliza la acción de inicio de sesión en VPN. Esto también significa que las plantillas de la versión 3 no son compatibles (porque no admiten CSP).

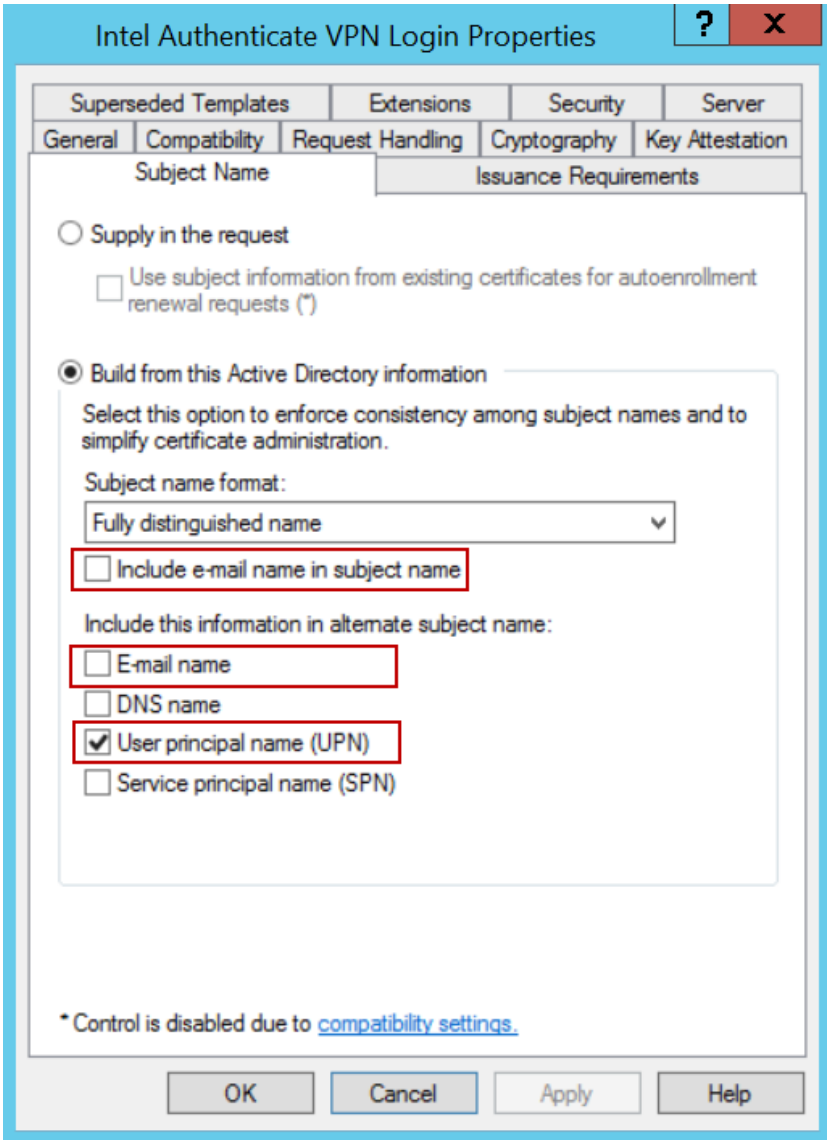
Extensión de directivas de aplicación



En la ficha Extensiones:

- Agregue una extensión de directivas de aplicación específicamente para la acción de inicio de sesión en VPN.
- Defina un único identificador de objeto (OID) para identificar esta directiva. Este es el OID que necesitará configurar en la appliance de VPN de su organización. Compruebe el máximo de caracteres admitidos por su dispositivo de VPN. (Muchos dispositivos de VPN tienen limitado el tamaño del OID a menos de 30 caracteres).

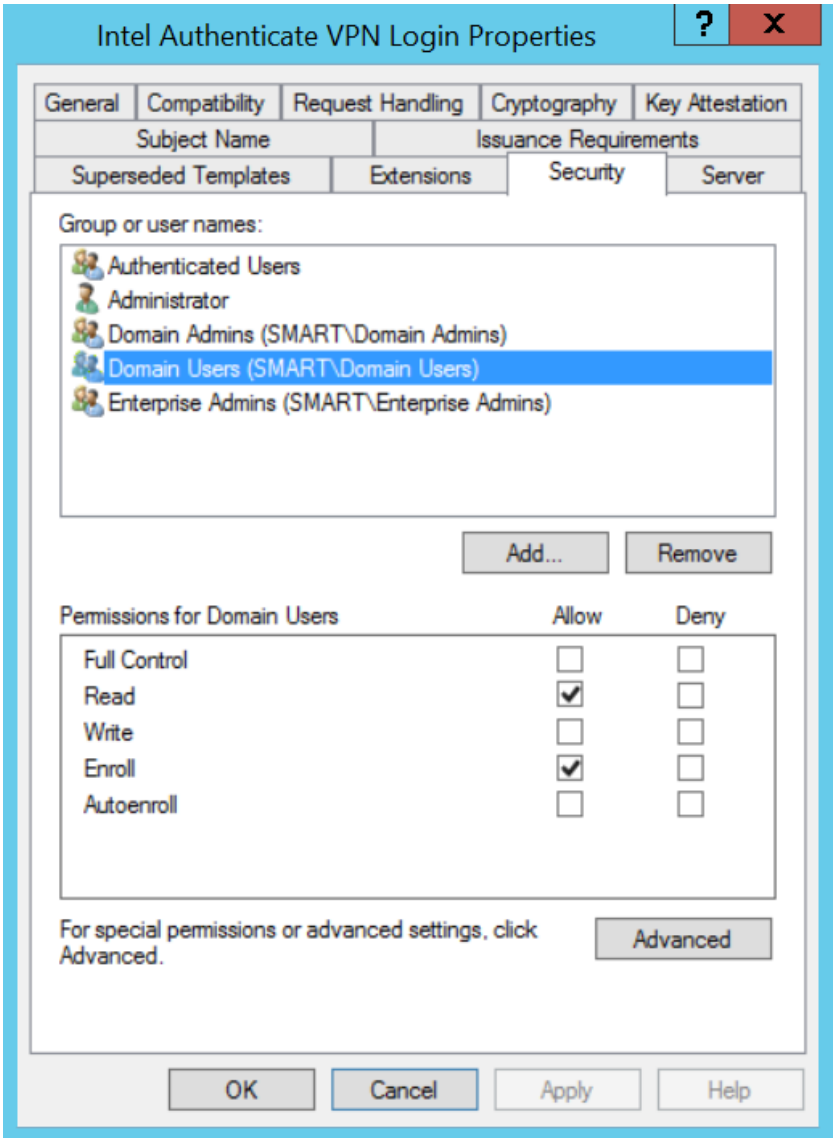
Nombre del firmante



En la ficha Nombre del firmante,

- Asegúrese de que la casilla **User principal name (UPN)** está seleccionada
- Si sus cuentas de usuario están definidas en Active Directory sin cuentas de correo electrónico, asegúrese de que estas dos casillas no estén seleccionadas:
  - **Incluya el nombre del correo electrónico en el nombre del firmante alternativo**
  - **Nombre del correo electrónico**

Ficha Seguridad



En la ficha Seguridad, asegúrese de que todos los grupos de usuarios que desea que tengan acceso al certificado de VPN se definan con estos permisos:

- **Leer**
- **Registrarse**

3.5 Configuración de la appliance de VPN

Para utilizar la acción de inicio de sesión en VPN, debe configurar su appliance de VPN para que requiera certificados en lugar de contraseñas. Cuando defina los detalles de certificados en la appliance de VPN, asegúrese de utilizar el OID que creó específicamente para la acción de inicio de sesión en VPN. Para obtener instrucciones sobre cómo definir la appliance de VPN para que utilice certificados, consulte la documentación que se proporciona con su appliance de VPN.

3.6 Generación de un certificado en el cliente

Cada cuenta de usuario que vaya a utilizar la acción de inicio de sesión mediante VPN requiere la instalación en el almacén de certificados del usuario de un certificado basado en la plantilla de inicio de sesión en VPN. Durante la instalación de Intel Authenticate, se instala la utilidad `CertificateUtility.exe` en todas las plataformas. La utilidad se instala en esta carpeta: `C:\Program Files\Intel\Intel(R) Identity Protection Technology with PKI`. Se puede utilizar para generar el certificado en las plataformas cliente.

Esta es la sintaxis para crear un certificado para el inicio de sesión en VPN:

```
CertificateUtility.exe -c create_cert [-a <action name>] [-u <ca_url>]
[-t <template name>] [-i <yes|no>]
```

Marca	Detalles
`-a <action_name>`	Valores válidos al generar un certificado para el inicio de sesión en VPN: • **Unattended_VPNLogin** – El usuario no está obligado a proporcionar ninguna entrada cuando se instala el certificado. Esta opción también permite instalar el certificado en la plataforma antes de que el usuario haya registrado sus factores. • **VPNLogin** – Durante la instalación del certificado, el usuario debe autenticarse usando los factores definidos para la acción de inicio de sesión en VPN. Si la autenticación falla, el certificado no se instalará. Utilizar esta opción no permite instalar el certificado hasta después de que el usuario haya registrado sus factores de inicio de sesión en VPN. **Nota:** El valor que se defina en este indicador dependerá de lo que se haya definido en la directiva de Intel Authenticate sobre la acción de inicio de sesión en VPN. Para utilizar la opción `Unattended_VPNLogin`, primero debe activarla en la directiva.
`-u <ca_url>`	La URL de certificación autorizada. Si no se proporciona, la herramienta volverá a todos los CA encontrados en el dominio y tratará de enviar la solicitud a cada uno de ellos.
`-t <template_name>`	El nombre de la plantilla de certificado de VPN. Asegúrese de escribir el nombre tal y como precisó en la plantilla de certificado. Si no especifica ningún nombre, el valor predeterminado para el inicio de sesión en VPN es: `IntelAuthenticateVPNLogin`.
`-i <yes|no>`	Determina si el usuario debe autenticarse cuando se use el certificado. La opción predeterminada es `no`. **Nota:** Para realizar el inicio de sesión en VPN, siempre se debe establecer este parámetro en `yes`.

1er ejemplo: Generar un certificado que no requiere que el usuario introduzca datos durante la instalación:

```
CertificateUtility.exe -c create_cert -a Unattended_VPNLogin -t <My_VPN_Template>
-yo sí
```

2º ejemplo: Generar un certificado que requiere la autenticación del usuario durante la instalación:

```
CertificateUtility.exe -c create_cert -a VPNLogin -t <My_VPN_Template> -yo sí
```

4 Configuración del inicio de sesión con tarjeta inteligente

Nota:

- Las instrucciones descritas en esta sección solo son necesarias si desea usar la opción de tarjeta inteligente virtual de la acción Inicio de sesión de SO (véase Inicio de sesión de SO en la página 7).
- Consulte también Consideraciones al utilizar tarjetas inteligentes en la página 37.

Tiene dos opciones para implementar la opción de tarjeta inteligente virtual:

- Utilizar la opción integrada predeterminada.
- Utilizar un gestor de certificados externos. Intel Authenticate admite actualmente la integración con Intercede MyID*.

En esta tabla se describen las opciones y lo que debe hacer para implementarlas.

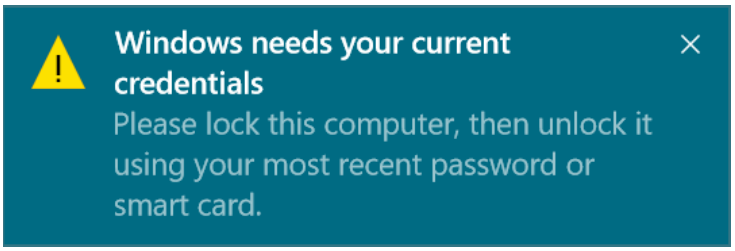
Opción	Descripción
Opción integrada	Esta es la opción predeterminada. Cuando se utiliza esta opción, Intel Authenticate instala automáticamente todos los componentes necesarios en la plataforma cliente. Además, Intel Authenticate también gestiona los certificados. • **Instalación en la CA:** debe definir una plantilla específica en la Entidad de certificación de Microsoft (consulte Definición de la plantilla de CA para la tarjeta inteligente en la página 37). • **Instalación en el cliente:** durante la instalación de Intel Authenticate en las plataformas cliente, Intel Authenticate comprueba si el software de cliente Intercede MYID* está instalado. Si no está instalado, Intel Authenticate instala los componentes de tarjeta inteligente necesarios. Esto incluye una entrada Tarjeta inteligente en el Administrador de dispositivos, así como el software y los controladores necesarios. A continuación, el servicio Intel Authenticate solicita e instala automáticamente un certificado para la autenticación de tarjeta inteligente, que se basa en la plantilla definida en la CA. Además, 10 días antes de que el certificado caduque, Intel Authenticate lo renueva automáticamente. Todas estas acciones se producen sin necesidad de ningún tipo de interacción del usuario.

Opción	Descripción
Gestor de certificados externos	Si desea ejercer más control sobre los certificados utilizados para la autenticación de tarjeta inteligente, puede recurrir a la integración de un gestor de certificados externos. • **Instalación en la CA:** debe definir una plantilla específica según las instrucciones de la documentación de MyID. • **Instalación en el cliente:** debe instalar una versión compatible del software de cliente Intercede MyID* en sus plataformas cliente. Si el instalador de Intel Authenticate detecta que el software de cliente MYID* está instalado, la opción integrada no se activa. En su lugar, el registro y la gestión del certificado de tarjeta inteligente la realiza completamente MyID. Para obtener más información, consulte la documentación de MyID. **Nota:** Si desea utilizar esta opción, se recomienda comprobar que MyID esté instalado en la plataforma cliente antes de instalar Intel Authenticate.

4.1 Consideraciones al utilizar tarjetas inteligentes

Es importante comprender estos puntos antes de implementar la opción de tarjeta inteligente:

- Cuando se implementa la opción de tarjeta inteligente, el proceso de inicio de sesión puede tardar un poco más en completarse (uno o dos segundos). Esto se debe a que la autenticación mediante certificados implica más acciones además de comprobar que se ha indicado la contraseña correcta.
- El primer inicio se sesión mediante la opción de tarjeta inteligente es más lento que los demás intentos posteriores (aproximadamente 10 segundos). Esto se debe a que se realizan varias acciones durante el primer inicio de sesión que son necesarias para configurar y confirmar la fiabilidad. Este tiempo adicional solo se necesita al iniciar sesión cuando se utiliza el certificado por primera vez.
- En ocasiones, el proceso de cambio de estados de alimentación puede tardar entre 7 y 15 segundos en realizarse.
- En algunos entornos de red, cuando se usa la autenticación basada en certificados, los usuarios pueden ver ocasionalmente mensajes emergentes solicitándoles que proporcionen sus credenciales:

  En la mayoría de los casos, el usuario puede ignorar este mensaje. Pero si el acceso a la red está bloqueado, basta con que bloquee el PC y se vuelva a conectar mediante Intel Authenticate.

  Este mensaje lo genera Windows y suele indicar que Windows considera que ha caducado alguna incidencia de autenticación y, por lo tanto, es necesario volver a realizar la autenticación. Si se generan estos mensajes en su entorno de red, compruebe la configuración de Active Directory. Preste especial atención a los valores de configuración de Kerberos en la red. Para obtener más información, consulte la documentación de Microsoft correspondiente.

4.2 Definición de la plantilla de CA para la tarjeta inteligente

Nota:

Las instrucciones descritas en esta sección solo son relevantes si se pretende utilizar la opción "integrada" (consulte Configuración del inicio de sesión con tarjeta inteligente en la página 35). Si va a utilizar la opción de administrador de certificado externo, consulte la documentación de MyID para obtener más información sobre cómo definir la plantilla.

Para crear una plantilla de certificado de tarjeta inteligente para la opción "integrada":

1. En el servidor de su entidad de certificación, seleccione **Inicio** > **Ejecutar**. Aparecerá la ventana Ejecutar.
2. Escriba mmc y haga clic en **Aceptar**. Se abrirá la ventana de Microsoft Management Console.

3. Si el complemento Entidad de certificación no está instalado, lleve a cabo estos pasos:

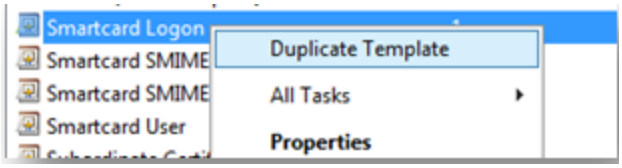
   a. Seleccione **Archivo** > **Agregar o quitar complemento**. Se abrirá la ventana Agregar un complemento independiente.

   b. Haga clic en **Agregar**. Se abrirá la ventana Agregar o quitar complemento.

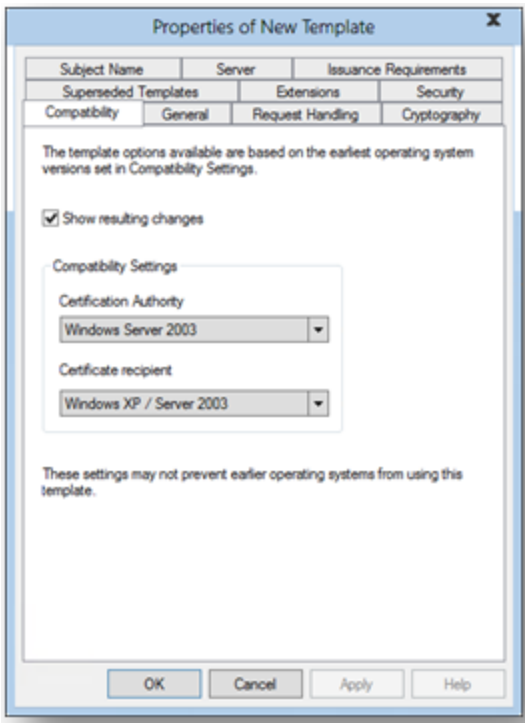
   c. En la lista de complementos disponibles, seleccione **Plantillas de certificado** y haga clic en **Agregar**.

   d. Haga clic en **Aceptar**. La ventana Agregar o quitar complemento se cerrará y el complemento Entidad de certificación se agregará al árbol raíz de la consola.

4. En la lista de complementos disponibles, seleccione **Plantillas de certificado** y haga clic en **Agregar**.
5. En la raíz de la consola de MMC, haga doble clic en **Plantillas de certificado**. Aparecerán todas las plantillas de certificado disponibles.
6. Haga clic con el botón derecho en la plantilla **Inicio de sesión de tarjeta inteligente** y seleccione **Duplicar plantilla**. Se agregará una nueva plantilla de certificado a la lista.



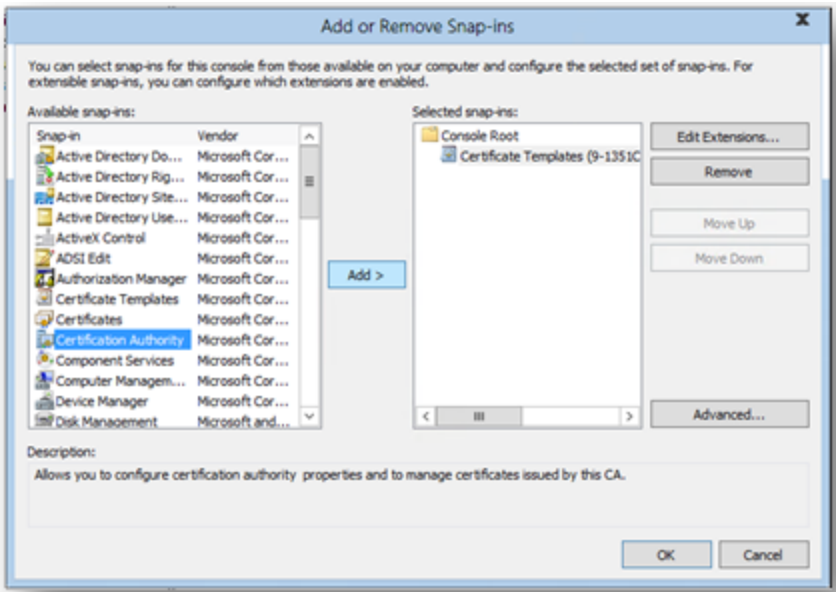
7. Haga clic con el botón derecho en la nueva plantilla de certificado y seleccione **Propiedades**. Se abrirá la ventana Nuevas propiedades de tarea.



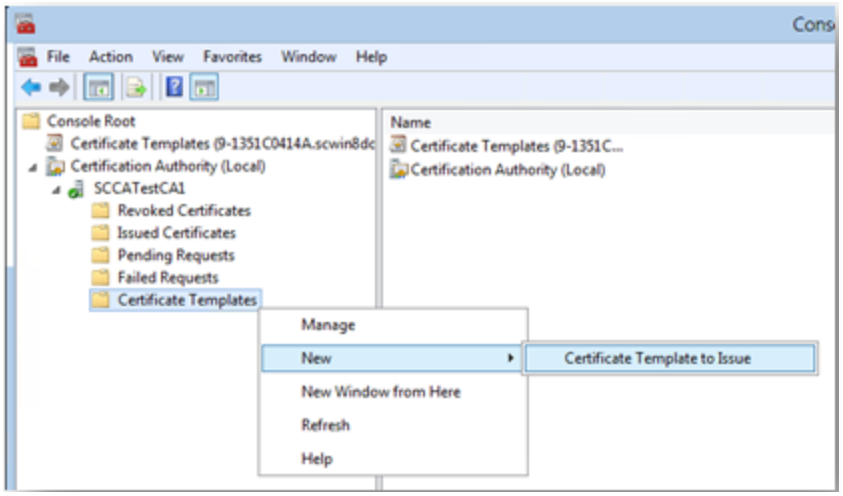
8. Seleccione la ficha **Compatibilidad** y, en la lista desplegable Entidad de certificación, seleccione **Windows Server 2003**.

9. Seleccione la ficha **General**:
    a. Cambie el nombre de la plantilla por **Inicio de sesión de SO con tarjeta inteligente de Intel Authenticate**.
    b. Establezca el período de validez requerido.
10. Haga clic en la ficha **Tratamiento de la solicitud**:
    a. Defina el **Propósito** como **Firma** e **Inicio de sesión de tarjeta inteligente**.
    b. Haga clic en **Preguntar al usuario durante la inscripción**.
11. Haga clic en la ficha **Criptografía**:
    a. Establezca el tamaño mínimo de la clave en 2048.
    b. Haga clic en **Las solicitudes deben usar uno de los proveedores siguientes** y, después, seleccione **Proveedor base de cifrado para tarjetas inteligentes de Microsoft**.
12. Haga clic en la ficha **Seguridad**. Agregue el grupo de seguridad al que desee conceder acceso para el registro. Por ejemplo, para conceder acceso a todos los usuarios, seleccione el grupo Usuarios autentificados y, después, seleccione los permisos de registro para ellos.
13. Haga clic en **Aceptar** para finalizar los cambios y crear la nueva plantilla. La plantilla nueva aparecerá en la lista de **Plantillas de certificado**.
14. Si el complemento Plantillas de certificado no está instalado, lleve a cabo estos pasos:
    a. Seleccione **Archivo** > **Agregar o quitar complemento**. Se abrirá la ventana Agregar un complemento independiente.
    b. Haga clic en **Agregar**. Se abrirá la ventana Agregar o quitar complemento.
    c. En la lista de complementos disponibles, seleccione **Entidad de certificación** y haga clic en **Agregar**.
    d. Haga clic en **Aceptar**. La ventana Agregar o quitar complemento se cerrará y el complemento Plantillas de certificado se agregará al árbol raíz de la consola.

15. Aparecerá el mensaje para seleccionar el equipo que administrará este complemento. Seleccione el equipo donde se encuentre la CA; probablemente, será Equipo local.



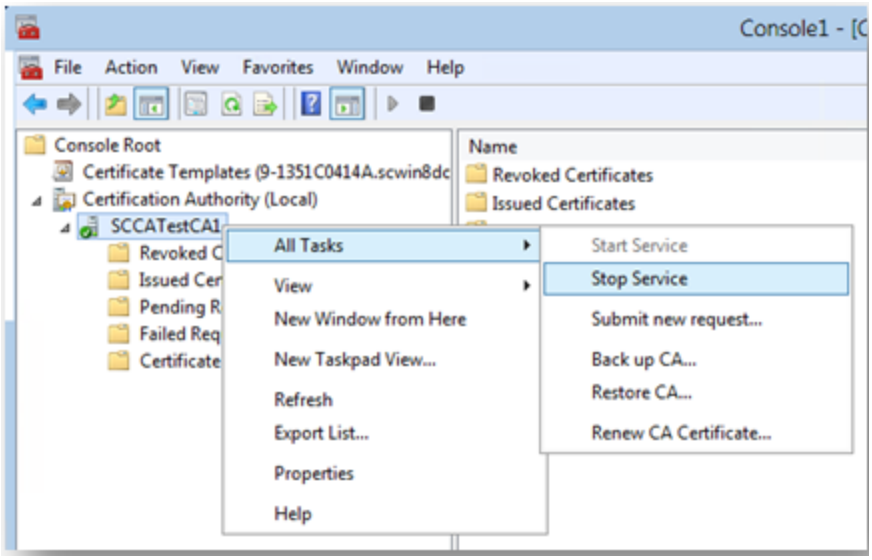
16. En el panel izquierdo de MMC, expanda **Entidad de certificación (local)** y, después, expanda la CA dentro de la lista **Entidad de certificación**.
17. Haga clic con el botón derecho en **Plantillas de certificado**, haga clic en **Nueva** y, después, haga clic en **Plantilla de certificado que se va a emitir**.



18. En la lista, seleccione la plantilla nueva que acaba de crear (**Inicio de sesión de SO con tarjeta inteligente de Intel Authenticate**) y, después, haga clic en **Aceptar**.

> **Nota:**
>
> Puede que su plantilla tarde algún tiempo en replicarse en todos los servidores y estar disponible en esta lista.

19. Una vez que se replique la plantilla, en MMC haga clic con el botón derecho en la lista **Entidad de certificación**, haga clic en **Todas las tareas** y, después, haga clic en **Detener servicio**. A continuación, vuelva a hacer clic con el botón derecho en el nombre de la CA, haga clic en **Todas las tareas** y, después, en **Iniciar servicio**.



5 Preparación para la integración

En esta sección se describen las tareas previas que se deben realizar antes de instalar el complemento.

5.1 Preparación de un certificado de firma digital

Todas las directivas de Intel Authenticate deben estar firmadas por un certificado de "firma digital". La firma de la directiva es un paso obligatorio en el complemento de Profile Editor antes de poder guardar la directiva. Si no tiene un certificado válido, no se le permitirá guardar la directiva. Se recomienda preparar un certificado que solamente utilizará Intel Authenticate. Después de adquirir un certificado para su uso con Intel Authenticate, deberá instalarlo en el equipo donde pretenda ejecutar Profile Editor.

Requisitos de certificado

- El certificado debe ser emitido por una entidad de certificación (CA) de confianza y debe contener una clave privada válida.
- El certificado NO tiene que ser un certificado de firma de código.
- El tamaño de la clave debe ser de 2048 o 4096 bits (el resto de tamaños de claves no son compatibles).
- La clave debe ser generada por un proveedor de servicios criptográficos (CSP). Se recomienda usar un CSP que admita SHA256. Si emplea un CSP que no admita SHA256, deberá asegurarse de que se pueda exportar la clave.
- Las claves generadas por un proveedor de almacenamiento de claves (KSP) no se admiten.
- Asegúrese de instalar el certificado en el almacén de equipo o el almacén de certificados de usuario del usuario que ejecute Profile Editor. Solo se mostrarán como disponibles en el complemento de Profile Editor los certificados instalados en estos almacenes de certificados. Si instala el certificado en el almacén de equipo, debe ejecutar Profile Editor con privilegios de administrador. Además, el certificado raíz debe estar instalado en el almacén de certificados raíz de confianza.

Obtención de un certificado

Puede utilizar certificados de firma digital generados por una CA externa o una CA interna ubicada en su red. Para obtener un certificado, debe solicitarlo a la CA mediante una solicitud de firma de certificado (CSR). El proceso para adquirir un certificado varía según el proveedor y no se explica en esta guía.

Nota:

El botón Seleccionar certificado de firma de Profile Editor muestra una lista de los certificados de firma que ya están instalados en el equipo donde se ejecuta Profile Editor. Con fines de ensayo, puede utilizar cualquiera de los certificados que estén marcados como válidos (en la columna de certificados válidos). Si no hay ningún certificado válido, puede crear un certificado de prueba, como se describe en el siguiente procedimiento.

Creación de un certificado de prueba

Desde PowerShell versión 5, puede utilizar el comando `New-SelfSignedCertificate` para crear un certificado. (PowerShell 5 está incluido por defecto en Windows 10). Con este procedimiento, se crea un certificado de prueba y se instala en el almacén de certificados personales del usuario actual.

Para crear e instalar un certificado de prueba:

1. Seleccione el equipo en el que desea ejecutar Profile Editor y cree la directiva de Intel Authenticate.
2. Inicie sesión en el equipo con un usuario administrador.
3. Abra un símbolo del sistema y ejecute este comando:

   ```
   New-SelfSignedCertificate -Subject "CN=TestCert" -KeyUsageProperty All
   -KeyAlgorithm RSA -KeyLength 2048 -KeyUsage DigitalSignature
   -Provider "Microsoft Enhanced RSA and AES Cryptographic Provider"
   -CertStoreLocation "Cert:\CurrentUser\My"
   ```

   En este ejemplo, se instala un certificado denominado "TestCert" en el almacén de certificados personales. Puede utilizar cualquier nombre para su propio certificado de prueba. Cuando finalice el comando, deberá copiar manualmente el certificado en el almacén de certificados raíz de confianza del usuario actual. En los pasos restantes se describe cómo hacerlo con Microsoft Management Console.
4. Haga clic en **Inicio**, escriba mmc.exe y, a continuación, pulse <Intro>. Se abre la ventana de Microsoft Management Console.
5. Seleccione **Archivo** > **Agregar o quitar complemento**. Se abrirá la ventana Agregar o quitar complementos.
6. En la lista de complementos disponibles (en el panel izquierdo de la ventana), seleccione **Certificados** y haga clic en **Agregar**. Se abre la ventana Complemento Certificados.
7. Seleccione **Mi cuenta de usuario** y haga clic en **Finalizar**. La ventana Complemento Certificados se cierra y el complemento "Certificados: usuario actual" se agrega a la lista de los complementos seleccionados.
8. Haga clic en **Aceptar**. La ventana Agregar o quitar complementos se cierra y los complementos se agregan al árbol Raíz de consola (en el panel izquierdo de la ventana).
9. En el panel izquierdo, seleccione **Certificados**: **usuario actual** > **Personal** > **Certificados**.
10. En el panel de la derecha, haga clic con el botón derecho en **TestCert** y seleccione **Copiar**.
11. En el panel izquierdo, haga clic en **Certificados**: **usuario actual** > **Entidades de certificación raíz de confianza** > **Certificados** y seleccione **Pegar**.
12. Aparece un mensaje de advertencia de seguridad. Haga clic en **Sí**. El certificado TestCert se copia en el almacén Autoridades de certificación raíz de confianza.
13. Cierre la ventana de Microsoft Management Console. El certificado de prueba está ahora listo para utilizarse. Cuando ejecute Profile Editor en el equipo, el certificado de prueba aparecerá en la lista de certificados válidos.

5.2 Creación de una directiva

Las directivas de Intel Authenticate se crean mediante el complemento de Profile Editor de Intel Authenticate. El complemento se carga en el componente Profile Editor de Intel SCS. Cuando está cargado, el complemento de Profile Editor de Intel Authenticate muestra la configuración que admite. Para ver las descripciones de las opciones de configuración, haga clic en el icono de ayuda del complemento.

Para crear una directiva:

1. En la carpeta `ProfileEditor`, haga clic con el botón derecho en **ProfileEditor.exe** y seleccione **Ejecutar como administrador**.
2. En el panel izquierdo, seleccione el complemento de Intel Authenticate.
3. En el panel de la derecha, haga clic en **Crear nuevo perfil**. Se abrirá un nuevo perfil vacío.
4. En la sección Certificado de firma, haga clic en **Seleccionar certificado de firma** y seleccione un certificado que se usará para firmar la directiva (consulte Preparación de un certificado de firma digital en la página 42).

   Nota:

   La lista contiene todos los certificados encontrados en los almacenes de certificados relevantes. Sin embargo, solo se puede seleccionar un certificado si está marcado como válido (en la columna Válido). Si el certificado aparece como no válido porque la cadena no se puede validar, intente conectar la plataforma a Internet o instalar manualmente los certificados ausentes en la cadena.

5. Defina la configuración que desee incluir en la directiva. La mayoría de las opciones de configuración incluye información sobre herramientas para explicar su uso. Para obtener información detallada sobre las opciones de configuración, haga clic en el icono de ayuda de la barra de herramientas del complemento.

   Nota:

   En sistemas que no sean Intel vPro, solo puede definir dos factores obligatorios para cada acción. La aplicación de una directiva que contiene una acción con más de dos factores obligatorios fallará en sistemas que no sean vPro. Esta restricción no se aplica a sistemas Intel vPro. En sistemas Intel vPro, puede definir tantos factores obligatorios por acción como desee.

6. En la barra de herramientas del complemento, haga clic en **Guardar** o en **Guardar como**. Se abrirá la ventana Guardar como.
7. Especifique el nombre y la ubicación donde desee guardar la directiva; a continuación, haga clic en **Guardar**. La ventana Guardar como se cerrará y el perfil se guardará. La directiva permanecerá abierta en el complemento de Profile Editor y el nombre de la directiva aparecerá en la barra de herramientas del complemento.

Nota:

El archivo XML de la directiva ya está listo para su uso. Tendrá que seleccionar este archivo XML en el Asistente para complementos durante la instalación.

6 Integración con Microsoft SCCM

En esta sección se describe cómo utilizar el contenido del paquete de integración de SCCM para integrar Intel Authenticate con SCCM. Tras la integración, podrá utilizar SCCM para configurar y administrar Intel Authenticate.

6.1 Flujo de despliegue con SCCM

Estos son los pasos principales para desplegar y configurar Intel Authenticate mediante SCCM:

1. Complete las tareas descritas en Preparación para la integración en la página 42.
2. Asegúrese de que su versión y configuración de SCCM sean compatibles (véase Versiones compatibles de SCCM abajo).
3. Importe las clases de inventario de hardware (véase Para agregar las clases de inventario de hardware: en la página siguiente).
4. Instale el complemento para crear recopilaciones, despliegues, paquetes y secuencias de tareas en SCCM (véase Instalación del complemento en la página 49).
5. Cree un paquete de despliegue para los instaladores de Intel Authenticate (consulte Creación de un paquete de instalación del cliente en la página 53).
6. Active las secuencias de tareas en el orden correcto (véase Activación de las secuencias de tareas (en orden) en la página 58).
7. Después aplicar la directiva en una plataforma de cliente, el usuario puede registrar los factores que ha definido en la directiva y empezar a usar Intel Authenticate. Para obtener más información sobre el proceso de registro, consulte la guía de registro incluida en el paquete de integración.

6.2 Versiones compatibles de SCCM

Las versiones compatibles de SCCM podrían variar según la versión del complemento. Consulte la documentación del complemento para obtener detalles sobre las versiones compatibles.

Nota:

Para la jerarquía SCCM 2012 con un sitio de administración central (tal como se describe aquí: http://technet.microsoft.com/en-us/library/gg712320.aspx), asegúrese de instalar el complemento en el sitio de administración central (y no en un sitio primario/secundario).

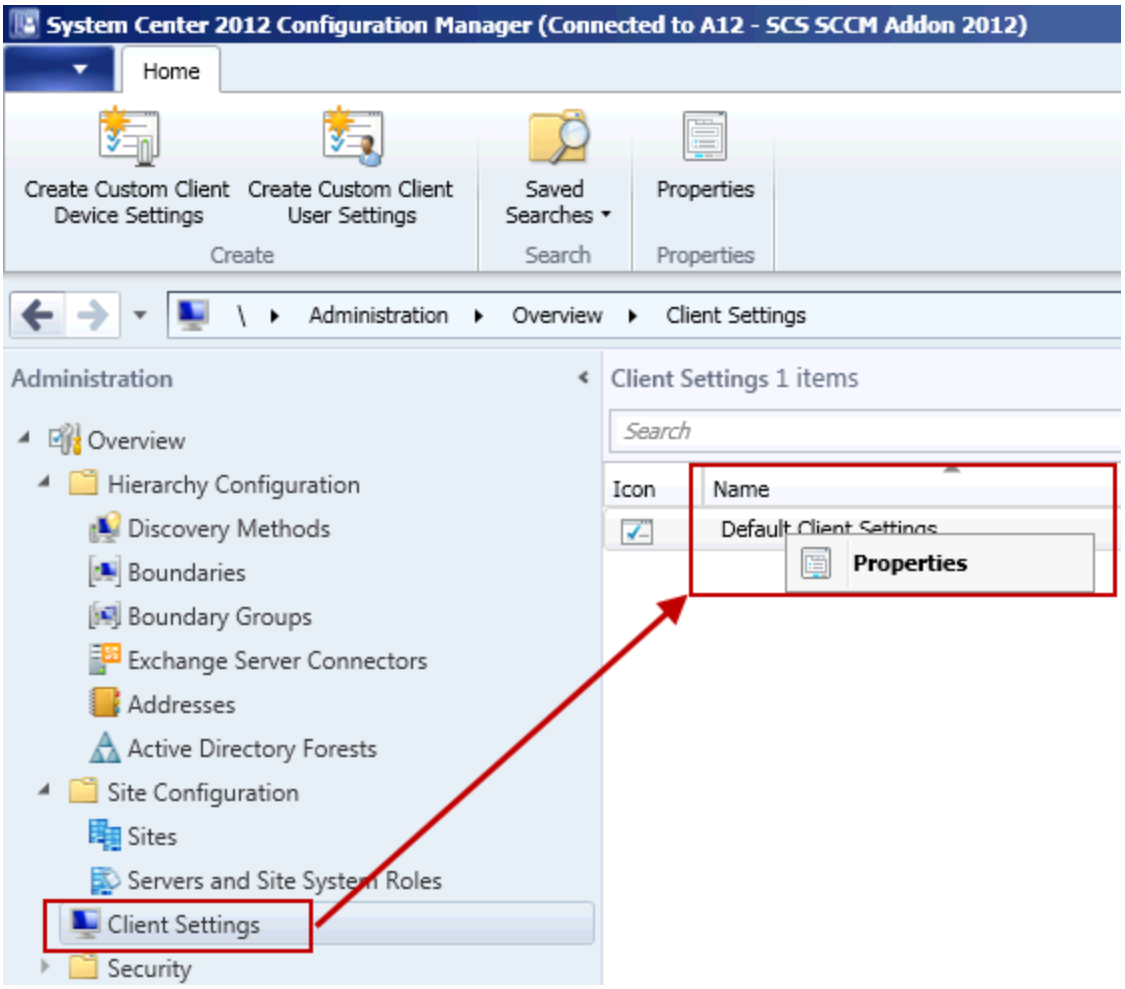
6.3 Para agregar las clases de inventario de hardware:

Antes de instalar el complemento, es necesario agregar algunas clases de inventario de hardware a SCCM. Estas clases se utilizan para rellenar las recopilaciones con datos, incluidas las recopilaciones correspondientes a Intel Authenticate. Las clases se importan desde dos archivos que se proporcionan con el complemento.

- `sms_def_SCSDiscovery.mof`: agrega una clase llamada `Intel_SCS_Discovery`.
- `sms_def_AMT.mof`: agrega una clase con el prefijo `Intel_AMT`.

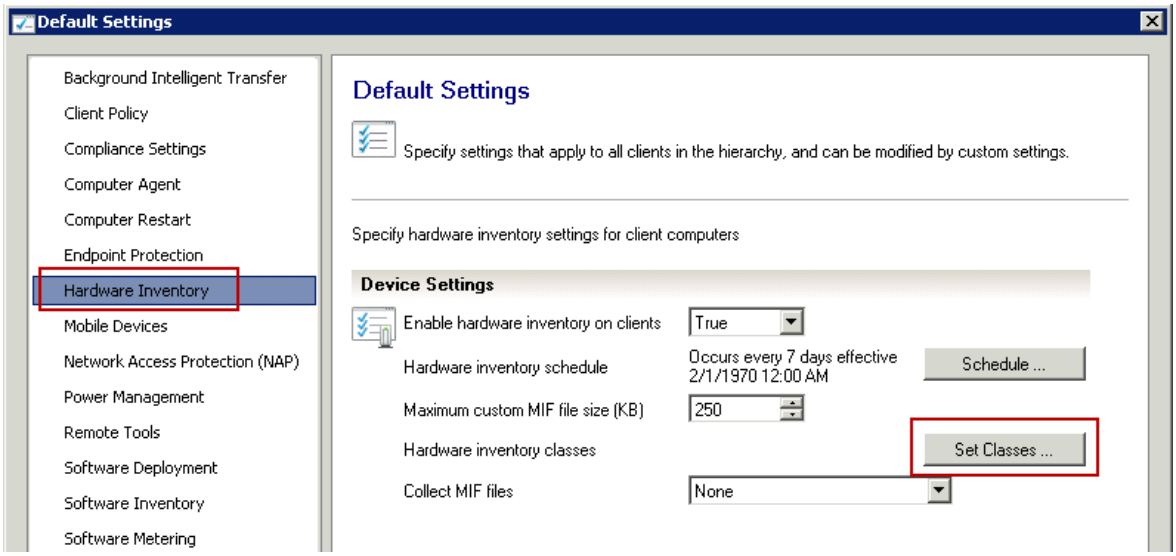
Adición de las clases de inventario de hardware

1. Abra la consola de Configuration Manager.
2. En el panel izquierdo, seleccione **Administración** > **Configuración de cliente**.
3. En el panel derecho, haga clic con el botón derecho en **Configuración de cliente predeterminada** y seleccione **Propiedades**.

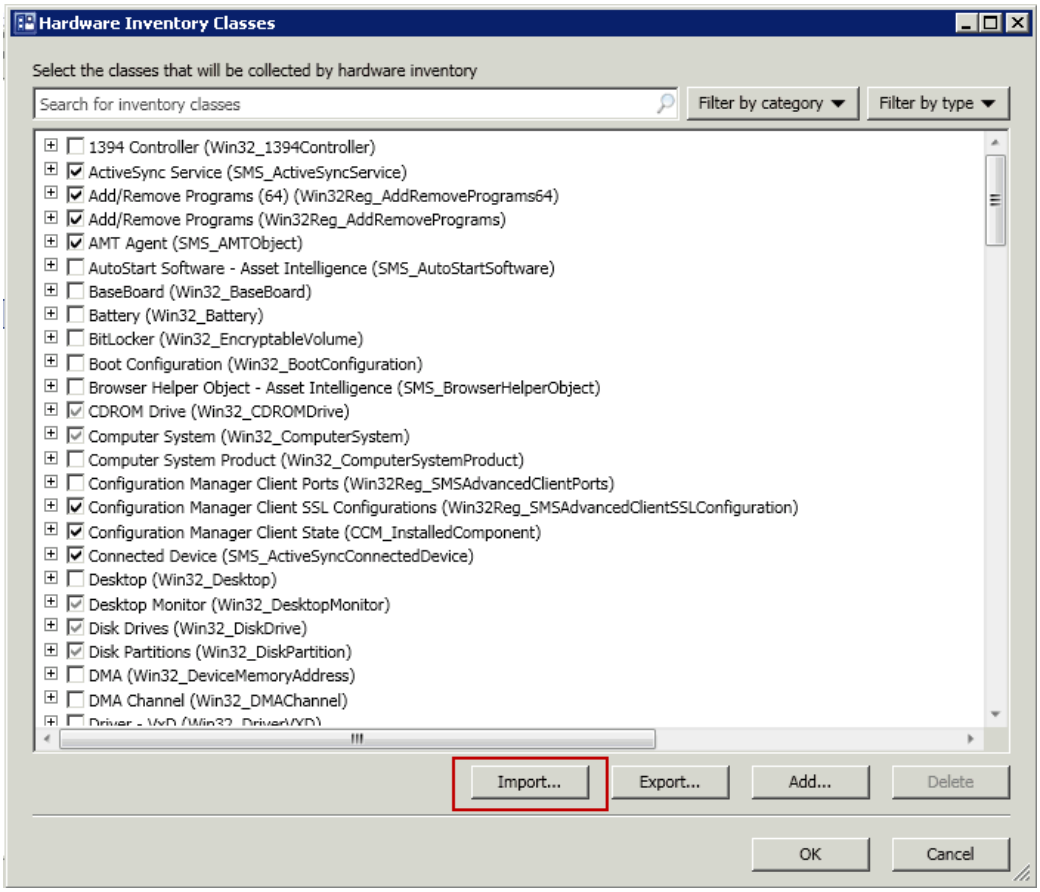


Aparecerá la ventana de configuración predeterminada.

4. Seleccione **Inventario de hardware**.

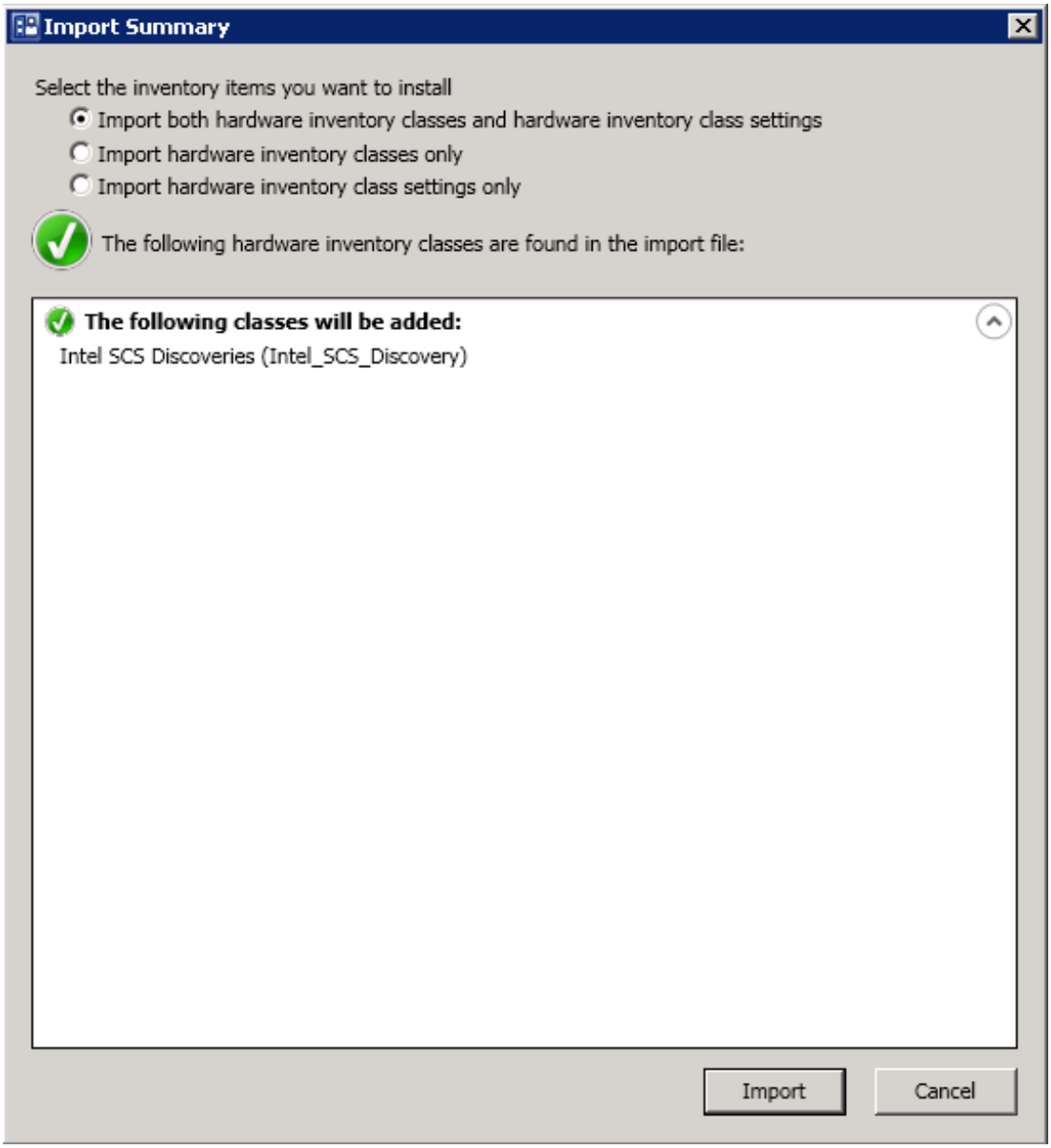


5. Haga clic en **Establecer clases**. Se abrirá la ventana Clases de inventario de hardware.



6. Haga clic en **Importar**.

7. Desplácese a la carpeta `SCCMAddon`, seleccione el archivo `sms_def_SCSDiscovery.mof` que se incluía con el complemento y haga clic en **Aceptar**. Se abrirá la ventana Resumen de importación.



> **Nota:**
>
> Si aparece un error en la ventana Resumen de importación, consulte Problemas con la importación de clases de inventario de hardware en la página 81.

8. Haga clic en **Importar** y, después, haga clic dos veces más en **Aceptar** para cerrar las ventanas abiertas.
9. Repita los pasos del 6 al 8 para importar el archivo `sms_def_AMT.mof`.

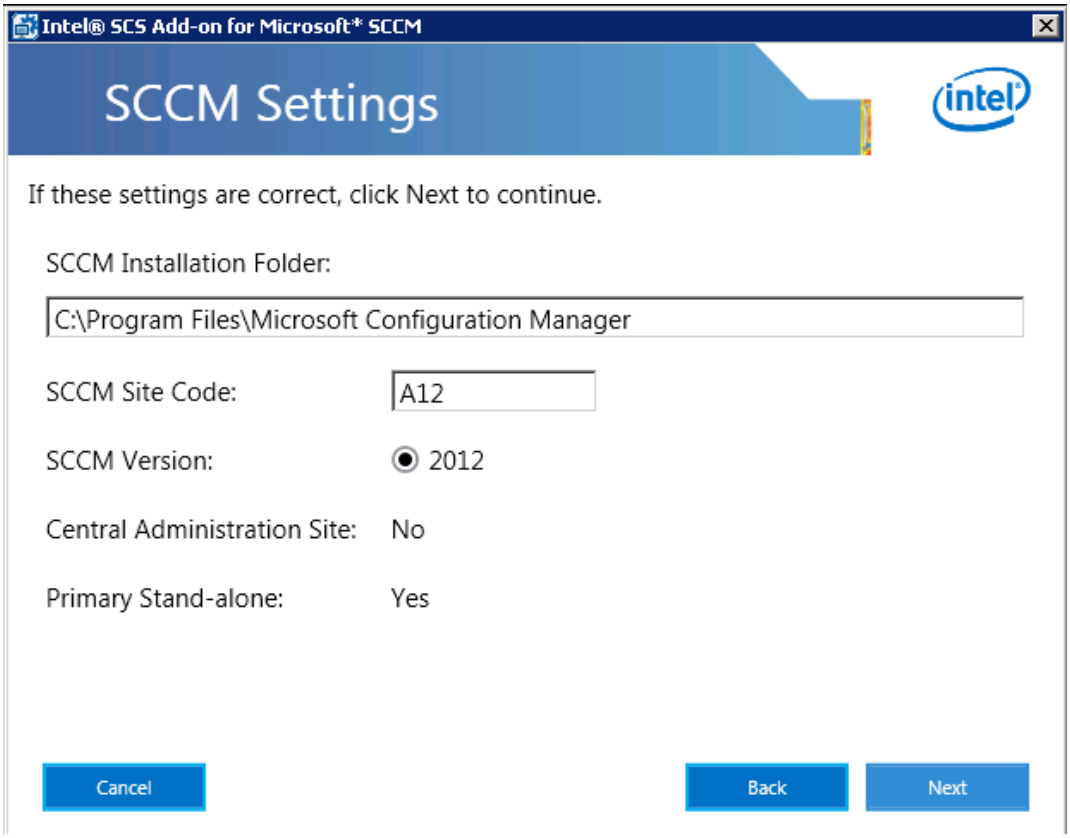
6.4 Instalación del complemento

En este procedimiento se describe cómo instalar los componentes mínimos del complemento necesarios para integrar Intel Authenticate con SCCM.

En este procedimiento se da por sentado que aún no está instalado ningún componente de complemento. Si alguno de los componentes de complemento está ya instalado, al abrir el instalador de complementos, seleccione **Modificar configuración del complemento**. A continuación, siga las instrucciones desde el paso 7 para agregar los componentes que faltan y el complemento de Intel Authenticate.

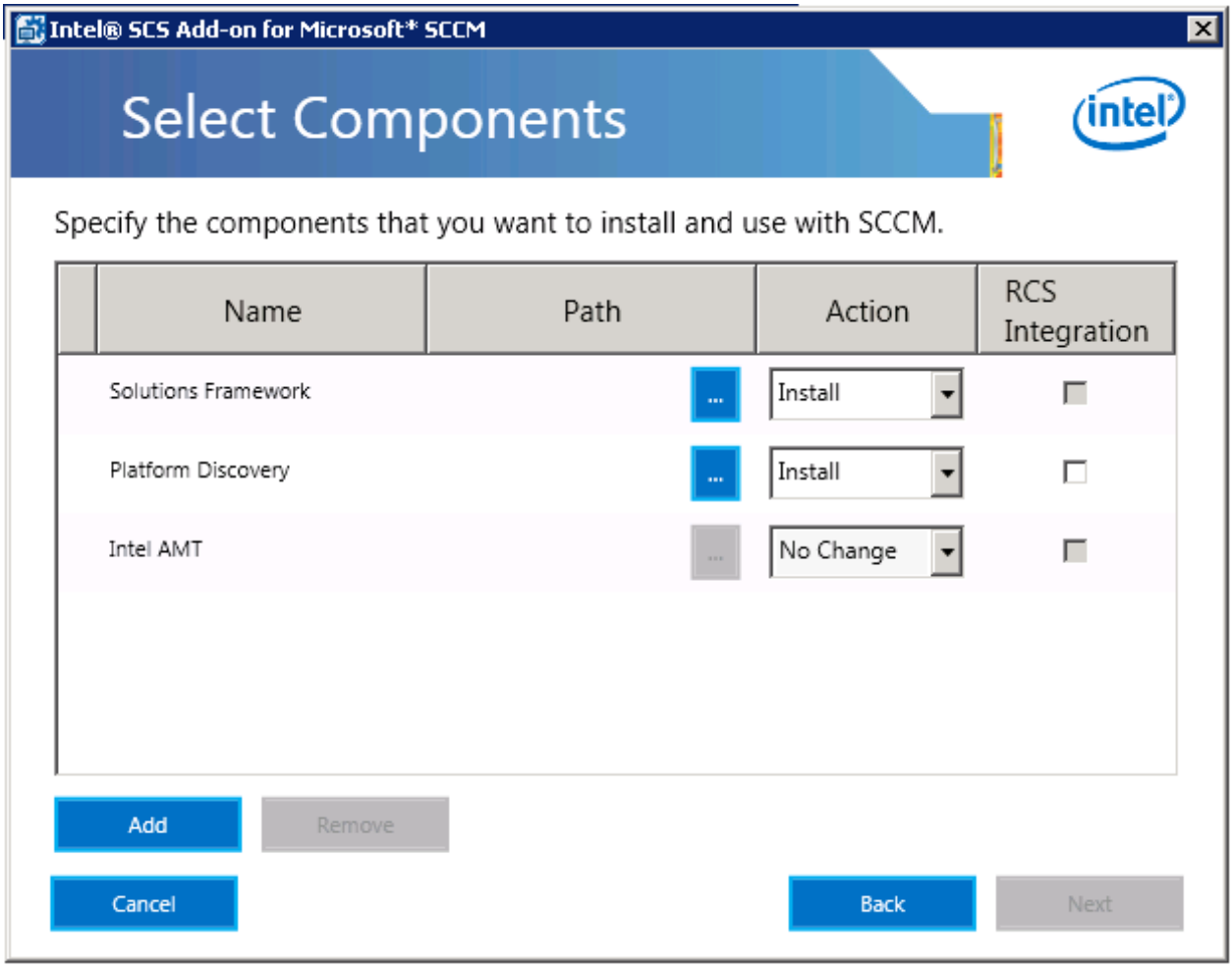
Para instalar el complemento:

1. Copie el contenido del paquete de integración de SCCM en el servidor donde se ejecuta la Consola de Configuration Manager. (En una jerarquía con un sitio de administración central, debe ser el servidor del sitio de administración central).
2. En la carpeta `Intel_SCS_Components > IntelSCS_SCCMAddon > SCCMAddon`, haga doble clic en **SCCMAddon.exe**. Aparecerá la pantalla de bienvenida.
3. Haga clic en **Siguiente**. Se abrirá la ventana correspondiente al acuerdo de licencia de usuario final.
4. Tras leer el acuerdo de licencia, seleccione **Acepto los términos del acuerdo de licencia** y haga clic en **Siguiente**. Aparecerá la ventana Configuración de SCCM.



5. El asistente detectará automáticamente la configuración de SCCM necesaria. Asegúrese de que la configuración que aparece en la ventana de configuración de SCCM sea correcta (si no es así, no continúe).

6. Haga clic en **Siguiente** para continuar. Se abrirá la ventana Seleccionar recopilación.



7. Lleve a cabo estos pasos para agregar los componentes Solutions Framework y Platform Discovery a SCCM:

   a. En la columna Ruta de la fila Solutions Framework, haga clic en ... y vaya a la carpeta `Intel_SCS_Components > Intel_SCS_Framework > Framework`.

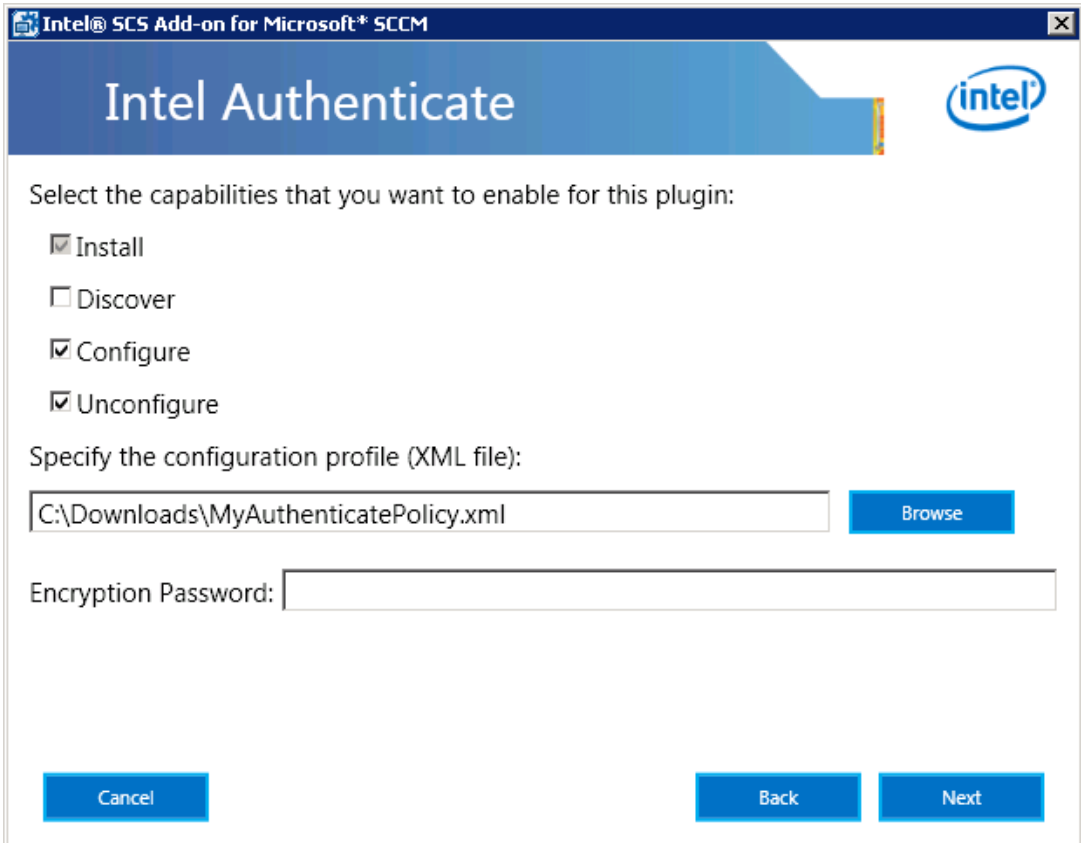
   b. Seleccione el archivo llamado `HostSolutionManagerInstaller.msi` y haga clic en **Abrir**. La ruta del archivo se actualizará en la columna Ruta.

   c. En la columna Ruta de la fila Platform Discovery, haga clic en ... y vaya a la carpeta `Intel_SCS_Components > Platform_Discovery`.

   d. Seleccione el archivo llamado `PlatformDiscovery.exe` y haga clic en **Abrir**. La ruta del archivo se actualizará en la columna Ruta.

   e. En la columna Acción de las filas Solutions Framework y Platform Discovery, asegúrese de que esté seleccionada la acción **Instalar**.

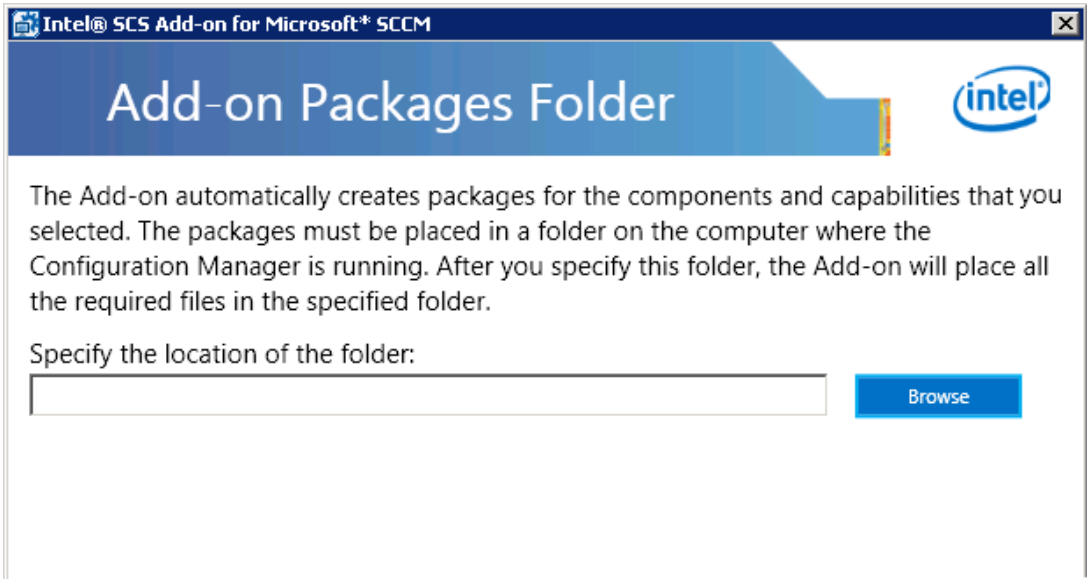
8. En la columna Acción del componente Intel AMT, seleccione **Sin cambios**. (La integración de Intel AMT con SCCM queda fuera del ámbito de esta guía Para obtener más información, consulte la documentación del complemento).
9. Realice estos pasos para agregar el complemento de Intel Authenticate a SCCM:
   a. Haga clic en **Agregar** y vaya a la carpeta `HostPluginInstaller` .
   b. Seleccione el archivo `AuthenticatePlugin.msi` y haga clic en **Abrir**. Intel Authenticate se agregará a la lista de componentes y la ruta del archivo se actualizará en la columna Ruta.
   c. En la columna Acción de la fila Intel Authenticate, asegúrese de que la acción **Instalar** esté seleccionada.
10. Haga clic en **Siguiente**. Aparecerá la ventana de Intel Authenticate.



11. Seleccione solo las casillas de verificación **Configurar** y **Anular configuración**. (La casilla de verificación "Instalar" es obligatoria y ya aparece seleccionada).

> **Nota:**
>
> La capacidad Descubrir no se admite actualmente en el complemento de Intel Authenticate. Si selecciona esta casilla de verificación por error, el complemento creará objetos para esta capacidad aunque el complemento no los pueda utilizar.

12. Haga clic en **Examinar** y seleccione el perfil XML (directiva) creado para Intel Authenticate (consulte Creación de una directiva en la página 44).
13. Haga clic en **Siguiente**. Se abrirá la ventana Carpeta de paquetes del complemento.



Durante la instalación, el complemento crea automáticamente paquetes para los componentes seleccionados para su instalación. Por cada paquete, el complemento crea una carpeta que contiene los archivos que necesita el paquete. Para mayor simplicidad, todas estas carpetas estarán ubicadas en una única carpeta principal que se define en esta ventana. La carpeta principal debe estar en una ubicación a la que Configuration Manager siempre pueda acceder.

a. Haga clic en **Examinar**. Aparecerá la ventana Buscar carpeta.
b. Navegue a una ubicación a la que siempre pueda acceder Configuration Manager y cree una carpeta principal para los paquetes del complemento. Asigne a la carpeta un nombre que le ayude a reconocer su finalidad.
c. Haga clic en **Aceptar** para cerrar la ventana Buscar carpeta.

14. Haga clic en **Siguiente**. El asistente instalará los componentes seleccionados. Cuando termine, haga clic en **Siguiente** Aparecerá la ventana Finalizado correctamente.
15. Haga clic en **Finalizar** para salir del asistente. Los elementos creados por el complemento están listos para su uso (consulte ¿Qué crea el complemento en SCCM? en la página 15).

6.5 Creación de un paquete de instalación del cliente

El complemento no crea un paquete de instalación para instalar Intel Authenticate en las plataformas cliente. (El paquete "Intel Authenticate: Instalación" solo instala el complemento de host. Para obtener más información, consulte ¿Qué crea el complemento en SCCM? en la página 15).

Esto significa que debe crear el paquete necesario (incluyendo la secuencia de tareas y el despliegue) para desplegar los instaladores de Intel Authenticate en las plataformas cliente. Puede crear este paquete manual o automáticamente mediante un pequeño archivo ejecutable que se proporciona en el paquete de integración de SCCM.

Para crear automáticamente el paquete del instalador de Authenticate:

1. Desde el paquete de integración de SCCM, copie la carpeta `AuthenticateInstallers` en la raíz de la carpeta que definió en la ventana de la carpeta de paquetes de complementos del instalador de complementos. (La carpeta que definió en el paso 13 de Instalación del complemento en la página 49).
2. En el paquete de integración de SCCM, abra un símbolo del sistema administrativo en esta carpeta:

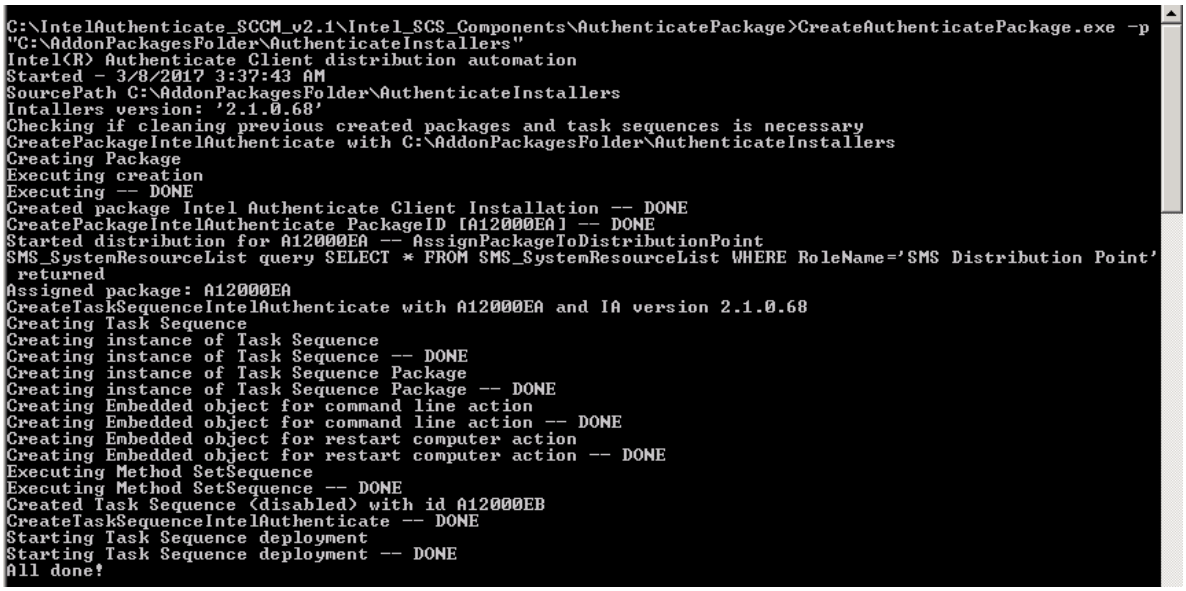
   `Intel_SCS_Components > AuthenticatePackage`.
3. Introduzca este comando:

   ```
   CreateAuthenticatePackage.exe -p [ruta de la carpeta AuthenticateInstallers]
   ```

   Por ejemplo, si su carpeta de paquetes de complementos se llama "AddonPackagesFolder" y está ubicada en la unidad C:

   ```
   CreateAuthenticatePackage.exe -p
   "C:\AddonPackagesFolder\AuthenticateInstallers"
   ```

   Este es un ejemplo del resultado que se obtiene si el comando se ejecuta correctamente:



4. Compruebe que se hayan creado los componentes siguientes.
   - Paquete: `Intel Authenticate Client Installation`
   - Secuencia de tareas: `Intel Authenticate Client Installation`
   - Despliegue: `Intel Authenticate Client Installation`

Para crear manualmente el paquete del instalador de Intel Authenticate:

1. Desde el paquete de integración de SCCM, copie la carpeta `AuthenticateInstallers` en la raíz de la carpeta que definió en la ventana de la carpeta de paquetes de complementos del instalador de complementos. (La carpeta que definió en el paso 13 de Instalación del complemento en la página 49).
2. Cree un paquete nuevo y defina la carpeta `AuthenticateInstallers` como origen:
   a. En el panel Navegación, seleccione **Biblioteca de software > Introducción > Administración de aplicaciones > Paquetes**.
   b. En el panel de la derecha, haga clic con el botón derecho y seleccione **Crear paquete.** Se abrirá el Asistente para crear paquetes y programas.
   c. En el campo **Nombre**, defina un nombre para el paquete. Por ejemplo, `Intel Authenticate Client Installation`.
   d. (Opcional) Introduzca el resto de información de referencia sobre el paquete, como la descripción, el fabricante, el idioma y la versión.
   e. Seleccione esta casilla de verificación: **This package contains source files** (Este paquete contiene archivos de origen).
   f. En la carpeta de origen, haga clic en **Examinar**. Se abrirá la ventana Establecer carpeta de origen.
   g. Seleccione **Carpeta local en el servidor del sitio** y haga clic en **Examinar** para navegar a la carpeta `AuthenticateInstallers` que ha copiado en la carpeta de paquetes del complemento.
   h. Haga clic en **Seleccionar carpeta** y, a continuación, haga clic en **Aceptar** y en **Siguiente**. Se abre la ventana Tipo de programa.
   i. Seleccione **No crear un programa** y, a continuación, haga clic en **Siguiente** dos veces para llegar a la pantalla de finalización.
   j. Haga clic en **Cerrar**. El paquete ya se puede establecer para su distribución y despliegue.

3. Distribuya el paquete en los puntos de distribución:

    a. Haga clic con el botón derecho en el nuevo paquete y seleccione **Propiedades**. Se abrirá la ventana Propiedades.

    b. En la ficha Configuración de distribución, seleccione **Descargar contenido automáticamente cuando los paquetes se asignen a puntos de distribución** y haga clic en **Aceptar**. Se cerrará la ventana Propiedades.

    c. Haga clic con el botón derecho otra vez en el nuevo paquete y seleccione **Distribuir contenido**. Se abrirá el asistente para la distribución de contenido.

    d. Haga clic en **Siguiente**. Se abrirá la ventana Destino de contenido.

    e. En la lista desplegable **Agregar**, seleccione **Punto de distribución**. Se abrirá la pantalla Agregar puntos de distribución con una lista de puntos de distribución.

    f. Seleccione la casilla de verificación de los puntos de distribución requeridos y haga clic en **Aceptar**.

    g. Haga clic en **Siguiente** hasta que se muestre la pantalla de finalización y, a continuación, haga clic en **Cerrar**.

4. Cree una nueva secuencia de tareas para instalar el paquete de software de Intel Authenticate:

    a. En el panel de navegación, seleccione **Biblioteca de software > Introducción > Sistemas operativos > Secuencias de tareas**.

    b. Haga clic con el botón derecho en la secuencia de tareas **Intel Authenticate: Installation** y seleccione **Copiar**. Se creará una nueva tarea llamada Intel Authenticate: Installation - Axxxxx (donde Axxxxx distingue esta tarea de la original).

    c. Haga clic con el botón derecho en la nueva tarea y seleccione **Propiedades**. Cambie el nombre y la descripción para describir la instalación del paquete. Por ejemplo, Nombre: "Instalación del cliente Intel Authenticate" y Descripción: "Instala Intel Authenticate".

    d. Haga clic en **Aceptar**. Se cerrará la ventana Propiedades.

    e. Haga clic con el botón derecho en la nueva tarea y seleccione **Editar**. Vuelva a escribir el nombre y la descripción que introdujo en la ventana Propiedades en el paso anterior.

    f. En la sección Línea de comandos, cambie el comando existente por este: `"powershell.exe" -ExcecutionPolicy Bypass -File ".\Install_IA.ps1"`.

    g. En la sección Paquete, haga clic en **Examinar** y seleccione el paquete que creó en el paso 2.

    h. Haga clic en **Aceptar**.

5. Despliegue la secuencia de tareas y asóciela a la recopilación Intel Authenticate: Exists:

   a. Haga clic con el botón derecho en la secuencia de tareas que creó en el paso anterior y seleccione **Desplegar**. Aparece un mensaje emergente para preguntarle si desea activar la secuencia de tareas.

   b. Haga clic en **No**. Se abrirá el asistente de despliegue de software.

   c. En la sección Recopilación, haga clic en **Examinar**. Se abrirá la ventana que permite seleccionar la recopilación.

   d. En la lista, seleccione la recopilación **Intel Authenticate: Exists** y haga clic en **Aceptar**.

   e. Haga clic en **Siguiente**. Se abrirá la ventana de configuración de implementación.

   f. En la lista desplegable **Propósito**, seleccione **Obligatorio** y, a continuación, haga clic en **Siguiente**. Se abrirá la ventana Programa.

   g. Haga clic en **Nuevo**. Se abrirá la ventana Programa de asignaciones. Seleccione **Asignar inmediatamente después de este evento** y haga clic en **Aceptar**. Se cerrará la ventana Programa de asignaciones.

   h. Las pantallas restantes especifican la configuración de despliegue. Haga clic en **Siguiente** (acepte la configuración predeterminada) hasta que aparezca la ventana Finalización con un resumen de la configuración de despliegue.

   i. Haga clic en **Cerrar**. El paquete de despliegue de Intel Authenticate ya está listo para su uso.

6.6 Activación de las secuencias de tareas (en orden)

De forma predeterminada, las secuencias de tareas creadas por el complemento están desactivadas. Tendrá que activarlas para poder utilizarlas. Es importante activar las secuencias de tareas en el orden recomendado. Al activar una secuencia de tareas, no olvide definir una planificación de periodicidad de acuerdo con la directiva de su empresa.

El orden recomendado para activar las secuencias de tareas es:

1. La secuencia de tareas se ejecutará en la recopilación "Intel SCS: Platform Discovery". Active la secuencia de tareas "Intel SCS: Platform Discovery".

   Nota:

   Una vez completada esta secuencia de tareas en los miembros de la recopilación, se rellenarán las recopilaciones de tipo "Exists". Asegúrese de que la recopilación "Intel Authenticate: Exists" se haya rellenado antes de continuar.

2. Active la secuencia de tareas creada para instalar el software de Intel Authenticate (consulte Creación de un paquete de instalación del cliente en la página 53). Asegúrese de que la secuencia de tareas se ejecute en la recopilación "Intel Authenticate: Exists".
3. Active la secuencia de tareas "Intel SCS: Solutions Framework Installation". La secuencia de tareas se ejecutará en la recopilación "Intel SCS: Solutions Framework Not Installed".
4. Active la secuencia de tareas "Intel Authenticate: Installation". La secuencia de tareas se ejecutará en la recopilación "Intel Authenticate: Plugin Not Installed". Una vez ejecutada esta secuencia de tareas, asegúrese de que la secuencia de tareas "Intel SCS: Platform Discovery" se ejecute de nuevo para actualizar la recopilación "Intel Authenticate: Plugin Available".
5. Active la secuencia de tareas "Intel Authenticate: Configuration". La secuencia de tareas se ejecutará en la recopilación "Intel Authenticate: Plugin Available".

6.7 Modificación de los componentes del complemento

Puede ejecutar el complemento varias veces para modificar los elementos definidos en SCCM por parte del complemento. Esto incluye agregar y eliminar componentes, además de cambiar la configuración de los componentes instalados.

Los elementos creados en SCCM por el complemento están listos para su uso sin necesidad de personalización. No obstante, podría interesarle realizar cambios y personalizaciones en la configuración predeterminada que el complemento crea. Si selecciona la acción "Cambiar" para un componente (en la ventana de selección de componentes), todos los elementos existentes de dicho componente se eliminan y reemplazan. Esto implica que se perderán las personalizaciones realizadas en los objetos en SCCM o los archivos de las carpetas de los paquetes.

Si desea editar los paquetes de un componente o realizar cambios en ellos, haga una copia de la carpeta correspondiente a los paquetes relevantes. A continuación, cambie el nombre de la carpeta antes de editar o realizar cambios (y cree secuencias de tareas nuevas para usar esta nueva carpeta de paquetes). Así se asegurará de que los cambios realizados no se eliminen si ejecuta el complemento de nuevo y decide cambiar el componente.

6.8 Cambiar la directiva

Si desea cambiar la directiva una vez desplegada, debe volver a ejecutar el complemento y seleccionar la nueva directiva.

Para cambiar la directiva:

1. En la subcarpeta `SCCMAddon`, haga doble clic en **SCCMAddon.exe**. Aparecerá la pantalla de bienvenida.
2. Seleccione **Modificar configuración del complemento**.
3. Haga clic en **Siguiente**. Se abrirá la ventana Seleccionar recopilación.
4. En la columna Acción de la fila Intel Authenticate, seleccione **Cambiar**.
5. Haga clic en **Siguiente**. Aparecerá la ventana de Intel Authenticate.
6. En la sección "Seleccionar las funciones que desea activar para este complemento", asegúrese de que las casillas de verificación **Configurar** y **Anular configuración** están seleccionadas.
7. Haga clic en **Examinar** y seleccione el nuevo archivo XML de directivas (observe que el botón Siguiente solo está activado si el archivo XML está seleccionado).
8. Haga clic en **Siguiente**. Aparecerá la ventana Configuración de la cuenta de usuario. Si se define una cuenta de usuario en esta ventana durante la instalación, introduzca la contraseña de la cuenta de usuario.
9. Haga clic en **Siguiente**. Se abrirá la ventana Carpeta de paquetes del complemento.
10. Haga clic en **Siguiente**. Se muestra un mensaje indicando que los archivos y scripts existentes en las carpetas de paquetes se sobrescribirán.
11. Haga clic en **Aceptar**. Se abre la ventana Progreso de modificación y muestra el progreso de las modificaciones. Cuando termine, haga clic en **Siguiente** Aparecerá la ventana Finalizado correctamente.
12. Haga clic en **Finalizar** para salir del asistente.

6.9 Flujo de despliegue con SCCM

Si ya ha desplegado una versión anterior de Intel Authenticate en la red, puede actualizar las instalaciones existentes a la versión 3.0.

Nota:

Las directivas creadas en la versión 3.1 no se admiten en plataformas que tienen instaladas versiones anteriores de Intel Authenticate. Asegúrese de actualizar las plataformas cliente a la versión 3.1 antes de configurar las directivas creadas con la versión 3.1. Las directivas establecidas con versiones anteriores seguirán funcionando con la versión 3.1.

Para actualizar a la versión 3.1:

1. Si utiliza Proximidad Bluetooth, es recomendable que solicite a los usuarios que actualicen Intel Authenticate a la versión más reciente en sus teléfonos. (Excepto para usuarios de Windows 10, versión 1607, que no hayan instalado la aplicación Intel Authenticate).

   Nota:

   En Windows 10, versión 1703 o superior, se cancelará cualquier inscripción existente de un iPhone tras la actualización. El usuario no podrá autenticarse con su teléfono hasta que lo haya registrado. Se pedirá al usuario que vuelva a registrar su teléfono (e instalar la aplicación Intel Authenticate) para activar el nivel de seguridad "Protegido" del factor de Proximidad Bluetooth. Si desea activar el nivel de seguridad "Débil" para iPhone en Windows 10, deberá aplicar una nueva directiva creada con la versión 3.1.

2. Sustituya la versión anterior de los instaladores de Intel Authenticate:

   a. En el servidor SCCM, busque la carpeta en la que se encuentran los instaladores de la versión anterior de Intel Authenticate. (La carpeta `AuthenticateInstallers` de la carpeta de paquetes de complementos que creó al instalar el complemento).

   b. Elimine los archivos del instalador de la versión anterior y la secuencia de comandos de instalación de PowerShell (`Install_IA_v0.1.ps1`).

   c. Desde la versión 3.1 del paquete de integración de SCCM, copie el contenido de la carpeta `AuthenticateInstallers` en la carpeta `AuthenticateInstallers` del servidor de SCCM.

> **Nota:**
>
> No es necesario volver a ejecutar el instalador de complementos. Los componentes existentes que se instalaron mediante el instalador de complementos en el servidor de SCCM ya contienen la información necesaria para detectar un flujo de actualización. Lo único que necesita actualizar es el paquete de instalación de cliente que ha creado (consulte Creación de un paquete de instalación del cliente en la página 53). El modo de actualizar el paquete de instalación del cliente depende de cómo lo haya creado al instalar la versión anterior:
>
> - Si utilizó el procedimiento del método automático, siga solo el paso 3.
> - Si utilizó el procedimiento manual, siga solo el paso 4.

3. Si creó originalmente los componentes mediante el método automático, siga estos pasos:

   a. Con la versión 3.1 del paquete de integración de SSCM, repita los pasos 2 y 3 del procedimiento automático descrito en Creación de un paquete de instalación del cliente en la página 53.

   b. Active la secuencia de tareas de `Intel Authenticate Client Installation`. (Después de ejecutar el archivo `CreateAuthenticatePackage.exe`, la secuencia de tareas actualizada se recrea como desactivada de forma predeterminada).

4. Si creó originalmente los componentes mediante el método manual, siga estos pasos:

   a. En el panel de navegación, seleccione **Biblioteca de software** > **Descripción general** > **Sistemas operativos** > **Secuencias de tareas**.

   b. Haga clic con el botón derecho en la secuencia de tareas que creó originalmente para el paquete de despliegue y seleccione **Editar**. Se abre el editor de secuencias de tareas.

   c. En la línea de comandos, cambie el número de versión existente por el número de versión 3.0 nueva de los archivos del instalador.

   d. En la lista desplegable Agregar, seleccione **Reiniciar equipo**. Se agrega una nueva tarea a la lista de tareas.

   e. (Opcional) En el campo Nombre, cambie el nombre de la tarea por el de "Reiniciar el equipo después de la actualización" y añada una descripción.

   f. Seleccione **Sistema operativo predeterminado instalado actualmente**.

   g. Asegúrese de que esta casilla de verificación está seleccionada: **Notificar al usuario antes de reiniciar**.

   h. En la sección Mensaje de notificación, añada un mensaje en el que indique al usuario que se debe reiniciar el equipo.

   i. Seleccione la pestaña **Opciones**.

   j. En la lista desplegable **Agregar condición**, seleccione **Variable de secuencia de tareas**. Se abre la ventana Variable de secuencia de tareas.

   k. Defina estos valores para la variable:

      - Variable: `_SMSTSLastActionRetCode`
      - Condición: igual
      - Valor: 3010

   l. Haga clic dos veces en **Aceptar** para cerrar el editor de secuencias de tareas.

7 Solución de problemas

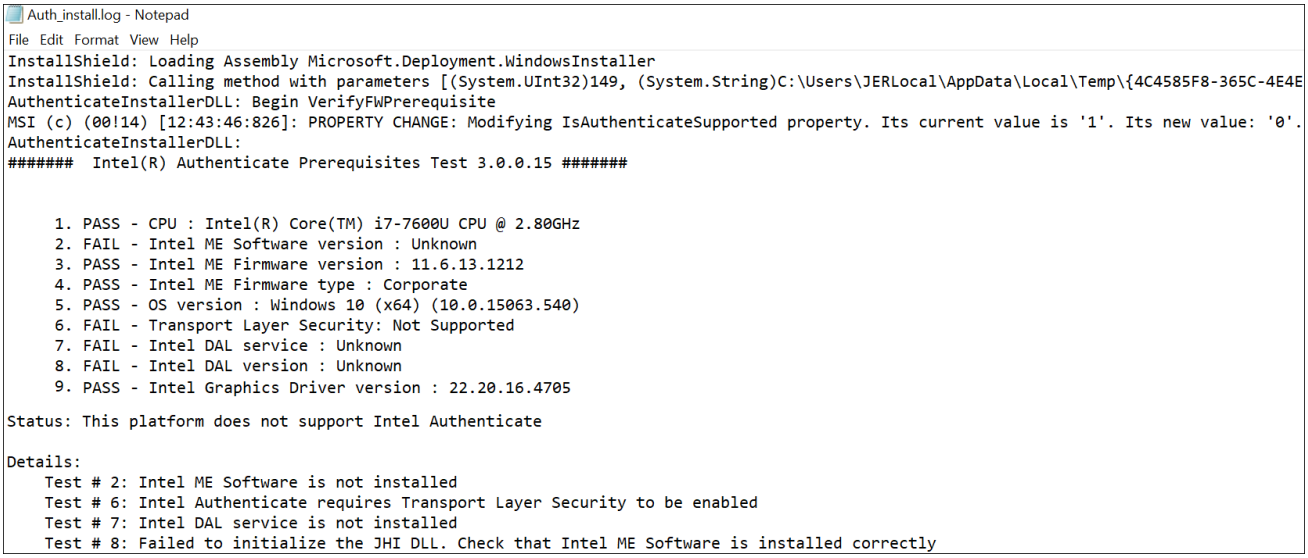
Esta sección describe problemas que podrían surgir al utilizar Intel Authenticate y proporciona las soluciones.

Nota:

Para obtener información sobre las opciones de asistencia técnica para Intel Authenticate, visite Asistencia al cliente de Intel.

7.1 Solución de problemas de instalación

Antes de la instalación, el instalador ejecuta la prueba de requisitos previos /P de la herramienta de comprobación. Si la prueba falla, la instalación se interrumpe y los resultados se añaden al archivo de registro del instalador.



7.2 Solución de problemas de registro

Esta sección explica cómo solucionar los problemas que pueden producirse durante el proceso de registro.

Para obtener más información sobre el proceso de registro, consulte la guía de registro en el paquete de integración.

La aplicación de gestión de factores no se abre, o se bloquea nada más abrirla

La aplicación de gestión de factores requiere que se instale la versión 4.5.2 o superior de .NET Framework en la plataforma. En algunos casos, es posible abrir la aplicación si hay una versión anterior de .NET Framework instalada, aunque esta no funcionará correctamente. Si tiene problemas con la aplicación de gestión de factores, asegúrese de que está instalada la versión 4.5.2 o superior de .NET Framework en la plataforma.

La aplicación de gestión de factores muestra el mensaje: "No hay factores que administrar"

Este mensaje aparece cuando se ha instalado Intel Authenticate pero no se ha implementado una directiva válida. Asegúrese de haber desplegado la directiva en la plataforma y de que la directiva sea una directiva válida con una acción y factor de autenticación como mínimo.

El usuario ha aplazado el registro, pero ahora quiere registrar sus factores

El usuario puede abrir manualmente la aplicación de gestión de factores; para ello, hay que abrir la ventana de búsqueda y escribir "Intel Authenticate".

Problemas con el registro del factor de proximidad Bluetooth

El registro del factor de proximidad Bluetooth incluye diversos pasos, cada uno de los cuales puede fallar por distintos motivos. A continuación se describen los pasos principales en orden, junto con los problemas que podrían surgir y sus soluciones:

1. Asegúrese de que la función de Bluetooth está activada tanto en el equipo del usuario como en el teléfono que el usuario desea registrar.
2. El nivel de seguridad "Protegido" del factor de Proximidad Bluetooth requiere instalar la aplicación Intel Authenticate en el teléfono. Asegúrese de que el usuario haya instalado la aplicación en el teléfono que está intentando registrar. La página Proximidad Bluetooth de la aplicación de gestión de factores incluye vínculos para descargar e instalar la aplicación. Puede que el usuario haya continuado el proceso de registro sin haber instalado antes la aplicación. Pida al usuario que busque y abra la aplicación en su teléfono. Necesitarán utilizar la app más tarde en el proceso de registro.
3. El primer paso del proceso de registro del factor Proximidad Bluetooth consiste en detectar el teléfono del usuario. La aplicación de gestión de factores muestra una lista de los teléfonos cercanos. La lista incluye los teléfonos emparejados y los no emparejados. Si el teléfono del usuario no aparece en la lista:
   - En el caso de los teléfonos Android, solicite al usuario que abra la aplicación y haga clic en el botón "Hacer reconocible".
   - Para iPhone:
     - Nivel de seguridad "Protegido": la aplicación Intel Authenticate debe estar abierta en el teléfono para que la aplicación de gestión de factores pueda detectar el teléfono. Pida al usuario que abra la aplicación en el teléfono si aún no lo ha hecho.
     - Nivel de seguridad "Débil": solicite al usuario que abra la página Configuración > Bluetooth en su teléfono.
   - En la aplicación de gestión de factores, pida al usuario que haga clic en **Actualizar la lista** para buscar el teléfono de nuevo.
   - Si el usuario del teléfono todavía no aparece en la lista, asegúrese de que Windows puede detectar el teléfono. En Windows, pida al usuario que compruebe si su teléfono aparece en la lista de dispositivos Bluetooth detectados por Windows. La aplicación de gestión de factores solo puede detectar y registrar los teléfonos que Windows haya detectado correctamente. Si Windows no puede detectar el teléfono, deberá solucionar los problemas subyacentes de conectividad Bluetooth para que el usuario pueda registrar su teléfono.
   - Si el teléfono ya está emparejado en Windows pero sigue sin aparecer en la lista, solicite al usuario que compruebe el estado del teléfono en la ventana Administrador de dispositivos. El teléfono emparejado del usuario aparece en la sección de Bluetooth. Si aparece un icono de advertencia amarillo junto al nombre del teléfono, haga clic con el botón derecho en el nombre del teléfono y seleccione **Deshabilitar** y, después, **Habilitar**. La aplicación de gestión de factores no puede detectar teléfonos que se hayan desactivado o que tengan advertencias en la ventana del Administrador de dispositivos.

4. Una vez que el teléfono del usuario se haya detectado correctamente, el usuario deberá seleccionarlo en la lista. Si el teléfono no está emparejado, se mostrará un código de emparejamiento y se pedirá al usuario que confirme el emparejamiento del teléfono. El usuario debe confirmar esta solicitud tanto en el teléfono como en el equipo:
   - En ocasiones, el código de emparejamiento no se detecta fácilmente en el teléfono porque puede ejecutarse en segundo plano. Si el usuario oye un sonido de notificación pero no se ve el código de emparejamiento, pídale que se desplace hacia abajo en la pantalla para buscarlo.
   - Si el usuario ha cometido un error (por ejemplo, si ha confirmado en el teléfono pero denegado en el equipo), deberá esperar a que la conexión Bluetooth se "libere" para volver a intentarlo.
5. Con nivel de seguridad "Protegido", tras emparejar el teléfono, deberá registrarlo en Intel Authenticate:
   - Antes de continuar, el usuario debe abrir la aplicación de Intel Authenticate y asegurarse de que aparezca un mensaje de tipo "A la espera de la señal". Si la aplicación no está abierta, aparecerá un mensaje de error. Para continuar, el usuario debe hacer clic en **Volver a intentarlo** en la aplicación de gestión de factores.
   - La aplicación de gestión de factores mostrará un código. El usuario deberá introducir este código en la aplicación Intel Authenticate. Si se introduce un código incorrecto, se mostrará un mensaje de error tanto en la aplicación de gestión de factores como en el teléfono. Para continuar, el usuario deberá hacer clic en **Volver a empezar** en la aplicación y en **Volver a intentarlo** en la aplicación de gestión de factores.

7.3 Solución de problemas de inicio de sesión en SO

Esta sección explica cómo solucionar los problemas que pueden producirse al utilizar la acción de inicio de sesión en SO.

No se puede iniciar sesión en el SO con Intel Authenticate

A continuación se explican los motivos más comunes por los que un usuario podría ser incapaz de iniciar sesión en Windows con Intel Authenticate:

- Después del registro, el usuario intentó iniciar sesión con Intel Authenticate sin haber iniciado sesión primero con su contraseña de Windows. El primer inicio de sesión después del registro debe realizarse utilizando la contraseña de Windows. A continuación, el usuario puede empezar a iniciar sesión utilizando Intel Authenticate.
- El usuario ha cambiado su contraseña. El primer inicio de sesión después de cambiar la contraseña de Windows debe realizarse utilizando la contraseña de Windows. A continuación, el usuario puede seguir iniciando sesión con Intel Authenticate.
- El usuario no ha registrado suficientes factores requeridos para la acción de inicio de sesión en el SO. Si esta es la causa del problema, el estado de la sección Inicio de sesión en SO mostrará el mensaje "No se han registrado suficientes factores" en la aplicación de gestión de factores.
- Uno de los servicios requeridos no está en ejecución (consulte Client y Engine en la página 10).
- Si se ha definido el factor Proximidad Bluetooth como factor obligatorio, el inicio de sesión solo podrá realizarse si se detecta el teléfono registrado (consulte Solución de problemas de Proximidad Bluetooth en la página 69).

Cuentas de usuario no compatibles

Intel Authenticate no admite:

- Cuentas de sistema Windows integradas.
- Cuentas de usuario sin contraseña o con una contraseña en blanco. (Después del registro con Intel Authenticate, ya no será posible iniciar sesión en Windows con la cuenta de usuario).

7.4 Solución de problemas de inicio de sesión de SO con tarjeta inteligente

Esta sección explica cómo solucionar los problemas que pueden producirse al utilizar la acción de inicio de sesión en SO.

El inicio de sesión tarda mucho en un entorno exclusivo de intranet

En las plataformas cliente conectadas a una intranet pero sin acceso a Internet, la opción de inicio de sesión de SO con una tarjeta inteligente puede tardar hasta 17 segundos. Esto se debe a que se realizan varios intentos de acceder a Internet para comprobar la lista de revocación de certificados. Para solucionar este problema, agregue una clave al registro de las plataformas cliente en esta ubicación:

`HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters`

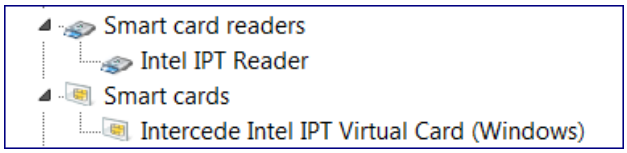
Agregue un nuevo valor DWORD con estas propiedades:

- Nombre del valor: `UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors`
- Datos del valor: 1

La opción de tarjeta inteligente integrada de forma predeterminada no funciona

Al utilizar la opción de tarjeta inteligente integrada de forma predeterminada:

- Asegúrese de que ha definido la plantilla correctamente (consulte Definición de la plantilla de CA para la tarjeta inteligente en la página 37).
- Compruebe en el almacén de certificados personales del usuario que se ha expedido un certificado basado en la plantilla "Intel Authenticate Smartcard Os Logon" (Inicio de sesión en el sistema operativo de la tarjeta inteligente de Intel Authenticate).
- En Administrador de dispositivos:
  - Asegúrese de que existe "Intel IPT Reader" y también de que es la primera entrada de la lista.
  - Asegúrese de que existe la tarjeta inteligente denominada "Intercede Intel IPT Virtual Card".



Nota:

En Windows 10, las "tarjetas inteligentes" están ocultas de forma predeterminada. Para ver estos dispositivos, seleccione **Ver > Mostrar dispositivos ocultos**.

Si falta alguno de estos componentes, significa que se ha producido un problema durante la instalación.

Nota:

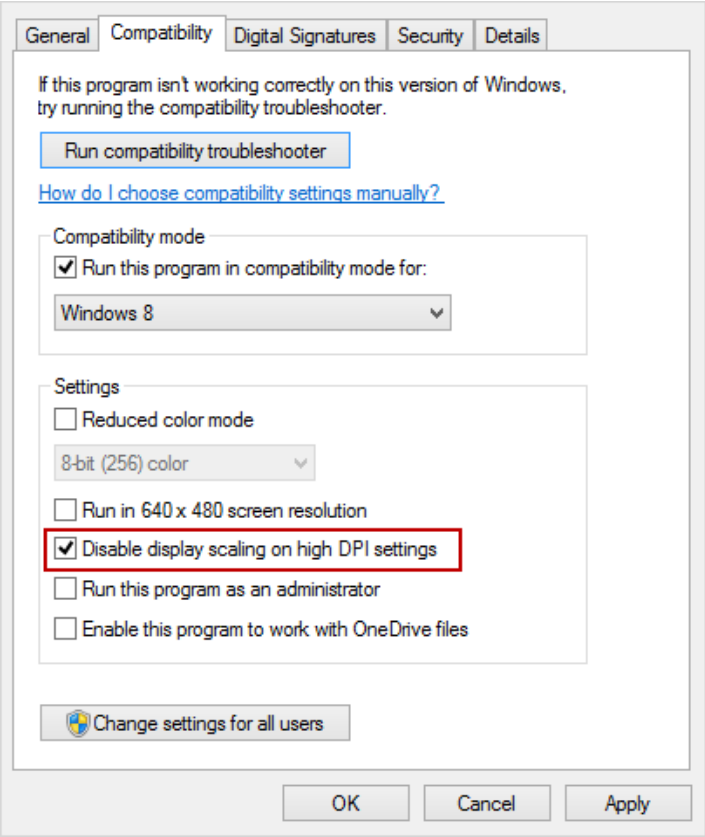
Si se utiliza la opción del administrador de certificados externos, los nombres de estos componentes son diferentes. Para solucionar problemas mediante la opción del administrador de certificados externos, consulte la documentación de MyID.

7.5 Solución de problemas de inicio de sesión en VPN

En ciertas circunstancias, durante el inicio de sesión en VPN, la pantalla de la aplicación cliente de VPN se "contrae" y el usuario no puede ver el teclado de código PIN para introducir su código PIN protegido. Este problema solo se produce si se cumplen estas dos condiciones:

- El código PIN protegido está definido como factor de autenticación para la acción Inicio de sesión en VPN.
- La plataforma tiene una configuración de PPP elevada para el texto y otros elementos.

Para solucionar este problema, hay que cambiar una opción de configuración de compatibilidad de la aplicación cliente de VPN utilizada en la plataforma. La opción es **Deshabilitar el ajuste de escala de la pantalla si se usa la configuración elevada de ppp**, y está situada en la ficha Compatibilidad de la aplicación cliente de VPN.

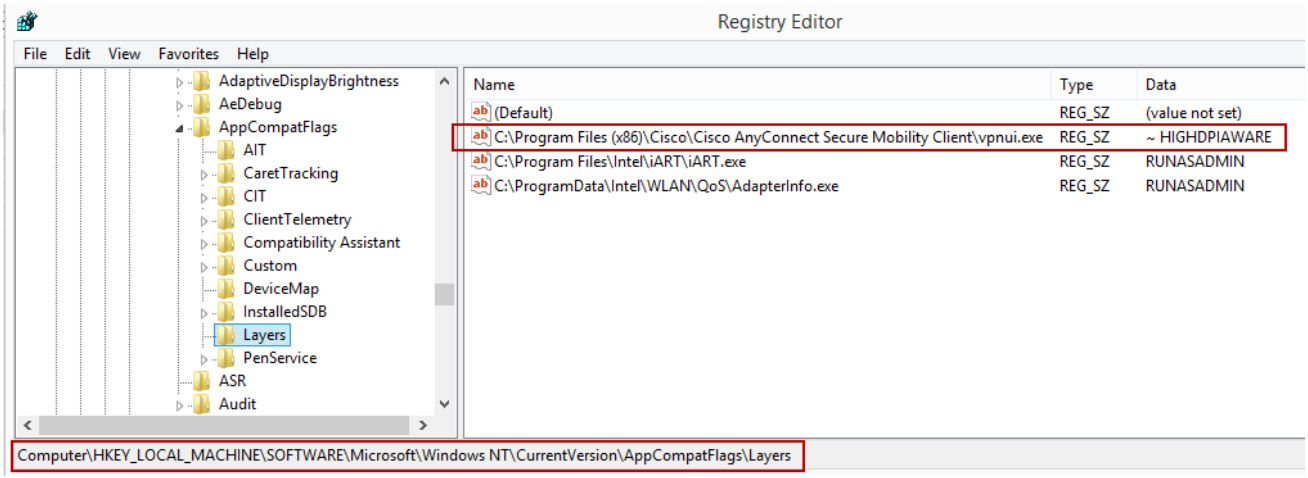


Esta opción se puede definir directamente en el Registro de la plataforma. Si desea aplicar esta configuración a todos los usuarios de la plataforma, defina la opción en esta ubicación:

`HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\AppCompatFlags\Layers`

Agregue un nuevo valor de cadena con estas propiedades:

- Nombre del valor: el nombre y la ruta completa del archivo ejecutable correspondiente a la aplicación cliente de VPN
- Datos del valor: `~ HIGHDPIAWARE`



7.6 Solución de problemas de Proximidad Bluetooth

Estas son las razones más habituales por las que Proximidad Bluetooth puede dejar de funcionar:

- La aplicación Intel Authenticate no se está ejecutando en el teléfono del usuario (solo nivel de seguridad "Protegido"):
  - En muchos teléfonos Android, las aplicaciones en segundo plano no tienen permiso para iniciarse automáticamente. Asegúrese de que el usuario haya activado la aplicación de Intel Authenticate para que siempre se reinicie automáticamente. Después de actualizar el sistema operativo de Android en algunos teléfonos, es posible que tenga que reiniciar la aplicación manualmente.
  - Si el usuario usa un iPhone, asegúrese de que no haya cerrado accidentalmente la aplicación. Además, si el usuario ha reiniciado su iPhone, tendrá que abrir la aplicación una vez y ponerla en primer plano. A continuación, pídale que espere un minuto para que el equipo y el iPhone restablezcan las comunicaciones. Después, puede cambiar la aplicación a segundo plano (pero no debe cerrarla).
- Hay problemas de conexión Bluetooth con el teléfono del usuario. Pida al usuario que reinicie su teléfono.
- El teléfono del usuario no está dentro del alcance de su equipo.
- La función Bluetooth está desactivada en el equipo o el teléfono del usuario.
- El teléfono del usuario tiene poca batería, está en modo avión o se encuentra en un modo de suspensión en el que se ha desactivado la función de Bluetooth.
- El usuario ha desinstalado la aplicación del teléfono. Al desinstalar la aplicación, se interrumpe la conexión para el registro con el equipo (solo nivel de seguridad "Protegido"). La única forma de solucionar este problema es restablecer la directiva y pedir al usuario que vuelva a registrar sus factores.
- El usuario ha desemparejado su iPhone del equipo. Un iPhone genera una nueva dirección Bluetooth exclusiva cada vez que se empareja. Esto implica que la dirección utilizada para emparejar el iPhone con Intel Authenticate ya no existe. La única forma de solucionar este problema es restablecer la directiva y pedir al usuario que vuelva a registrar sus factores.

7.7 Resolución de problemas de huellas digitales

Para utilizar el factor Huella digital, el usuario debe registrar previamente sus huellas digitales en Windows. Cualquier fallo al registrar huellas digitales en Windows debe resolverse antes de que pueda inscribirse y usar el factor Huella digital. Lo primero que hay que comprobar es que el usuario puede registrar sus huellas digitales correctamente en Windows. (Consulte también Solución de problemas de Windows Hello en la página 73).

Si el registro de huellas digitales en Windows se realiza correctamente, lo siguiente que hay que comprobar es que existen los archivos DLL y de registro correctos. Durante la instalación, Intel Authenticate detecta si hay un lector de huellas digitales instalado en la plataforma.

Nota:

- El tipo de lector de huellas digitales detectado determina el tipo de lector de huellas digitales que se integra. Para que la detección funcione correctamente, el controlador del lector de huellas digitales para el lector de huellas digitales específico se debe instalar antes de instalar Intel Authenticate.
- Una plataforma solo puede incluir un tipo de lector de huellas digitales.
- Puede utilizar la herramienta de comprobación para verificar el tipo de lector de huellas digitales detectado:

  ```
  Authenticate_Check.exe /f /v
  ```

  (El tipo de lector se muestra en el apartado de información).

Lectores de huellas digitales protegidas

El lector de huellas digitales protegidas que admite actualmente Intel Authenticate requiere que haya un controlador específico de Synaptics WBDI instalado en la plataforma. Si este controlador no está instalado, el lector de huellas digitales no se integrará con Intel Authenticate. Durante la instalación, el instalador del controlador agrega claves de registro (`DllPath`) en estas ubicaciones:

- `HKLM\SOFTWARE\Intel\Intel Authenticate\Engine\Factors\SecureFP`
- `HKLM\SOFTWARE\Wow6432Mode\Intel\Intel Authenticate\Engine\Factors\SecureFP`

La clave de registro `DLLPath` contiene la ruta del archivo DLL de huella digital que se integra con Intel Authenticate. Si esta clave de registro no existe (después de instalar el controlador), asegúrese de haber instalado el controlador correcto. Si instala el controlador correcto, las claves de registro y los archivos DLL se agregarán y el factor Huella digital protegida estará listo para su uso.

Lectores de huellas digitales ligeras

Si se detecta un lector de huellas digitales ligeras, el instalador de Intel Authenticate agrega claves de registro (`DllPath`) en estas ubicaciones:

- `HKLM\SOFTWARE\Intel\Intel Authenticate\Engine\Factors\SoftFP`
- `HKLM\SOFTWARE\Wow6432Mode\Intel\Intel Authenticate\Engine\Factors\SoftFP`

La clave de registro `DLLPath` contiene la ruta a un `SoftFingerprint.DLL` que instala el instalador de Intel Authenticate. Si esta clave no existe, deberá hacer lo siguiente:

1. Desinstale Intel Authenticate (y reinicie el equipo).
2. Instale el controlador del lector de huellas digitales.
3. Mediante la herramienta de comprobación, asegúrese de que el factor Huella digital ligera esté listo para su uso.
4. Instale Intel Authenticate y establezca la directiva de nuevo.

El registro de huellas digitales de Windows no lee las huellas

Para que el factor Huella digital de Intel Authenticate funcione correctamente, el lector de huellas digitales debe poder realizar una lectura fiable de la huella digital del usuario. Si el lector de huellas digitales tiene dificultad para leer las huellas digitales del usuario, la autenticación con el factor Huella digital de Intel Authenticate también dará problemas. El primer momento en el que se identifica este tipo de problema es durante el proceso de registro de las huellas digitales del usuario en Windows. Si Windows informa de problemas de reconocimiento de huellas digitales, debe investigar con el fabricante de la plataforma la causa de dichos problemas.

Nota:

Si se produce este problema, inténtelo con otro dedo. En ocasiones, las huellas de algunos dedos son demasiado finas o están demasiado deterioradas para que el lector de huellas digitales pueda realizar una lectura fiable.

Intel Authenticate bloquea el registro de Huella digital ligera

La aplicación de gestión de factores bloquea el registro del factor Huella digital si se dan las siguientes condiciones:

- La plataforma dispone de un lector de Huella digital ligera
- Ya existen las entradas de registro del lector de huellas digitales protegidas

Para resolver el problema:

1. Compruebe que el lector de huellas digitales es de "Huella digital ligera". (Ejecute `Authenticate_Check.exe /f /v`.)
2. Si no existe ninguna de estas entradas, elimínelas:
   - `HKLM\SOFTWARE\Intel\Intel Authenticate\Engine\Factors\SecureFP`
   - `HKLM\SOFTWARE\Wow6432Mode\Intel\Intel Authenticate\Engine\Factors\SecureFP`

7.8 Solución de problemas de Reconocimiento facial

Para utilizar el factor Reconocimiento facial, el usuario debe registrar previamente su rostro en Windows. Se debe resolver cualquier fallo al registrar el rostro en Windows para poder inscribirse y usar el factor Reconocimiento facial. Lo primero que hay que hacer es asegurarse de que el usuario puede registrar su rostro correctamente en Windows (consulte Solución de problemas de Windows Hello en la página siguiente).

La cámara no autentica el rostro del usuario

Durante la autenticación, aparecen mensajes en la pantalla que indican por qué la cámara tiene dificultades a la hora de autenticar su rostro. Normalmente, si se siguen las instrucciones, la autenticación se realizará correctamente. Las diferencias en el nivel de luz que recibe la cámara pueden provocar que falle la autenticación. La mayoría de los usuarios registra su rostro en el trabajo, pero la iluminación en casa suele ser muy diferente. Si la autenticación falla cuando se encuentra en casa, pídale al usuario que registre de nuevo el rostro allí. Para ello, solo tiene que hacer clic en **Mejorar el reconocimiento** en la página Opciones de inicio de sesión. No necesita volver a registrar el factor en Intel Authenticate.

7.9 Solución de problemas de Windows Hello

La solución de problemas de Windows Hello no se explica en esta guía. Pero como los factores Huella digital y Reconocimiento facial en Windows 10 dependen de Windows Hello, esta sección incluye información que puede resultarle útil. Para obtener las instrucciones completas sobre cómo solucionar problemas de Windows Hello, consulte la documentación de Microsoft.

Las opciones de configuración de Windows Hello están desactivadas en la página "Opciones de inicio de sesión"

En función de la versión de Windows, Microsoft ha realizado varios cambios en la forma en que se activa Windows Hello. En estos artículos se explican algunos de los cambios que suelen desactivar las opciones de Windows Hello:

- Cambios en el PIN cómodo
- Windows Hello para usuarios del dominio

La opción de reconocimiento facial no aparece en la página "Opciones de inicio de sesión"

Esta opción solo aparece si se ha instalado un controlador de cámara válido (consulte Requisitos previos para el reconocimiento facial en la página 23). En el Administrador de dispositivos, compruebe que se ha instalado un controlador de cámara compatible y que funciona correctamente. Consulte el sitio web del fabricante para comprobar que tiene instalado el controlador adecuado para la plataforma.

Nos hemos dado cuenta de que en algunas plataformas, como Dell XPS 13 9365, la opción de reconocimiento facial no está disponible en Windows 10 versión 1607. Pero, tras actualizar a Windows 10 versión 1703, la opción aparece en la página "Opciones de inicio de sesión".

La opción de huella digital no aparece en la página "Opciones de inicio de sesión"

Esta opción solo está disponible si se ha instalado un controlador de huella digital válido. En el Administrador de dispositivos, compruebe que se ha instalado un controlador de huella digital y que funciona correctamente. Consulte el sitio web del fabricante para comprobar que tiene instalado el controlador adecuado para la plataforma.

La GUI de registro de huellas digitales o reconocimiento facial no se abre

En algunas plataformas no ocurre nada al hacer clic en el botón de **configuración** para abrir la GUI de registro de huellas digitales o reconocimiento facial. En su lugar, la GUI parpadea durante una fracción de segundo, pero no se abre.

Para resolver el problema:

1. Abra el editor de directivas de grupo
2. Vaya a **Configuración del equipo** > **Configuración de Windows** > **Configuración de seguridad** > **Directivas locales** > **Opciones de seguridad**.
3. Haga clic con el botón derecho del ratón en **Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta Administrador integrado** y seleccione **Propiedades**.
4. Seleccione **Activado**.
5. Restart the computer. (ACCIÓN: Reinicie el sistema.)

6. Vuelva a la página Opciones de inicio de sesión y abra la GUI de registro de huellas digitales o reconocimiento facial.

7.10 Utilización de la herramienta de comprobación

La herramienta de comprobación es una herramienta basada en la interfaz de la línea de comandos que se encuentra en la carpeta `Tools > CheckTool`.

En la sintaxis de la interfaz de la línea de comandos no se distingue entre mayúsculas y minúsculas. La sintaxis es la siguiente:

```
Authenticate_Check.exe { /PreCheck | /Factors | /? } /Verbose
```

Marca	Detalles
`/PreCheck` (o `/P`)	Comprueba si la plataforma cumple los requisitos previos de instalación correspondientes a Intel Authenticate (consulte Requisitos previos para la instalación en la página 18)
`/Factors` (o `/F`)	Comprueba el estado de todos los factores de autenticación admitidos por Intel Authenticate
`Verbose`	Agrega información más detallada a la salida (solo cuando se usa con el indicador `/Factors`)
`?`	Ayuda

Nota:

La herramienta de comprobación:

- Debe ejecutarse desde un símbolo del sistema que se haya abierto con privilegios de administrador.
- Requiere .NET Framework versión 4.5.2 o posterior.
- Se basa en el controlador de Intel MEI para ejecutar algunas de las pruebas. Si el controlador de Intel MEI no está instalado, estas pruebas podrían fallar.
- Si en Windows 7 se muestra un mensaje que indica que falta un archivo DLL llamado "`api-ms-crt-runtime-[1-1-0.dll`", ejecute la actualización de Windows. Como alternativa, puede instalar este KB2999226.

7.10.1 Requisitos previos de instalación

Intel Authenticate solo se admite en las plataformas que satisfacen los requisitos previos de instalación (consulte Requisitos previos para la instalación en la página 18). El indicador `/PreCheck` de la herramienta de comprobación proporciona información sobre el estado de estos requisitos previos y determina si se admite la plataforma.

Nota:

- Los requisitos previos de instalación son los requisitos mínimos para que se admita la plataforma. Algunos de los factores de autenticación también tienen requisitos previos adicionales que se pueden comprobar mediante el indicador `/Factors`.
- También puede utilizar el indicador `/Precheck` para ayudar a solucionar problemas cuando Intel Authenticate no funciona correctamente. Por ejemplo, si el servicio Intel DAL no se está ejecutando, Intel Authenticate no funciona correctamente.

Requisitos previos de instalación:

```
Authenticate_Check.exe /P
```

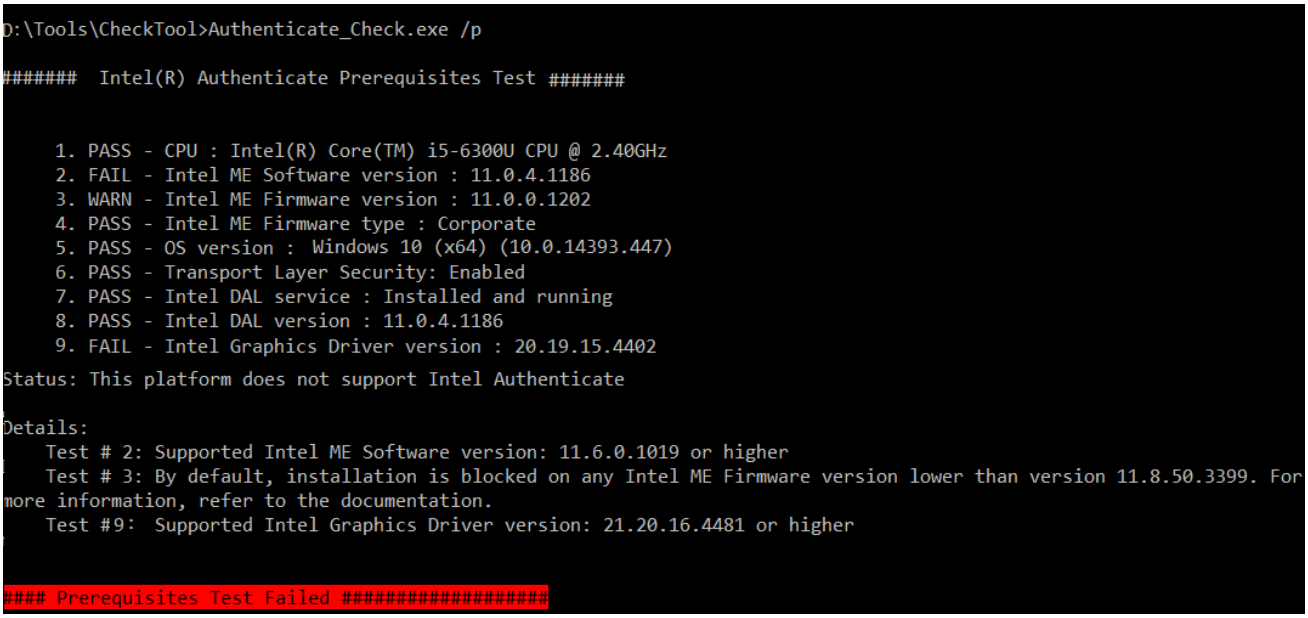
O

```
Authenticate_Check.exe /Precheck
```

Una vez superadas todas las pruebas, el resumen de resultados se resalta en verde.

```
D:\CheckTool>Authenticate_Check.exe /p

#######  Intel(R) Authenticate Prerequisites Test #######


     1. PASS - CPU : Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz
     2. PASS - Intel ME Software version : 11.7.0.1043
     3. PASS - Intel ME Firmware version : 11.8.50.3425
     4. PASS - Intel ME Firmware type : Corporate
     5. PASS - OS version : Windows 10 (x64) (10.0.15063.726)
     6. PASS - Transport Layer Security: Enabled
     7. PASS - Intel DAL service : Installed and running
     8. PASS - Intel DAL version : 11.7.0.1043
     9. PASS - Intel Graphics Driver version : 22.20.16.4785

Status: This platform includes all prerequisites for Intel Authenticate


#### Prerequisites Test Passed ####################
```

Si una de las pruebas falla, el resumen de resultados se resalta en rojo. Para cada prueba fallida, se muestran los detalles.



En esta tabla se describen las pruebas que se ejecutan mediante el indicador `/PreCheck`.

Probar	Detalles
1	Comprueba que el procesador pertenezca a una de las familias de procesadores admitidas. **Nota:** Se espera que la prueba 1 genere un mensaje de advertencia en plataformas de tipo muestra de ingeniería, muestra previa de calidad y muestra de calidad. Esto se debe a que, en este tipo de plataformas, la CPU devuelve un valor no reconocido. Ignore esta advertencia.
2	Comprueba el Registro para verificar que la versión instalada del software Intel ME sea compatible. Además, esta prueba también comprueba que el controlador de Intel MEI esté instalado. El controlador normalmente se encuentra en la sección "Dispositivos del sistema" de la ventana Administrador de dispositivos. Si el controlador no está instalado, algunas de las pruebas restantes fallarán (porque dependen de comunicaciones a través del controlador).
3	Comprueba que la versión del firmware Intel ME sea compatible
4	Comprueba que el firmware Intel ME sea el SKU corporativo (el SKU de consumidor no es compatible)
5	Comprueba que el sistema operativo sea compatible
6	Comprueba que esté activado el protocolo TLS.
7	Comprueba que el servicio de Intel DAL esté instalado y en ejecución (el nombre que aparece en la ventana Servicios es “Intel Dynamic Host Application Loader Host Interface Service”).
8	Comprueba las comunicaciones con Intel DAL; para ello, intenta obtener el número de versión de Intel DAL a través de una API de Intel DAL.
9	Comprueba que Intel Graphics Driver esté instalado y que su versión sea compatible.

7.10.2 Comprobación de los factores

Cada uno de los factores de autenticación admitidos por Intel Authenticate tiene distintas dependencias que deben estar presentes en la plataforma para que se puedan utilizar. El indicador `/Factors` de la herramienta de comprobación proporciona información sobre cada factor y determina si se admite.

Para comprobar el estado de los factores:

```
Authenticate_Check.exe /F
```

O

```
Authenticate_Check.exe /Factors
```

> **Nota:**
>
> Para obtener información más detallada sobre cada factor, agregue el indicador `/V`.

```
G:\CheckTool>Authenticate_Check.exe /f

####### Intel (R) Authenticate Factors Test #######


 Factor:        Bluetooth Proximity (Android)
 Status:        Not Supported
 Reason:        No Intel Network Adapter Card found or the driver is not installed

 Factor:        Bluetooth Proximity (iOS)
 Status:        Not Supported
 Reason:        No Intel Network Adapter Card found or the driver is not installed

 Factor:        Intel AMT Location
 Status:        Supported

 Factor:        Fingerprint
 Status:        Supported
 Reason:        The Soft Fingerprint DLLPath registry key is missing. (This registry key, and the DLL to which it
                points, are added when Intel Authenticate is installed.)

 Factor:        Protected PIN
 Status:        Ready For Use

 Factor:        Face Recognition
 Status:        Supported
 Reason:        The Face Recognition factor DLLPath registry key is missing. (This registry key, and the DLL to which
                it points, are added when Intel Authenticate is installed.)
```

En la tabla se describe la salida correspondiente al indicador `/Factors`.

Sección	Detalles
Factor	El nombre del factor.
Estado	A continuación se indican los estados posibles para cada factor: • **No admitido**: el factor no se admite en la configuración actual de la plataforma. Esto puede incluir software ausente o versiones incompatibles de hardware o software. Los detalles se muestran en la sección "Motivo". Puede ejecutar la herramienta de nuevo tras corregir los problemas detectados que tengan solución (por ejemplo, mediante la ampliación de software). • **Admitido**: el factor se admite pero no está listo para su uso por parte de Intel Authenticate. Se devuelve este estado para los factores que requieren configuración adicional a fin de poder usarlos. Por ejemplo, el factor Ubicación de Intel AMT solo se puede usar para la autenticación una vez que el administrador de TI ha configurado los dominios de inicio en Intel AMT. Antes de instalar Intel Authenticate, este estado también se espera para los factores Reconocimiento facial y Huella digital (ligera) (porque Intel Authenticate instala DLL adicionales). • **Listo para usar**: todos los requisitos previos para el factor existen en la plataforma y el factor está listo para su uso por parte de Intel Authenticate.
Motivo	Esta sección aparece cuando el estado de un factor es "No admitido". Se muestra información sobre cada uno de los problemas que impiden a Intel Authenticate utilizar un factor.
Información	Esta sección se muestra cuando se especifica el indicador `/Verbose` y proporciona información adicional sobre las dependencias para cada factor.

7.11 Utilización de la herramienta de soporte

La herramienta de soporte es una herramienta basada en la interfaz de la línea de comandos que se encuentra en la carpeta `Tools > SupportTool`. La herramienta de soporte también se instala en las plataformas cliente en esta carpeta: `C:\ProgramData\Intel\Intel Authenticate\Engine\SupportTool`.

Puede utilizar la herramienta de soporte para:

- Iniciar o detener las sesiones de registro de depuración
- Recopilar y empaquetar los registros de usuario final en un archivo zip.
- Reiniciar todos los servicios y procesos de Intel Authenticate (esto a veces puede solucionar problemas).

En la sintaxis de la interfaz de la línea de comandos no se distingue entre mayúsculas y minúsculas. Solo se puede usar una marca por llamada. La sintaxis es la siguiente:

```
Authenticate_Support.exe [ /StartDebug | /StopDebug
 /CollectLogs | /Restart | /? ]
```

Marca	Detalles
`/StartDebug`	Crea una sesión de depuración de registro y comienza a recopilar registros en un archivo ETL
`/StopDebug`	Detiene cualquier sesión de depuración de registro activa
`/CollectLogs`	Recopila todos los registros existentes de Intel Authenticate y los pone en un archivo zip
`/Restart`	Reinicia todos los servicios y procesos relacionados con Intel Authenticate.
`/?`	Ayuda

7.11.1 Recopilación de registros

Intel Authenticate guarda los registros en varias ubicaciones. La herramienta de soporte le permite recopilar fácilmente todos los registros. Una vez recopilados, la herramienta empaqueta los registros en un archivo zip en la carpeta desde la que se ejecutó. A continuación, puede enviar el archivo zip a su cliente o ingeniero de soporte de campo para la depuración. Se asigna automáticamente un nombre al archivo zip con el formato siguiente: `AuthenticateLogs_HostName_YYYY-MM-DD-HH-MM-SS.zip`.

Para obtener información sobre las opciones de asistencia técnica para Intel Authenticate, visite Asistencia al cliente de Intel.

Para recopilar los registros:

1. Abra un símbolo del sistema como administrador.
2. Inicie una sesión de depuración de registro:
   ```
   Authenticate_Support.exe /StartDebug
   ```
3. Lleve a cabo la acción problemática. Observe la hora del sistema de la plataforma al iniciar la acción. Esto ayudará al ingeniero de soporte a localizar el área relevante en los archivos de registro.
4. Recopile los registros:
   ```
   Authenticate_Support.exe /CollectLogs
   ```
5. Detenga la sesión de depuración de registro:
   ```
   Authenticate_Support.exe /StopDebug
   ```
6. Envíe el archivo zip de los registros recopilados al ingeniero de soporte que administre su ficha de soporte.

7.11.2 Reiniciar todos los servicios y procesos de Intel Authenticate

La herramienta de soporte reinicia:

- jhi_service.exe (servicio)
- IAClientService.exe (servicio)
- IAEngineService.exe (servicio)
- IAMonitor.exe (proceso)

Esta herramienta también desinstala y reinstala los applets de Intel Authenticate. Si el motor de Intel Authenticate no está instalado, el reinicio no se realizará correctamente y se generará un error (también para `ChangeLogLevel`). Asimismo, el comando `Restart` debe ejecutarse en modo elevado.

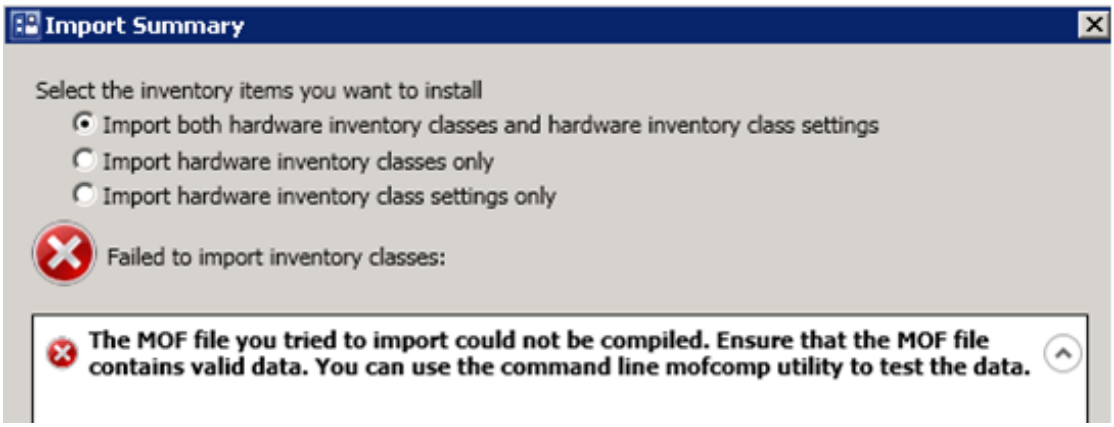
Al reiniciar los procesos de Intel Authenticate, se conservan la directiva aprovisionada y los datos de registro almacenados del usuario final. Esto resulta menos molesto para el usuario final que el restablecimiento del sistema o de un factor, lo cual eliminaría los datos de registro y directiva.

Para reiniciar los servicios y procesos asociados:

```
Authenticate_Support.exe /Restart
```

7.12 Problemas con la importación de clases de inventario de hardware

En ciertas situaciones, la importación de las clases de inventario de hardware podría fallar con este mensaje:



Este mensaje y las soluciones sugeridas son incorrectos y no son relevantes a la hora de importar los archivos MOF proporcionados con el complemento. Si aparece este mensaje, significa que las clases importadas del archivo MOF siguen existiendo en un espacio de nombres temporal utilizado por SCCM. Esto puede ocurrir a veces tras importar/eliminar los archivos varias veces mediante la interfaz gráfica de usuario de SCCM. El problema es que, además de no eliminar los archivos, SCCM también cambia la jerarquía de las clases. Esto impide volver a importar las clases e instalar el complemento.

Para solucionar este problema:

1. Copie los archivos siguientes del paquete de descarga del complemento en el equipo que ejecute Configuration Manager:
   - `fix_sccm_2012_mof.mof`
   - `fix_sccm_2012_mof.bat`
2. Abra un símbolo del sistema como administrador.
3. Ejecute el archivo por lotes llamado `fix_sccm_2012_mof.bat`. Este archivo por lotes elimina todas las clases agregadas por los archivos del complemento importados. Se eliminan del espacio de nombres temporal, situado en:

   `root\CIMv2\sms\inv_temp`
4. Importe las clases de nuevo (véase Para agregar las clases de inventario de hardware: en la página 46).
5. Ahora puede instalar el complemento.

7.13 Códigos de error

Esta tabla describe los códigos de error indicados por el componente Intel Authenticate Engine.

Código de error	Descripción
31	Error del sistema debido a: • Un fallo de funcionamiento de hardware o un tiempo de espera agotado al intentar registrar un factor basado en hardware • Una discordancia de versiones entre el cliente y el motor de Intel Authenticate • No ha sido posible leer los datos de registro. Esto se debe a que los datos están dañados o ausentes.
32	No se ha podido establecer la directiva debido a su firma. El error puede deberse a lo siguiente: • La versión de la directiva es inferior al de la directiva establecida actualmente • La directiva contiene datos no válidos • El formato de la directiva no es correcto
33	No se ha podido establecer la directiva debido a un problema con la firma de la directiva. Este error puede deberse a lo siguiente: • La directiva ha sido creada por un origen no autorizado • Se han realizado cambios en la directiva después de firmarla • El certificado utilizado para firmar la directiva ha caducado o no es válido
34	Se ha realizado una llamada a una función que no está implementada en esta versión
35	Se ha pasado un parámetro no válido a una función
36	El búfer de salida de la función es demasiado pequeño para la salida que debe albergar. Este error se produce normalmente al buscar dispositivos Bluetooth. Normalmente, se soluciona llamando de nuevo a la función con el tamaño de búfer correcto.
37	No se ha podido realizar una solicitud de registro porque el usuario ya había registrado el factor
38	No se ha podido registrar un factor. El factor en cuestión se indica en los registros. El motivo de los fallos de registro varía en función del factor. Estos son algunos ejemplos de fallos de registro. • Proximidad Bluetooth: no se ha podido establecer la confianza entre Intel Authenticate y el teléfono • Huella digital: no se ha podido establecer la confianza entre el dispositivo de huella digital e Intel Authenticate • Ubicación de Intel AMT: Intel AMT no estaba activo cuando se intentó el registro
39	El usuario introdujo un código PIN incorrecto durante el registro del factor Código PIN protegido

Código de error	Descripción
40	El usuario ha intentado el registro fuera de los límites de registro definidos para el factor
41	El usuario ha intentado anular el registro de un factor que no se había registrado previamente
42	Se ha intentado ejecutar un comando administrativo con datos incorrectos
43	Hay demasiados controladores abiertos
44	Se ha intentado ejecutar un comando administrativo que el applet no puede resolver. Por ejemplo, la ejecución de un comando administrativo para un usuario que no existe.
45	Se ha intentado establecer una credencial administrativa que ya se había establecido. Si el restablecimiento de credencial no ha sido realizado por TI, esto podría indicar que hay una infiltración en la red por parte de un origen no autorizado.
46	Las credenciales administrativas no se han establecido. Este error se devuelve cuando se intenta establecer una directiva o ejecutar un comando administrativo antes de establecer las credenciales administrativas.
47	La verificación de la firma ha fallado porque la directiva y el certificado no coinciden
48	El applet de Intel Authenticate está ocupado actualmente gestionando otra solicitud. Cuando se produce este error, se llama de nuevo a la función hasta que el applet deja de estar ocupado y puede procesar la solicitud.
49	El certificado no es de confianza porque no se ha podido verificar la cadena de certificados
50	Se ha intentado autenticar o registrar un factor cuando la directiva no se había establecido
51	Para anular el registro de un factor, este debe estar autenticado como genuino. Este error se devuelve si se produce un error al autenticar el factor.
52	El factor está definido en la directiva pero no se admite en la plataforma
53	El factor se admite y está definido en la directiva, pero no se puede registrar hasta que el usuario haya realizado los pasos previos al registro fuera de Intel Authenticate. Por ejemplo, el factor Huella digital requiere que el usuario registre sus huellas digitales en Windows antes de poder registrarlas en Intel Authenticate.
54	Cuando el Bloqueo por distancia se ha ejecutado durante más de 24 horas, se reinicia automáticamente.
55	No se ha podido realizar el registro porque el tipo de usuario no se admite. Intel Authenticate no admite: • Cuentas de sistema de Windows integradas • Registro de usuarios a través de una conexión a Escritorio remoto • Cuentas de usuario sin contraseña o con una contraseña en blanco

Código de error	Descripción
56	Se ha producido un error con un factor externo (Intel Authenticate admite la integración de factores de autenticación de proveedores de terceros)
57	Este error se devuelve cuando el factor cuyo registro se debe anular se ha autenticado correctamente (consulte el error 51) pero el proceso de anulación del registro en sí falla.
59	El applet de Intel Authenticate está ocupado actualmente gestionando otra solicitud de autenticación
5A	La solicitud de autenticación superó el límite del tiempo de espera
5B	La solicitud de autenticación ha finalizado y se debe volver a inicializar
5D	Se ha realizado un intento de establecer un factor que no está registrado o que existe en un conjunto de factores sin factores registrados actualmente
5E	La directiva no puede establecerse en un sistema que no sea Intel vPro porque la directiva contiene un conjunto de directivas con más de dos factores obligatorios. (Los conjuntos de autenticaciones con más de dos conjuntos de factores obligatorios solo son compatibles con los sistemas Intel vPro).
5F	La acción solicitada ha fallado porque la ha llamado un proceso que requiere permisos de niveles superiores.