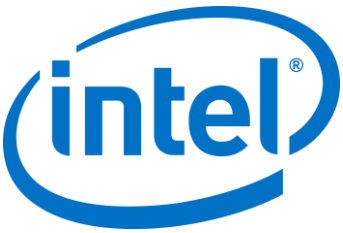
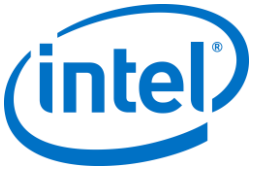


Solución Intel Unite®

Guía de implementación para empresas

Mayo de 2017



Limitación de responsabilidades legales y derechos de autor

Índice

1 Introducción

El software Intel Unite® posibilita espacios de reuniones seguras y conectadas que facilitan la colaboración. Fue diseñado para conectar a todas las personas que participan en una reunión, de un modo rápido y sencillo. Intel Unite es una solución de colaboración simple e instantánea que ya está disponible en el mercado y que proporciona la base para poder brindar más opciones e innovación en el futuro.
En este documento podrá encontrar información sobre cómo instalar el software Intel Unite, conocer mejor todas las funciones y obtener ayuda para resolver problemas.

1.1 Destinatarios

Este documento está diseñado para profesionales de TI que trabajen en un entorno empresarial, así como para aquellas personas que vayan a instalar la solución Intel Unite en un entorno empresarial.

1.2 Terminología y definiciones de la solución Intel Unite

Servidor empresarial (servidor): este término hace referencia al servicio PIN ejecutado en el servidor encargado de asignar y resolver números PIN. Proporciona una página de descarga a los clientes y el portal de administración para la configuración.

Cliente: este término hace referencia a un dispositivo (Windows*, macOS*, iOS*, Android* o Chromebook*) que se usará para conectarse al hub.

Hub: este término hace referencia a un mini PC con tecnología Intel® vPro™ conectado a una pantalla en la que se ejecuta la aplicación Intel Unite en una sala de conferencias.

FQDN: este es el acrónimo de Fully Qualified Domain Name (nombre de dominio completamente cualificado).

Complemento: este término hace referencia a un componente de software instalado en el hub, que amplía la funcionalidad de la solución Intel Unite.

IIS: este es el acrónimo de Internet Information Services, un servidor web proporcionado por Microsoft*.

1.3 Novedades en la solución Intel Unite

Para ayudarle a identificar qué se ha añadido a la solución, la tabla siguiente resume las funciones añadidas desde la versión 1.0.

v 2.0	v 3.0	v 3.0 MR	v 3.1
Pantalla ampliada	Transmisión de audio/vídeo acelerada por hardware para Windows (1080 a 20-30 fps)	Compatibilidad de iOS con Presentar	Experiencia de usuario mejorada para el portal de administración, una apariencia diferente en la que se incluyen cuadros de diálogo para facilitar la selección de la configuración
Compatible con Windows 10	Complemento para el acceso protegido de invitados		Portal de administración: Programar reunión
Complemento de inicio de sesión de usuario invitado	Reuniones programadas (aula individual)		Portal de administración: modo Moderador
Complemento para Skype Empresarial	Bloquear reunión		Portal de administración: PIN estático
	Compatibilidad de iOS con Ver		Portal de administración: Reserva del PIN
			Portal de administración: Transparencia del PIN
			Portal de administración: Desactivar la visualización remota
			Compatibilidad con Chrome OS
			Compatibilidad con Android

2 Requisitos de la solución Intel Unite

2.1 Requisitos del servidor empresarial

- Microsoft Windows* Server 2008 o posterior
- Microsoft Internet Information Services con SSL habilitado
    - Esto requerirá un certificado de servidor web basado en SHA2 con una raíz interna o pública de confianza
- Servidor de correo electrónico SMTP configurado en Microsoft Internet Information Services
- Microsoft SQL Server 2008 o posterior
- Microsoft .NET* 4.5 o posterior
- 4 GB de RAM
- 32 GB de espacio de almacenamiento disponible
  NOTA: El servidor web IIS y la base de datos de Microsoft SQL Server se pueden instalar en equipos diferentes

2.2 Requisitos del hub

- Microsoft Windows 7 (SP1), 8.1 o 10 (32 y 64 bits)
    - Se recomienda utilizar el nivel de parche más reciente
- Microsoft .NET 4.5 o superior
- Mini PC de [1] 4ª generación (o posterior) equipado con procesador Intel® Core™ vPro™ con SKU compatible
- Conexión de red, por cable o inalámbrica
- 4 GB de RAM
- 32 GB de espacio de almacenamiento disponible

2.3 Requisitos del cliente

- Microsoft Windows 7 (SP1), 8.1 o 10 (32 y 64 bits)
    - Se recomienda utilizar el nivel de parche más reciente
- Microsoft .NET 4.5 o superior
- OS X* 10.10.5 y posterior
- iOS 9.3 o posterior
- Conexión de red, por cable o inalámbrica

[1] Si desea obtener más información sobre los SKU compatibles, póngase en contacto con un fabricante de equipos originales de su elección o un representante de Intel.

2.4 Requisitos de red y factores que TI debe tener en cuenta

La instalación del hub y el cliente deben gestionarse utilizando el proceso establecido por su departamento de TI para la distribución de software.
Para garantizar la fiabilidad, se recomienda que el hub utilice una conexión de red por cable. Esto evitará que haya saturación del ancho de banda, especialmente en zonas congestionadas.
Otro factor que se debe tener en cuenta es que el software Intel Unite debe poder aceptar conexiones entrantes. Para ello, es posible que tenga que añadir una exención en el cortafuegos instalado en el hub. Para obtener detalles específicos sobre cómo crear excepciones para aplicaciones, póngase en contacto con el proveedor de su cortafuegos.

En un entorno de producción, es muy recomendable utilizar un nombre de dominio completamente cualificado (FQDN) y configurar un registro de servicio DNS para el servidor empresarial. Esta es la forma más sencilla para que los hubs y clientes localicen el servidor empresarial.
Como actualización de seguridad, la aplicación solo acepta certificados SHA-2 o superiores. Por ello, es posible que deba actualizar los certificados de su servidor web. Hable con su equipo de seguridad de TI para obtener certificados SHA-2 durante la configuración.

2.4.1 Dispositivos móviles para clientes

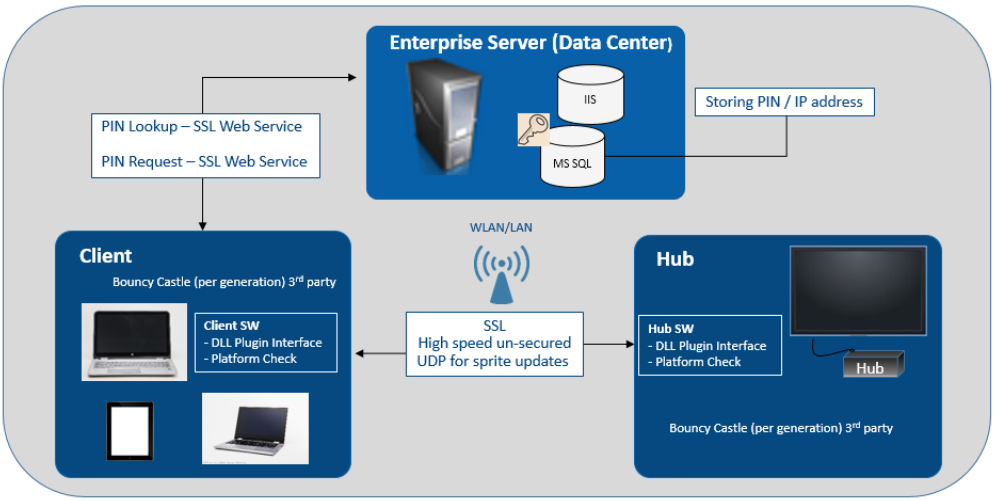
Si su organización va a implementar dispositivos móviles para clientes como parte de los sistemas operativos cliente Intel Unite, deberá tener en cuenta lo siguiente:
Para poder conectarse a la solución Intel Unite, todos los dispositivos cliente (incluidos los iOS y Android) deberán estar conectados a la red corporativa o utilizar una VPN con la configuración adecuada. Si se va a utilizar en tabletas y teléfonos (normalmente para uso personal) que no estén conectados a la red corporativa, sino que cuentan con su propio proveedor, es posible que no se puedan conectar a una sesión de la app Intel Unite, porque puede que el firewall corporativo no lo permita.

Para administradores de TI:

- Si los usuarios de la app Intel Unite están utilizando sus propios dispositivos móviles, asegúrese de que están en la red de la empresa para conectarse a Intel Unite o cree alguna forma para que puedan realizar estas conexiones.
- Asegúrese de que tiene las herramientas necesarias para gestionar adecuadamente estos dispositivos y mantener la red segura.
- Ponga en práctica la estrategia adecuada para administrar estos dispositivos, que pueden suponer un riesgo adicional para la seguridad.
- Aplique una política de gestión de dispositivos móviles a dispositivos personales, o dispositivos móviles de trabajo.
- Adapte las medidas de seguridad para que pueda proporcionar el nivel correcto de seguridad en función del grado de confidencialidad de los datos que se van a proteger. El grado de adaptación depende de los datos que la empresa considere importantes y de hasta dónde desee llegar para aplicar protecciones.

3 Descripción de la implementación

La solución Intel Unite consta de tres componentes: un servidor empresarial, un hub y un cliente.
El Servidor empresarial es el primer componente que debe configurar. Una vez ejecutadas las aplicaciones del cliente y del hub, utilizarán el servidor empresarial para intercambiar información de conexión y recibir asignaciones de PIN.
Hub es el mini PC equipado con procesador Intel Core vPro que, por lo general, se conecta a una pantalla o a un proyector en una sala de conferencias.
Los clientes deben seguir las instrucciones que se muestran en el hub para descargar el software de cliente y conectarse al hub introduciendo el PIN que aparece. Una vez conectado, el cliente puede presentar su contenido, así como ver, anotar y compartir archivos con los otros participantes conectados al mismo hub e interactuar con los complementos instalados en el hub.
Este diagrama ofrece una descripción general de los componentes instalados.



3.1 Recursos necesarios para la implementación

A fin de completar la instalación, necesitará lo siguiente:

- Derechos administrativos en la base de datos
- Derechos administrativos en el servidor empresarial
- Derechos administrativos en el hub

Puede que también necesite:

- Administrador de seguridad de TI que emita el certificado SHA-2
- Administrador de seguridad de TI para políticas de cortafuegos
- Administrador de TI para crear un registro de servicio DNS que el hub y los clientes van a utilizar para localizar el servidor empresarial (altamente recomendado)

4 Instalación del servidor empresarial

4.1 Descripción general del servidor empresarial

El instalador del servidor empresarial incluye la base de datos, el servidor PIN, el portal web de administración y la página de descarga del cliente.
El servidor empresarial contiene 4 componentes:

1) Base de datos Microsoft SQL: conserva toda la información de estado de la infraestructura de la solución Intel Unite.
2) Servicio web: es un servicio de mensajería estandarizado que se comunica con la base de datos, los clientes y los hubs.
3) Sitio web del portal de administración: gestiona los hubs y los clientes, genera estadísticas, y proporciona supervisión y alertas.
4) Página web de destino para las descargas de clientes: contiene el software Intel Unite del cliente.

Además, es importante saber que los hubs y los clientes localizan el servidor empresarial en su infraestructura de red mediante uno de estos dos métodos: el archivo ServerConfig.xml o el registro de servicio DNS.
Se recomienda utilizar el registro de servicio DNS, ya que posibilita la configuración del cliente y del hub sin necesidad de pulsar ningún botón. Consulta la sección sobre Creación de un registro de servicio DNS. No obstante, si no puede obtener un registro de servicio DNS, puede configurar el Servidor empresarial en el archivo ServerConfig.xml. Consulte el Apéndice B para ver un Ejemplo de archivo ServerConfig.xml.

4.2 Preinstalación del servidor empresarial

- Compruebe que el servidor cumple los requisitos mínimos de software y hardware especificados.
- Verifique que tiene instalada la versión de IIS 8.0 o posterior en el servidor. El instalador del servidor requiere que se active IIS o se producirá un error. Si necesita ayuda para activar y configurar IIS, consulte la sección Activación de IIS.
- Para configurar el servidor de correo electrónico SMTP en IIS Manager, consulte la sección
- Configuración del servidor de correo electrónico.
- Asegúrese de que tiene ASP.NET 4.5 instalado y activado.
- Compruebe que SSL esté habilitado en IIS (los sitios https deberían funcionar). **NOTA:** Puede que tenga que colaborar con su departamento de TI para instalar un certificado SHA-2 con una raíz de confianza válida.
- Asegúrese de que tiene acceso administrativo a MS SQL a través de la autenticación de Windows o de SQL. Consulte la sección en Instalación de Microsoft SQL Server.
- Agregue un registro de servicio DNS para activar la búsqueda automática del servidor empresarial. Consulta la sección sobre Creación de un registro de servicio DNS.

4.2.1 Actualización de software

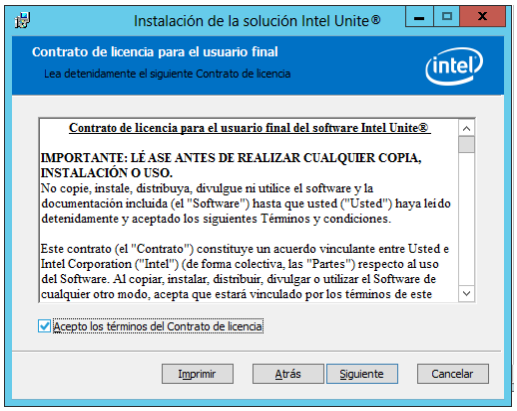
Si su organización está realizando una actualización de software:

- Asegúrese de que ha hecho una copia de seguridad de la base de datos porque los cambios no se pueden deshacer.
- Todas las conexiones con la base de datos deben cerrarse antes de la actualización (cierre la sesión desde el portal de administración)
- Durante la actualización, se seleccionará por defecto la opción Base de datos, tanto para la instalación local como para la remota, cuando Intel Unite server.msi se esté ejecutando en el servidor PIN.

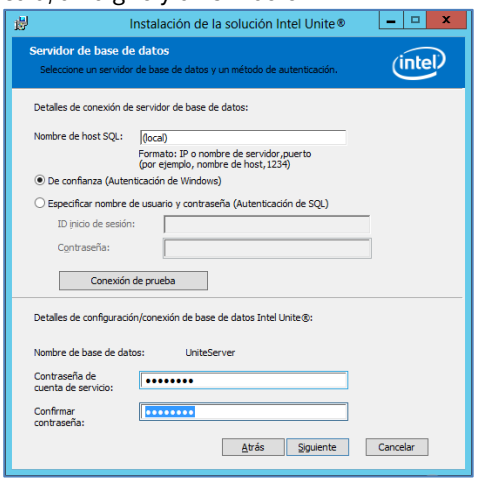
4.3 Instalación del servidor empresarial

Cuando haya verificado todos los pasos de la sección anterior (Preinstalación del servidor empresarial), continúe con los instaladores de software Intel Unite (este proceso debe ejecutarse en el servidor que aloja el entorno IIS).

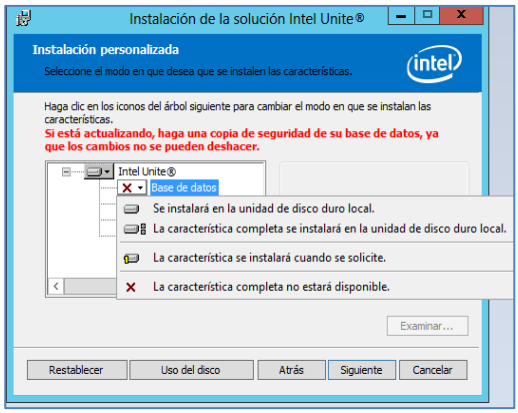
- Localice el archivo **Intel Unite Server.mui.msi** y haga doble clic para instalarlo en el servidor o servidores de destino.
- El asistente de instalación ofrece la posibilidad de instalar estos componentes: base de datos, servicio web, página de descarga del cliente y portal de administración.
- Después de ejecutar **Intel Unite Server.mui.msi**, acepte el contrato de licencia marcando la casilla **Acepto los términos del Contrato de licencia**.

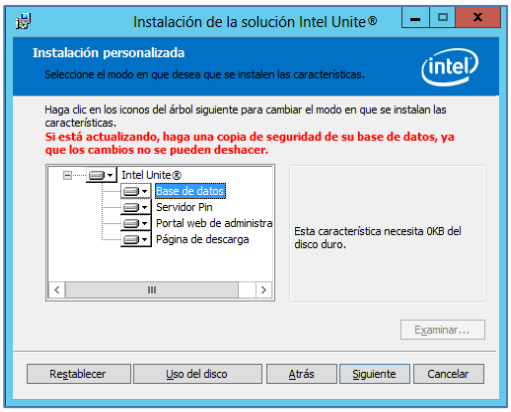


- Haga clic en **Siguiente** para pasar a la ventana Servidor de base de datos.
- En la ventana Servidor de base de datos, seleccione los **Detalles de conexión de servidor de base de datos**. Las opciones disponibles son las siguientes:
  - En el cuadro **Nombre de host SQL**, **(local)** es el valor predeterminado para SQL Server. Puede cambiarlo si modifica el nombre de host o puede dejar el valor predeterminado (dejar **(local)** si SQL está instalado en el mismo servidor).
  - El valor predeterminado para el servidor es **De confianza (autenticación de Windows)**, si ya ha iniciado sesión; o bien indique un **Nombre de usuario y contraseña (autenticación de SQL)**, si tiene credenciales válidas con acceso a la base de datos y prefiere la autenticación SQL. Si elige la segunda opción, no olvide hacer clic en **Conexión de prueba** para probar la conexión de la base de datos.
  - En la sección **Detalles de configuración/conexión de base de datos**, debe crear una contraseña para **UniteServiceUser**, que será la que se utilice para acceder a la nueva base de datos llamada UniteServer. Seleccione **Confirmar contraseña** en el cuadro siguiente.
  - La contraseña debe tener 8 caracteres como mínimo e incluir al menos un carácter en mayúscula, uno en minúscula, un dígito y un símbolo.



- Haga clic en **Siguiente** para pasar a la ventana **Instalación personalizada** para seleccionar funciones. Amplíe la función de la base de datos y seleccione si una de ellas **se instalará en la unidad de disco duro local** o **la característica completa se instalará completa en la unidad de disco duro local**. Esto creará la base de datos en SQL Server proporcionado en el paso anterior.

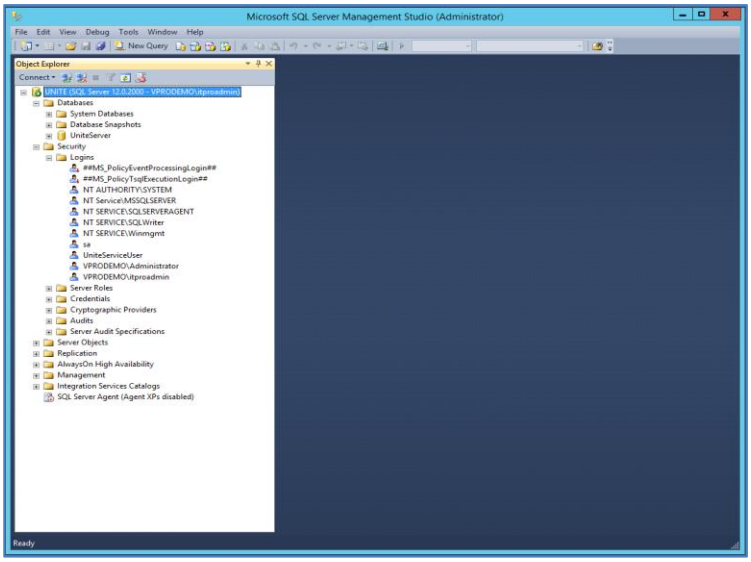




- Haga clic en **Siguiente** para verificar los componentes seleccionados y haga clic en **Instalar** para iniciar la instalación.
- Haga clic en **Finalizar** para completar la configuración.
- Acaba de instalar el Servidor empresarial. Continúe con la sección siguiente para instalar el hub.

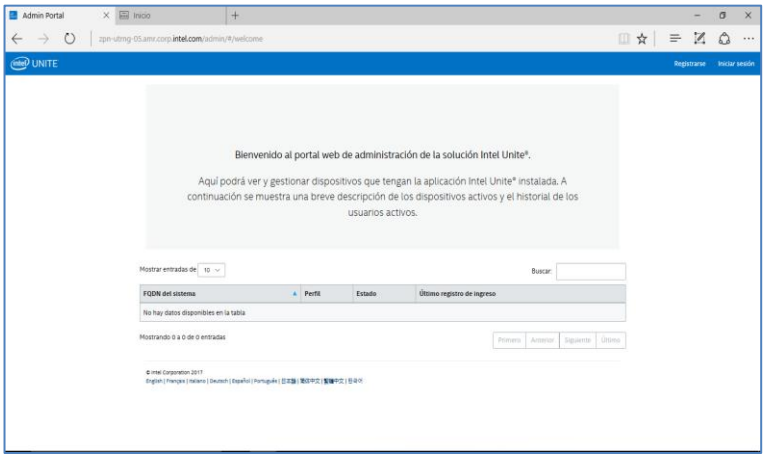
Opcional:

- Si lo desea, compruebe que se ha creado la base de datos UniteServer usando la opción para abrir SQL Management Studio de SQL Management Studio en su servidor y conéctese a SQL Server. Expanda las bases de datos en el panel izquierdo y asegúrese de que se ha creado la base de datos UniteServer.



- Acceda al portal de administración para comprobar que la instalación se ha realizado correctamente (si está instalada en el servidor junto con la base de datos y el servidor PIN), con este enlace:
  https://<yourservername>/admin

Puede iniciar sesión en su cuenta o puede utilizar la cuenta de administrador predeterminada (para la nueva instalación del software):
Usuario: admin@server.com
Contraseña: Admin@1

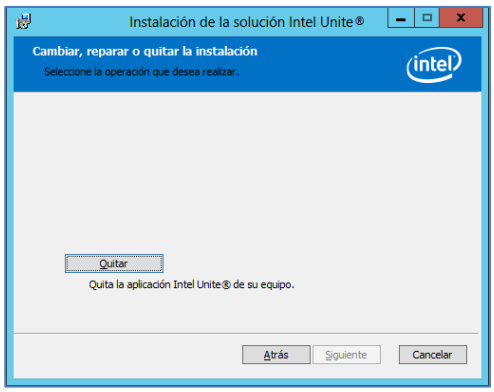


Nota: Si recibe un error al acceder al portal de administración, consulte la sección Solución de problemas.

4.4 Desinstalación de la aplicación Intel Unite

Si necesita desinstalar la aplicación, también deberá eliminar la base de datos UniteServer y la sesión de UnitServiceUser creada anteriormente para evitar conflictos dentro de la aplicación. Antes de hacerlo, **asegúrese de que ha creado una copia de seguridad de su base de datos**.

1. Inicie el instalador del **Servidor Intel Unite .mui**.
2. Haga clic en **Eliminar** y en **Siguiente** para continuar.



3. Vaya a *Microsoft SQL Server Management Studio* y elimine manualmente la base de datos de SQL **UniteServer** y la cuenta **UniteServiceUser**. Consulte las áreas resaltadas en la imagen siguiente.

5 Instalación del hub

5.1 Preinstalación del hub

La aplicación Intel Unite requiere una exención en el cortafuegos del hub para acceder al servidor empresarial y comunicarse con él, ya que el hub necesita poder localizar el servidor empresarial y comunicarse con él.

Cuando ejecute el instalador del hub, este le pedirá los detalles de conexión del servidor y le dará la opción de omitir la búsqueda manual (el paso llamado **Especificar servidor** en el proceso de instalación) para recuperar información del registro de servicio DNS. Cuando ejecute el instalador del hub, editará el archivo ServerConfig.xml.

Dependiendo del método elegido para buscar el PIN, necesitará saber si va a utilizar la opción **Buscar automáticamente servidor** o bien **Especificar servidor** al ejecutar la instalación.

Si sabe que existe el registro de servicio DNS, puede seleccionar **Buscar automáticamente servidor**; si no está seguro, utilice la opción **Especificar servidor** (búsqueda manual), en la que deberá conocer el nombre del host del Servidor empresarial.

Si ha editado ServerConfig.xml con la clave pública (consulte la siguiente sección Clave pública), no es necesario que vuelva a introducir la clave para los instaladores del cliente y del hub.

Nota: Si hay un servidor definido en ServerConfig.xml, tendrá prioridad sobre el registro de servicio DNS.

5.1.1 Clave pública

La clave pública es opcional y sirve para indicar el modo en que el cliente o el hub se comunicará con el servidor empresarial. Si se deja en blanco o no se especifica, el hub y el cliente validarán la raíz de confianza. Si la aplicación no acepta el certificado, se pedirá el usuario.

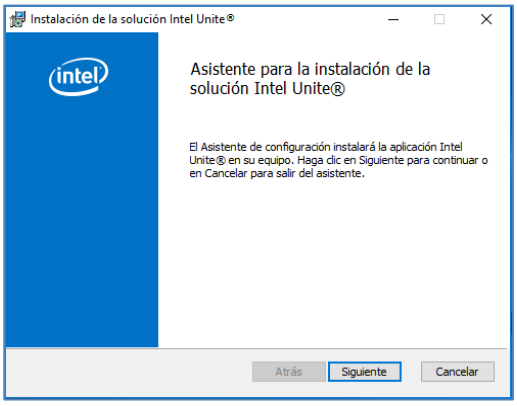
La clave pública se utiliza cuando ejecuta la instalación del hub y el cliente. La necesitará para ejecutar los instaladores del hub y del cliente. Para obtener la clave pública, visite:
https://yourservername/unite/ccservice.asmx

En la barra de dirección URL, haga clic en el candado para ver la información del certificado. Acceda a los detalles, haga clic en "Mostrar todo", desplácese hacia abajo por el campo hasta "Clave pública" y, a continuación, haga clic en ella para verla. Otra opción es copiar el valor que se muestra y pegarlo en el archivo ServerConfig.xml.

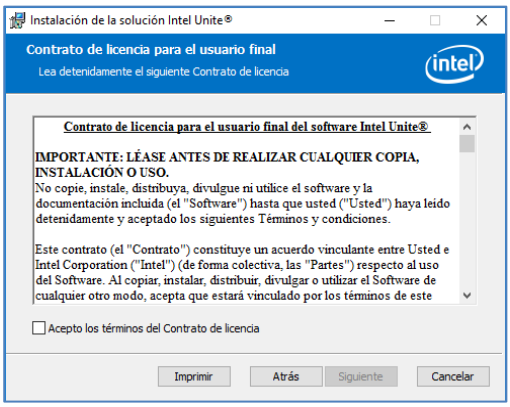
Asegúrese de eliminar los espacios de la cadena después de pegarla en el archivo ServerConfig. Si ha editado ServerConfig.xml con la clave pública, no es necesario que vuelva a escribir la clave para los instaladores del cliente y del hub. Consulte el Apéndice B para ver un ejemplo de ServerConfig.xml.

5.2 Instalación del hub

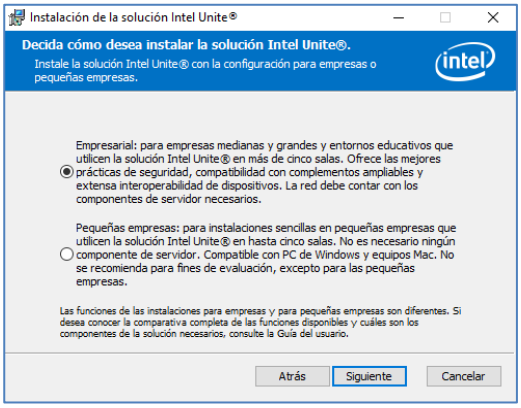
- Busque la carpeta del instalador y ejecute el instalador del hub: **Intel Unite Hub.msi.**
- Haga clic en **Siguiente** para continuar.



- Haga clic en **Siguiente** después de marcar la casilla de verificación **Acepto los términos del Contrato de licencia**.

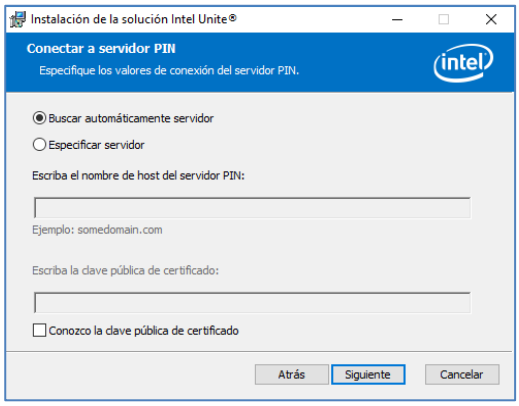


- Seleccione **Empresas** y haga clic en **Siguiente**.

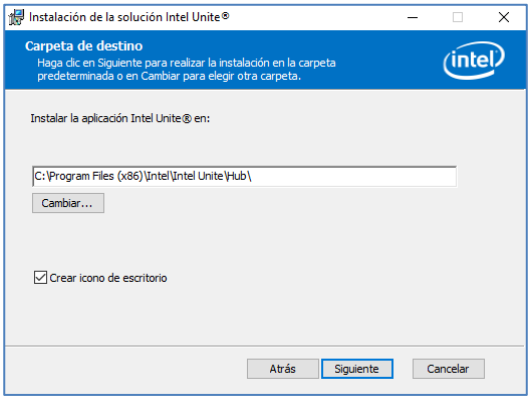


- En esta ventana, debe especificar la configuración de conexión del servidor PIN. Tiene las siguientes opciones:
  - **Buscar automáticamente servidor**: es la opción recomendada (predeterminada).
  - **Especificar servidor:** en este paso, debe conocer el nombre de host del servidor empresarial.
    - **Escriba el nombre de host del servidor PIN.**
    - Escriba la **clave pública de certificado** si ha marcado **Conozco la clave pública de certificado**.

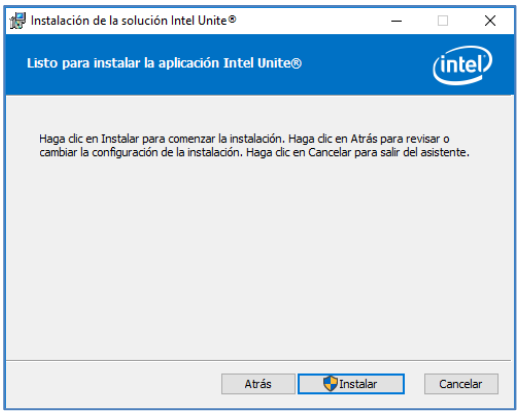
  Elija la opción que prefiera y haga clic en **Siguiente**.



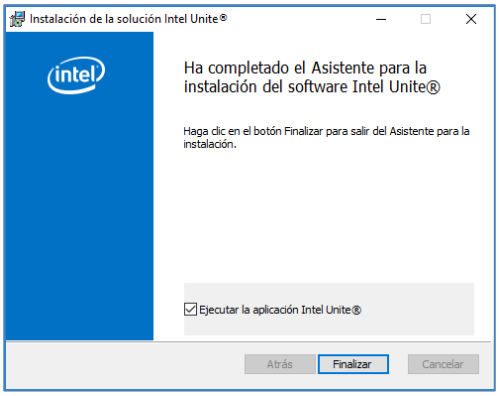
- Se abrirá la ventana **Carpeta de destino** con la carpeta predeterminada donde se instalará el hub. Puede cambiar la carpeta de destino si lo desea. En caso contrario, mantenga la ubicación predeterminada. En este paso, también puede crear un icono en el escritorio. Haga clic en **Siguiente** para continuar.



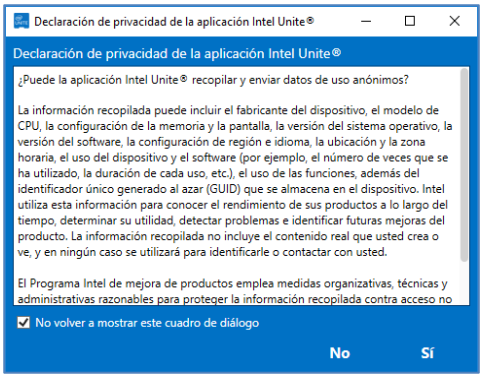
- En este paso, puede volver a revisar la configuración o bien hacer clic en **Instalar** para continuar.



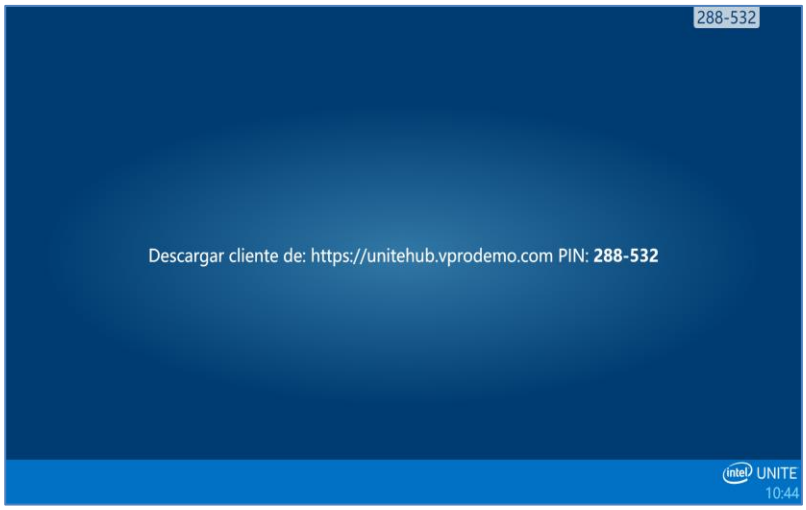
- Cuando haya terminado la instalación, verá la ventana **Ha completado el Asistente para la instalación del software Intel Unite®**. Haga clic en **Finalizar** para terminar el proceso de instalación.



  - Al iniciar la aplicación por primera vez, verá la **Declaración de privacidad de la aplicación Intel Unite®**.



  - La declaración de privacidad de la aplicación Intel Unite® se utiliza para recopilar datos anónimos de uso. Intel siempre se esfuerza por mejorar sus productos y desea recopilar datos para seguir esta mejora. Seleccione **SÍ** o **NO** y marque la casilla de verificación si no desea que vuelva a aparecer este cuadro de diálogo.
  - Ahora verá un PIN en su pantalla o monitor. Este es el PIN que necesitarán los clientes para conectarse al hub. (Consulte la sección Solución de problemas si no aparece el PIN).



5.3 Configuración del hub

Las opciones de configuración de los hubs que ejecutan el software Intel Unite se pueden modificar desde el portal de administración. El portal de administración contiene un perfil por defecto con unos ajustes de configuración predeterminados que se aplican a todos los hubs que acceden al servidor empresarial. Las opciones de configuración se envían al hub una vez que el hub haya establecido conexión con el servidor empresarial. La configuración se actualiza tras cada acceso del hub, la mayoría de los ajustes pueden personalizarse según las necesidades de su organización, por ejemplo, cada hub puede mostrar diferentes colores, imágenes o tamaño del PIN, contener diferentes complementos, etc.
Consulte la sección Guía del portal de administración para obtener más información sobre la configuración del hub.

5.4 Prácticas recomendadas del hub

Con el fin de garantizar la mejor experiencia posible al usuario final, debe configurar el hub para que siempre esté listo para usarse y para que se supriman las alertas del sistema o los mensajes emergentes que aparecen en pantalla. Entre las prácticas recomendadas, cabe destacar las siguientes:

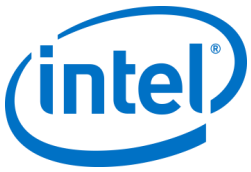
- Windows debe iniciar sesión automáticamente en el dominio o usuario que vaya a ejecutar la aplicación Intel Unite.
- Se deben desactivar los salvapantallas.
- El sistema se debe configurar de modo que nunca entre en estado de espera.
- El sistema se debe configurar para que nunca cierre sesión.
- La pantalla se debe configurar para que nunca se apague.
- Se deben suprimir las alertas del sistema.

5.5 Seguridad del hub

El administrador del hub debe garantizar que se siguen las prácticas recomendadas en materia de seguridad para cada hub. Si el usuario local ha iniciado sesión automáticamente, compruebe que no lo hace con privilegios administrativos.

5.6 Complementos

La aplicación Intel Unite admite el uso de complementos. Los complementos son elementos de software que amplían las funciones y capacidades de la aplicación, implementando modalidades de experiencia de usuario. Los complementos pueden ser exclusivos para cada hub.
En la actualidad están disponibles los siguientes complementos para la aplicación Intel Unite:



Complemento para acceso protegido de invitado: este complemento permite conectar un PC a un hub sin que sea necesario que tengan la misma red empresarial y sin validación de PIN del Servidor empresarial. El hub crea una red ad-hoc/hospedada (punto de acceso) a la que el cliente Intel Unite puede conectarse.

Complemento para Skype empresarial: este complemento es una solución que permite añadir usuarios de una reunión de Skype online a una sesión de la aplicación Intel Unite. Este complemento se ejecuta en el hub del software Intel Unite y gestiona una cuenta de correo electrónico específica para cada instancia.

Complemento de telemetría: si se ha instalado en el hub, se puede utilizar el servidor empresarial para aceptar y mostrar los datos del hub. El requisito mínimo es el servidor empresarial v.3.0 (compilación n.º 3.0.38.44).

Además, hay un SDK utilizado para escribir complementos:

Kit de desarrollo de software (SDK): guía de interfaz de aplicaciones que sirve de ayuda para los desarrolladores de software o cualquier otro usuario que quiera desarrollar funcionalidades adicionales para la aplicación Intel Unite.

Nota: Consulte las guías específicas del complemento que desee instalar o para obtener más información sobre sus componentes.

5.6.1 Notas de instalación del complemento

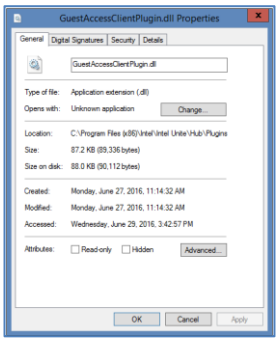
Cada complemento se instala de manera predeterminada en el directorio de complementos dentro del directorio de instalación [Archivos de programa(x86)\Intel\Intel Unite\Hub\Complementos\Nombredelcomplemento (Plugin.dll)]. Los complementos se enumeran al iniciar la aplicación. Si se agrega un nuevo complemento, deberá reiniciar la aplicación.
Antes de instalar el complemento, compruebe la compatibilidad con la versión de destino de su solución Intel Unite [consulte las guías específicas del complemento, ya que los requisitos son diferentes para cada complemento].
Debe asegurarse de conseguir y añadir el valor de hash del certificado de todos los complementos que utilice en el portal web de administración.
NOTA: Para un entorno de prueba, puede usar el valor clave predeterminado, pero esto no se recomienda para un entorno de producción.

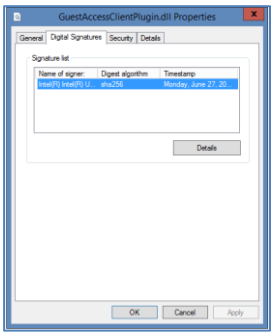
5.6.2 Valor de hash del certificado del complemento

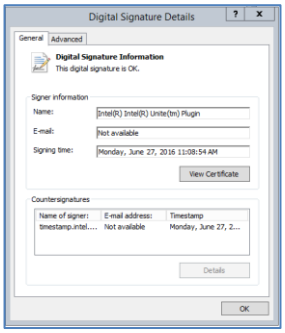
Siga estos pasos para buscar el valor de la clave hash del certificado del complemento:

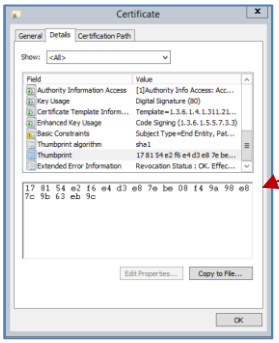
- Busque el complemento en la carpeta Complementos, haga clic con el botón derecho del ratón en ***Plugin.dll** y elija **Propiedades** (por ejemplo, GuestAccessClientPlugin.dll)
- Cuando se abra la ventana **Propiedades** del elemento, vaya a la pestaña **Firmas digitales** y haga clic para abrirla.
- Seleccione **Intel Unite Plugin** y haga clic en **Detalles**.
- En la ventana de **Detalles de la firma digital**, haga clic en **Ver certificado.**
- En la ventana **Certificados**, seleccione la pestaña **Detalles** y desplácese hacia abajo hasta que vea **Huella digital**.
- Seleccione **Huella digital** y, cuando aparezca el valor, cópielo en un archivo de texto o del bloc de notas, elimine los espacios y guárdelo.

- Este valor clave se utilizará cuando cree el perfil de su complemento. El valor clave se puede crear e introducir después de crear el perfil; continúe con la siguiente sección para obtener más información.





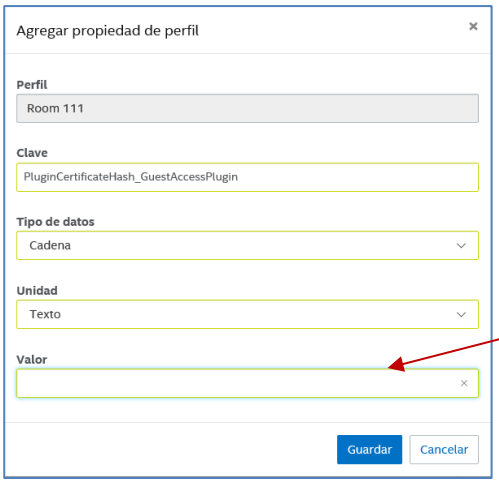




Copie y pegue el valor en un archivo de bloc de notas o texto, quite los espacios y guárdelo.

5.6.3 Añadir el hash del certificado a un complemento en el portal web de administración

Vaya al portal web de administración, en **Grupos**, y seleccione el perfil en el que desea activar el complemento.
En la ventana Perfil, haga clic en **Agregar propiedad de perfil** y escriba lo siguiente:



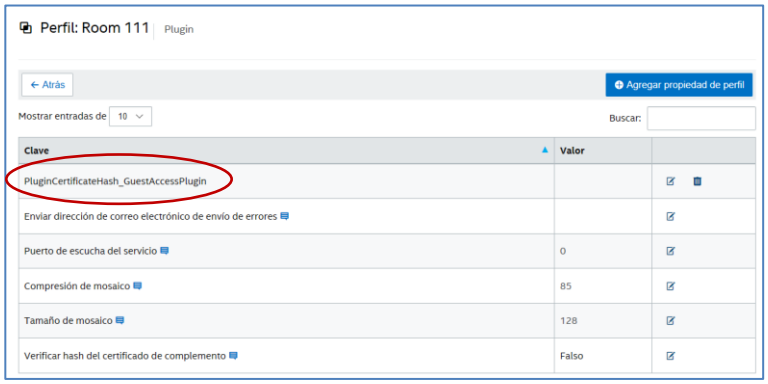
Utilice el valor guardado en el bloc de notas o en el archivo de texto que se describe en la sección anterior. Asegúrese de que es el valor correcto (sin espacios)

- **Clave**: PluginCertificateHash_XXX

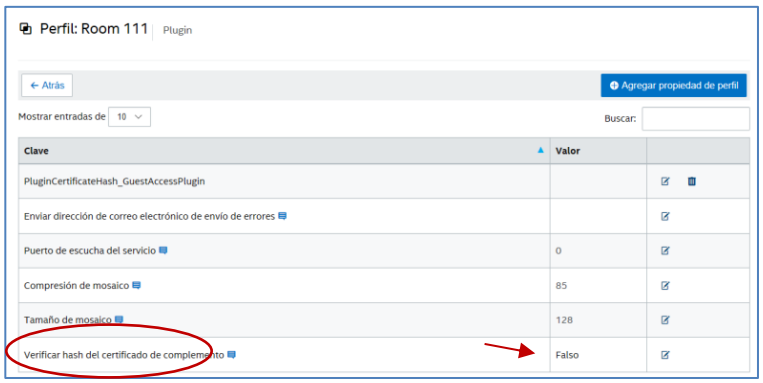
- XXX es el nombre del complemento para el que se ha agregado el hash, por ejemplo, GuestAccessPlugin, con fines de identificación; se recomienda utilizar el nombre del complemento que se corresponde con el hash.

- **Tipo de datos**: cadena
- **Unidad:** texto
- **Valor:** utilice el valor de huella digital que ha guardado en el bloc de notas o el archivo de texto que se menciona en la sección *Valor de hash del* certificado del complemento. El valor de clave también se puede introducir después de crear la clave.

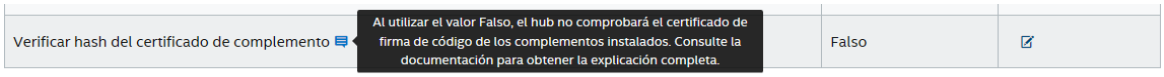
Haga clic en **Guardar**, puede actualizar los valores más adelante mediante el enlace **Editar**.
Se mostrará la nueva clave en la ventana Perfil.



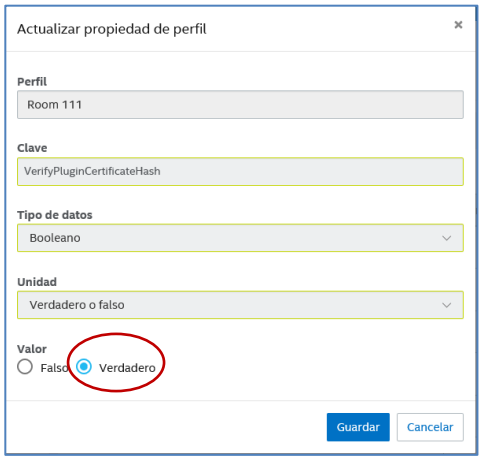
También deberá activar la clave **Verificar hash del certificado de complemento** estableciendo Verdadero; el valor predeterminado es Falso.



Puede elegir si quiere activar o desactivar el complemento. Para ello, cambie de Verdadero a Falso (o viceversa). Tenga en cuenta que los valores clave garantizan la validez del complemento.



Haga clic en el enlace Editar para cambiar el valor a **Verdadero** y seleccione **Guardar**.



Ya se ha activado la configuración del complemento.

6 Instalación del cliente

6.1 Preinstalación del cliente

Los clientes deben poder localizar el servidor empresarial y comunicarse con él. La aplicación Intel Unite requiere una exención en el cortafuegos del cliente para incorporar el Servidor empresarial y comunicarse con él.
Cuando ejecute el instalador del cliente, este le pedirá los detalles de conexión del servidor y le dará la opción de omitir la búsqueda manual (el paso llamado **Especificar servidor** en el proceso de instalación) para recuperar información del registro de servicio DNS. Cuando ejecute el instalador, editará el archivo ServerConfig.xml.

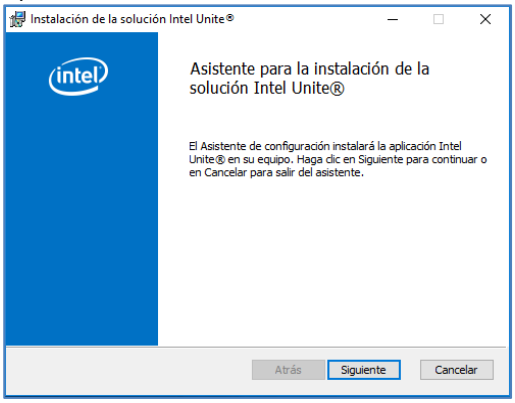
Dependiendo del método elegido para el bloqueo de PIN, necesitará saber si va a utilizar la opción **Buscar automáticamente servidor** o bien **Especificar servidor** al ejecutar la instalación.
Si sabe que existe el registro de servicio DNS, puede seleccionar **Buscar automáticamente servidor**. Es preferible utilizar la búsqueda automática para evitar errores de escritura. Si no está seguro, utilice la opción **Especificar servidor** (búsqueda manual). En este caso, debe conocer el nombre del servidor empresarial.

Nota: Si hay un servidor definido en ServerConfig.xml, tendrá prioridad sobre el registro de servicio DNS.

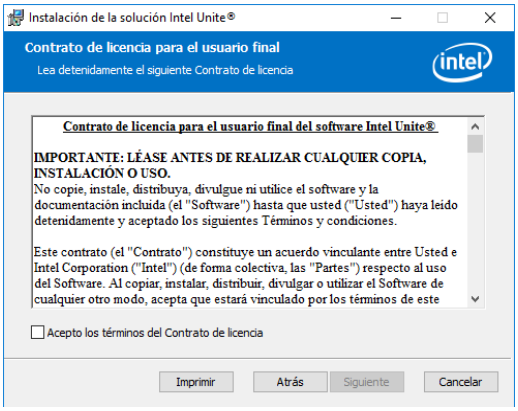
Dispositivos móviles para clientes: todos los dispositivos cliente (incluidos los iOS y Android) deberán estar conectados a la red corporativa o utilizar una VPN con la configuración adecuada. Si se va a utilizar en tabletas y teléfonos (normalmente para uso personal) que no estén conectados a la red corporativa, sino que cuentan con su propio proveedor, es posible que no se puedan conectar a una sesión de la app Intel Unite, porque puede que el firewall corporativo no lo permita. Consulte la sección Dispositivos móviles para clientes para obtener más información.

6.2 Instalación del cliente Windows

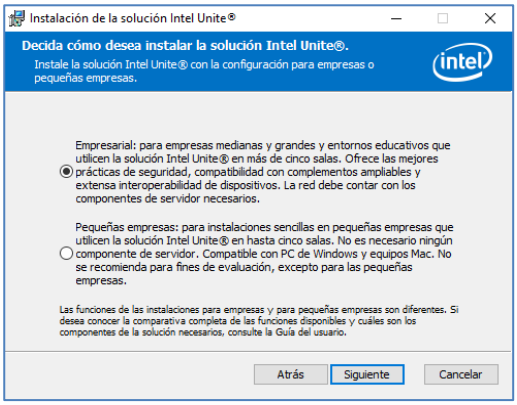
- Busque la carpeta del instalador y ejecute el instalador del cliente: **Intel Unite Client.mui.msi.** Haga clic en **Siguiente** para continuar.



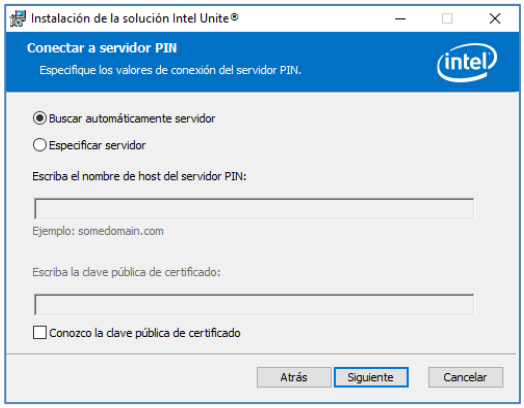
- Active la casilla **Acepto los términos del Contrato de licencia** y, a continuación, haga clic en **Siguiente**.



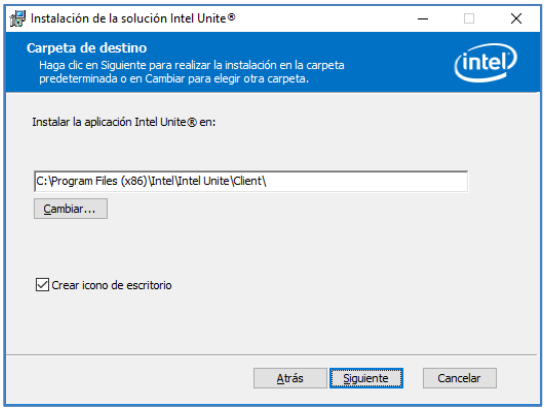
- Seleccione **Empresarial** y haga clic en **Siguiente.**



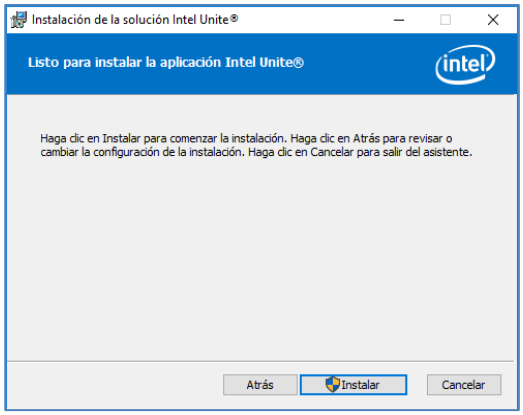
- En esta ventana, debe especificar los valores de conexión del servidor PIN. Las opciones son:
  - **Buscar automáticamente servidor**: es la opción más práctica (predeterminada).
  - **Especificar servidor:** en este paso, debe conocer el nombre de host del servidor empresarial.
    - **Introduzca la clave pública de certificado**: esta opción solo está disponible si selecciona **Especificar servidor**.
    - Introduzca la **clave pública de certificado**, si la tiene y ha seleccionado este método.
- Elija la opción que prefiera y haga clic en **Siguiente** para continuar.



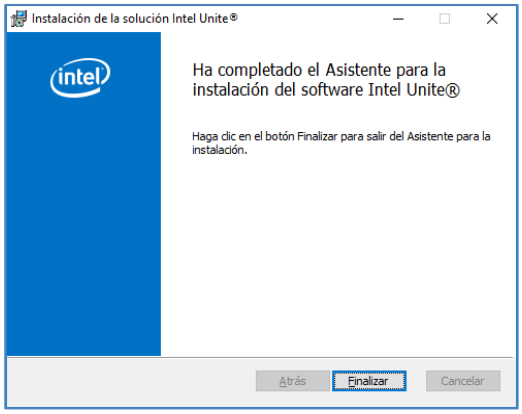
- Se abrirá la ventana **Carpeta de destino** con la carpeta predeterminada donde se instalará la aplicación Intel Unite en el cliente. Puede cambiar la carpeta de destino si lo desea. En caso contrario, mantenga la ubicación predeterminada.



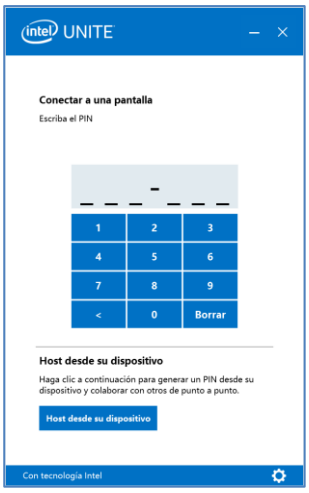
- Puede volver a revisar la configuración o bien hacer clic hacer clic en **Instalar** para continuar.



- Cuando haya terminado la instalación, verá la ventana **Ha completado el Asistente para la instalación del software Intel Unite®**, y después haga clic en **Finalizar**.



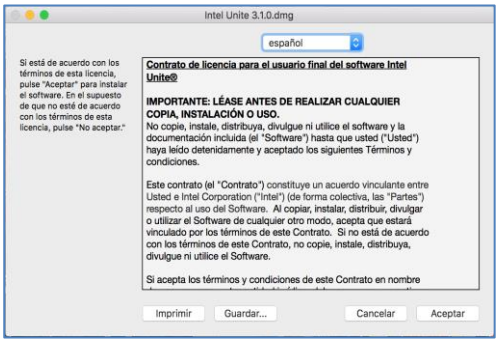
- Se mostrará la siguiente ventana **Conectar a una pantalla**:



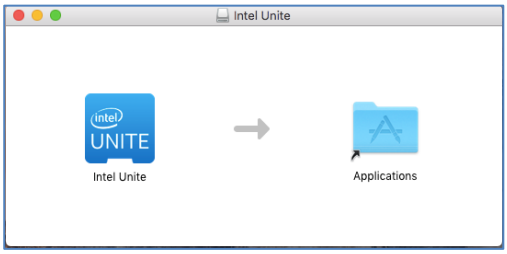
- Para conectarse al hub, introduzca el número PIN que aparece en el monitor o pantalla, por defecto el PIN cambia cada cinco minutos.
- Consulte la **Guía del usuario de la solución Intel Unite®** para obtener información sobre las funciones y la información del usuario.

6.3 Instalación del cliente macOS

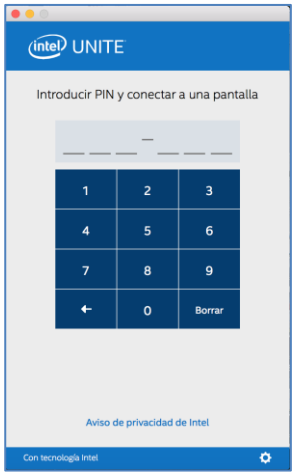
- Busque el archivo **Intel Unite macOS X,X.dmg** y descargue el software en el cliente Mac. Haga doble clic en el archivo para extraer la aplicación.
- Se le pedirá que acepte un **Contrato de licencia para el usuario final**. Haga clic en **Aceptar** para continuar.



- Cuando lo haya extraído, arrástrelo y suéltelo en la carpeta Aplicaciones.



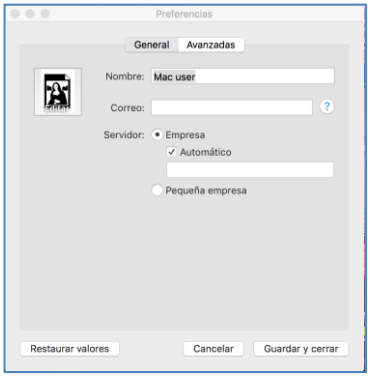
- Vaya a la carpeta Aplicaciones y busque la aplicación, haga clic para iniciarla.
- Se abrirá la pantalla **Introducir PIN y conectar a una pantalla**. Puede conectarse al hub con el PIN que aparece en el monitor o pantalla y empezar a compartir.

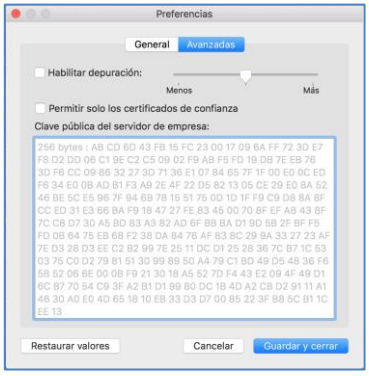


- Consulte la **Guía del usuario de la solución Intel Unite®** para obtener información sobre las funciones y la información del usuario.

Nota: La aplicación utilizará la detección automática de DNS (registro de servicio DNS) para localizar el Servidor empresarial. También se puede especificar un Servidor empresarial predeterminado

cambiando la configuración del archivo com.intel.Intel-Unite.plist localizado en la carpeta ~/Biblioteca/Preferencias del usuario:
defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD . Para obtener más información, consulte la sección *Solución Intel Unite para macOS* de esta guía.
También puede cambiar el Servidor empresarial al que la aplicación se conectará. Haga clic en el icono del engranaje en la esquina inferior derecha de **Conectar a una pantalla** para acceder a **Configuración**. Aparecerán dos pestañas:



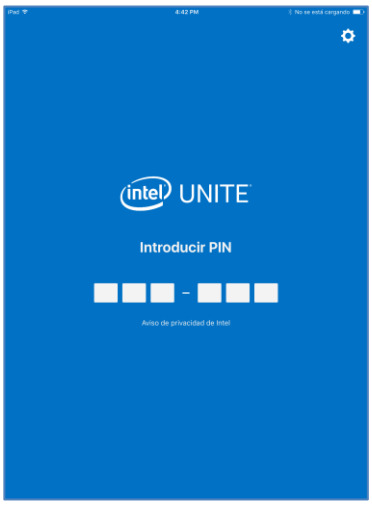


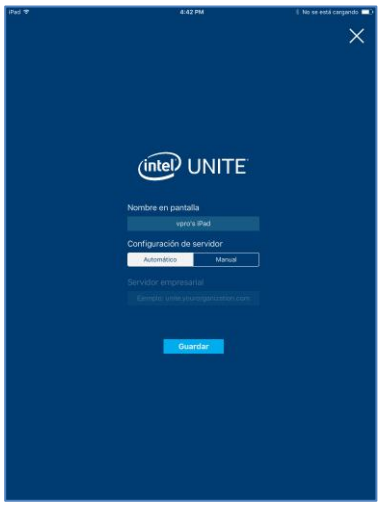
General: puede introducir el nombre, el correo electrónico y el avatar del usuario. También puede seleccionar si el equipo cliente se conectará al Servidor empresarial automáticamente (de manera predeterminada) o introduciendo una ruta definida al servidor.
Avanzadas: mediante esta pestaña puede seleccionar **Habilitar depuración** o seleccionar si se permitirán únicamente **Certificados de confianza**.

6.4 Instalación del cliente iOS

Esta aplicación es compatible con todos los iPads excepto el iPad original de 2010.

- En el cliente iOS (por ejemplo, un iPad) vaya a la App Store de Apple y descargue el software Intel Unite para su cliente.
- Una vez que haya descargado la aplicación, ábrala.
- Haga clic en el icono del engranaje en la esquina superior derecha para acceder a **Configuración** y escriba la información solicitada.



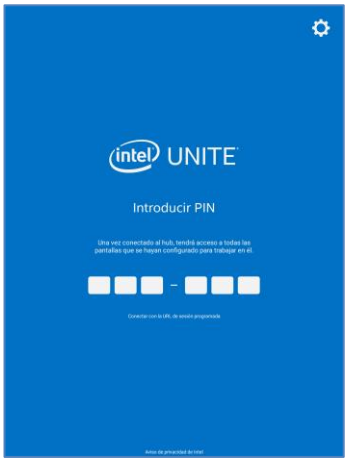


- En **Configuración** introduzca su nombre de pantalla y la información del servidor.
- Puede seleccionar **Automático** para buscar el servidor o, si desea conectarse a un servidor específico, haga clic en **Manual** e introduzca el servidor al que desea conectarse.
- Haga clic en **Guardar**.

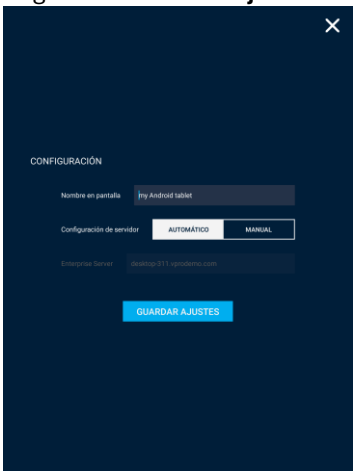
- Puede conectarse al hub con el código PIN que aparece en el monitor o pantalla y empezar a compartir.
- Consulte la **Guía del usuario de la solución Intel Unite®** para obtener información sobre las funciones y la información del usuario.

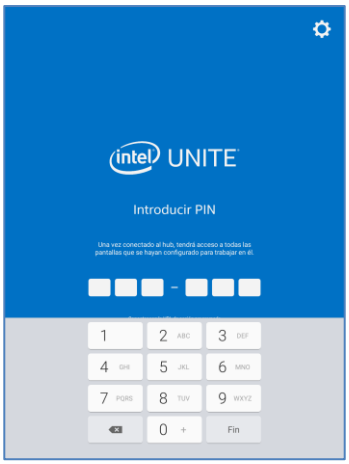
6.5 Instalación del cliente Android

- En su dispositivo Android vaya a la aplicación de Google Store y descargue el software Intel Unite para su cliente.
- Una vez que haya descargado la aplicación, ábrala.
- Haga clic en el icono del engranaje en la esquina superior derecha para acceder a **Configuración** y escriba la información solicitada.



- En **Configuración** introduzca su nombre de pantalla y la información del servidor.
- Puede seleccionar **Automático** para buscar el servidor o, si desea conectarse a un servidor específico, haga clic en **Manual** e introduzca el servidor al que desea conectarse.
- Haga clic en **Guardar ajustes.**

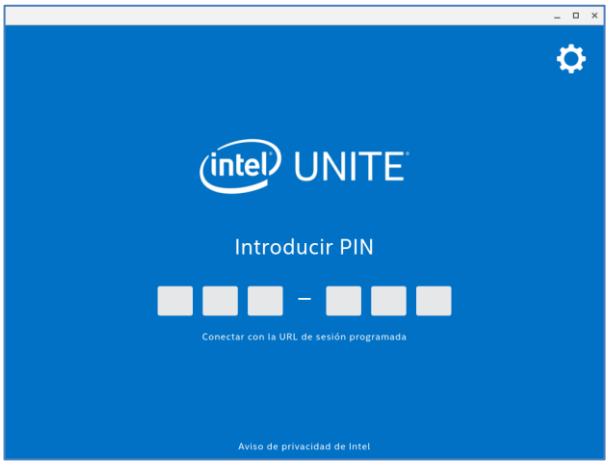




- Puede conectarse al hub con el código PIN que aparece en el monitor o pantalla y empezar a compartir.
- Consulte la **Guía del usuario de la solución Intel Unite®** para obtener información sobre las funciones y la información del usuario.

6.6 Instalación del cliente Chrome OS

- En su dispositivo Chromebook vaya a la aplicación de Google Store y descargue el software Intel Unite para su cliente.
- Una vez que haya descargado la aplicación, ábrala.
- Haga clic en el icono del engranaje en la esquina superior derecha para acceder a **Configuración** y escriba la información solicitada.



- En Configuración introduzca su nombre en pantalla, correo electrónico y la información del servidor. Puede seleccionar **Automático** para buscar el servidor o, si desea conectarse a un servidor específico, haga clic en **Manual** e introduzca el servidor al que desea conectarse.
- Haga clic en **Guardar ajustes.**

Puede conectarse al hub con el código PIN que aparece en el monitor o pantalla y empezar a compartir. Consulte la **Guía del usuario de la solución Intel Unite®** para obtener información sobre las funciones y la información del usuario.

6.7 Configuración del cliente

Los ajustes de configuración del cliente se pueden cambiar desde el portal de administración. El portal de administración contiene un perfil por defecto con los ajustes de configuración predeterminados que se aplican a todos los clientes que acceden al servidor. Las opciones de configuración se envían al cliente una vez que el cliente haya establecido conexión con el servidor empresarial. Los ajustes se actualizan cada vez que el cliente accede.
Consulte Configuración del perfil para conocer las opciones de configuración.

7 Instalación avanzada

7.1 Instaladores por scripts

Esta sección proporciona información para ejecutar los instaladores silenciosamente, sin que aparezcan menús ni ventanas. De esta manera, se indican los parámetros de propiedad al instalador a través de una línea de comandos.
Para ejecutar los instaladores silenciosos, abra el cuadro de comandos y use la siguiente línea de comandos:
msiexec /i "PATH_TO_CLIENT_MSI" PARAMETER=VALUE PARAMETER=VALUE ... /qn /l* “PATH_TO_LOG”

- /i indica los MSI especificados para la instalación. "RUTA_AL_CLIENTE-MSI" es el nombre de archivo del instalador al que está llamando.
- "PARAMETER=VALUE PARAMETER=VALUE ..." es una lista de los parámetros que se especifican en la tabla que aparece a continuación.
- El indicador /qn ejecutará el instalador en modo silencioso.
- El indicador /l* registrará la salida en el archivo de registro que especifique.

NOTA: Puede ver todas las opciones para **msiexec** ejecutando el comando: msiexec /?
A continuación, puede ver la lista completa de parámetros de propiedad que se pueden pasar a cada programa de instalación:

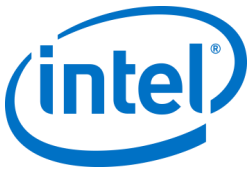
Parámetros de instalación del servidor	**Descripción**
DBHOSTNAME = "local" o "{IP}" o "{server},{port}" (definido como local)	Nombre de host de Microsoft SQL Server. Aquí será donde el instalador creará la base de datos UniteServer y añadirá la cuenta de servicio de la base de datos. Si está instalando la base de datos en el equipo actual, no es necesario incluir este parámetro, ya que de forma predeterminada está definido como local.
DBLOGONTYPE = “WinAccount” o “SqlAccount” → el valor predeterminado es WinAccount	Especifica el tipo de inicio de sesión para acceder a Microsoft SQL Server. Puede elegir entre la autenticación de Windows o la autenticación SQL.
DBUSER = “{SQL username}” DBPASSWORD = “{SQL password}”	Si el tipo de sesión es SqlAccount, indique el nombre de usuario y la contraseña. NOTA: Esta cuenta debe tener permisos para agregar la base de datos y crear la cuenta de servicio de la base de datos.
DBLOGONPASSWORD = “{contraseña de la cuenta de servicio}”	Contraseña que utilizará la cuenta de servicio para conectarse a la base de datos UniteServer.
DBLOGONPASSWORDCONF = “{contraseña de la cuenta de servicio}”	Esta variable debe tener el mismo valor que el especificado en DBLOGONPASSWORD
Parámetros de selección de las características del servidor	**Descripción**

ADDLOCAL = "ALL"	Solo hay dos opciones: ALL = instala la base de datos Y el servidor PIN, el portal de administración y la página de descarga. (no especifique esta variable) = instala el servidor PIN, el portal de administración y la página de descarga.
Parámetros de instalación del cliente y del hub	**Descripción**
PINSERVERLOOKUPTYPE = "Lookup" o "Manual" la opción predeterminada es la de "Lookup" (Búsqueda)	Especifica el modo en que la aplicación buscará el servidor PIN. La búsqueda empleará el registro de servicio DNS, mientras que "Manual" requiere que escriba los parámetros PINSERVER.
PINSERVER = “{hostname}”	El nombre de host del servidor al que desea conectarse.
CERTKEYCHECKED = "1" o "0" El valor predeterminado es 0	Este parámetro es opcional. 0 = no comprobar el hash de clave del certificado 1= comprobar el hash de clave del certificado; también es necesario especificar CERTKEY.
CERTKEY = “{certificate key}”	Este parámetro es opcional. Introduzca la clave pública de certificado del servidor PIN.
ACCESOS DIRECTOS	Opcional. Ajustar en "1" para colocar accesos directos en el escritorio.
INSTALLTYPE = hay dos valores posibles "Enterprise (Empresarial)" e "Independiente (Standalone)".	Si INSTALLTYPE está ajustado en "Enterprise (Empresarial)", el cliente/hub se instalará como empresa. Si INSTALLTYPE está ajustado en "Independiente (Standalone)", el cliente/hub se instalará como independiente.
SKIP_EXTENDED_DISPLAY= "1" o "0" El valor predeterminado es 0	0 = Falso 1= Verdadero

7.2 Claves de registro

Las claves de registro se escriben en el registro al ejecutar los instaladores y la aplicación. Los valores de algunas de estas claves se pueden ajustar de acuerdo con el resultado que se desea obtener. Consulte la lista que aparece a continuación para entender las claves escritas por la aplicación Intel Unite:

Claves de registro: (usuario actual)	Valor	Dispositivo
HKEY_CURRENT_USER\software\Intel\Unite\ ActiveConnection (DWORD)	[0 = No hay usuarios conectados 1 = Hay usuarios conectados]	Hub



HKEY_CURRENT_USER\software\Intel\Unite\ PublicKey (String)	[clave pública de certificado de conexión]	Ambos
HKEY_CURRENT_USER\software\Intel\Unite\ CurrentPin (String)	[PIN actual de este sistema]	Hub
HKEY_CURRENT_USER\software\Intel\Unite\ DoNotShowPrivacyStatement (DWORD)	[0 = Declaración de privacidad al iniciar 1 = No se muestra la declaración de privacidad]	Ambos
HKEY_CURRENT_USER\software\Intel\Unite\ HWThumbprint (String)	[hash de HW]	Ambos
HKEY_CURRENT_USER\software\Intel\Unite\ ServicePort (DWORD)	[puerto en el que se está escuchando el servicio]	Hub
HKEY_CURRENT_USER\software\Intel\Unite\ ActivePresenter	[1 = Hay un cliente presentando 0 = Ningún cliente está presentando]	Hub
HKEY_CURRENT_USER\software\Intel\Unite\PinPadWindows (DWORD)	[1 = La aplicación está preparada para introducir un PIN 0 = Lo contrario]	Cliente
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\SSID Referencia: Guía del complemento de acceso de invitado	Si define un valor predeterminado, se reducirá la seguridad en el acceso de invitado	Hub
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\PSK Referencia: Guía del complemento de acceso de invitado	Si define un valor predeterminado, se reducirá la seguridad en el acceso de invitado	Hub
HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\Download Referencia: Guía del complemento de acceso de invitado	El enlace de descarga predeterminado es http://192.168.173.1/download	Hub

HKEY_CURRENT_USER\software\Intel\Unite\ShowAvToggle (DWORD) = 1 (Modo A/V. Activar o desactivar la alternancia)	Modo Aero de Windows 7. Permite al usuario alternar entre RTF y WebRTC.	Client e
Claves de registro: (equipo)	**Valor**	**Dispo sitivo**
HKEY_LOCAL_MACHINE\software\Intel\Unite\ HubUnlockPassword (String)	[contraseña para salir de la aplicación del hub]	Hub
HKEY_LOCAL_MACHINE\software\Intel\Unite\ DisableCheckCertificateChain (DWORD)	[Conjunto para certificados autofirmados, donde 1 = no comprobar la cadena de certificado del Servidor empresarial]	Ambo s
HKEY_LOCAL_MACHINE\software\Intel\Unite\ DisableUsageCollection (DWORD)	[1 = desactivar la recopilación de datos de telemetría]	Ambo s
HKEY_LOCAL_MACHINE\software\Intel\Unite\WindowedMode (DWORD) (solo funciona en modo Pequeñas empresas, no en modo Empresarial)	[1 = El usuario quiere iniciar el hub en modo de ventana (con botones para minimizar, maximizar y salir) 0 = Lo contrario]	Hub
HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD)	[1 = Se debe omitir la comprobación de algoritmos del certificado 0 = El certificado empresarial está forzado a utilizar un certificado SHA2]	Ambo s

HKEY_LOCAL_MACHINE\software\Intel\Unite\ShowOnlyInOneMonitor (DWORD)	[Esta clave solo funciona si el modo de ventana se establece en 1. 1 = Solo se mostrará una ventana de PIN aunque haya más monitores conectados]	Hub
HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Unite\S4BPlugin Keywords (cadena) = lista,de,palabras,clave,separadas,por,comas	Clave que se utiliza para el complemento de Skype Empresarial	Hub
HKEY_LOCAL_MACHINE\software\Intel\Unite\ LogFile (String)	[ruta al nombre de archivo con acceso de escritura para registrar los mensajes de depuración en tiempo de ejecución]	Ambos

8 Guía del portal de administración

El portal de administración es el portal web del administrador de la aplicación Intel Unite que le permite ver y administrar los dispositivos en los que se instala la aplicación Intel Unite. Es uno de los componentes que se instalan en el servidor empresarial junto con el servicio PIN y el servidor web durante el proceso de instalación. (Consulte la sección Instalación del servidor empresarial). Es posible que el portal de administración no esté en el mismo servidor que la base de datos, siempre que tenga acceso a la base de datos.

Además de las nuevas funciones, la apariencia del portal de administración también ha cambiado; se han agregado menús de ayuda e información sobre las funciones para facilitar la configuración de los hubs y dispositivos cliente.

- Para acceder al portal de administración vaya a su navegador y siga el enlace asignado al portal, https://<sunombredeservidor>/admin, donde <sunombredeservidor> es el nombre asignado al servidor Intel Unite (Nombre predeterminado = UniteServer, por ejemplo https://uniteserver/admin)

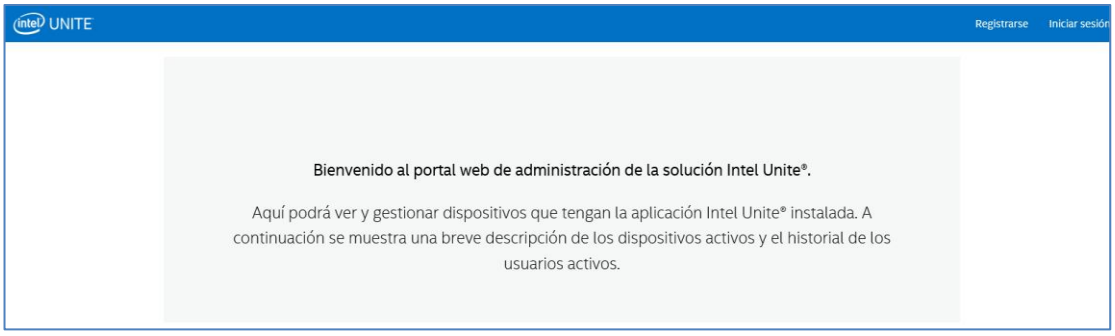
Cuando el administrador de TI ejecutó los instaladores de software, se creó una cuenta de administrador predeterminada con el siguiente nombre de usuario y contraseña:

- Usuario: admin@server.com
- Contraseña: Admin@1

Esta cuenta tiene acceso completo al portal de administración y le permitirá iniciar sesión, sin embargo, el sistema le pedirá que la cambie. Si ya ha registrado una cuenta, introduzca su información de inicio de sesión para acceder al portal de administración.

8.1 Página de bienvenida del portal web de administración

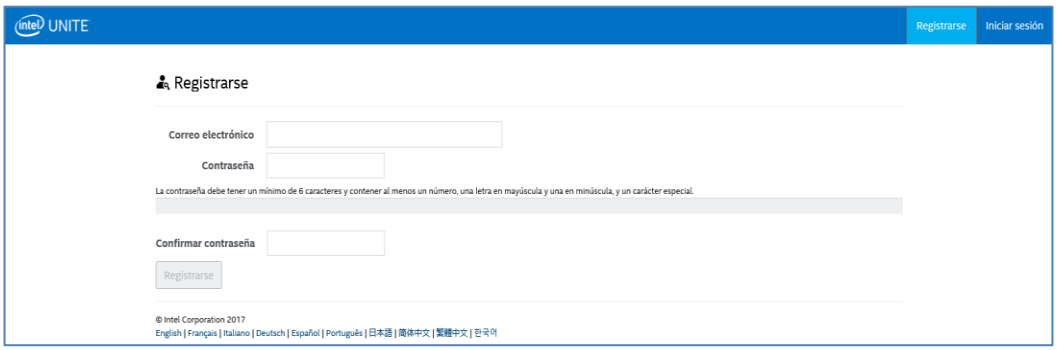
La página de bienvenida se mostrará cuando se conecte al portal de administración. Para acceder a la página de inicio debe iniciar sesión con la cuenta predeterminada creada durante la instalación o con la información de su cuenta.



8.1.1 Registrar una cuenta

Para registrar una cuenta, asegúrese de que está desconectado del portal de administración.

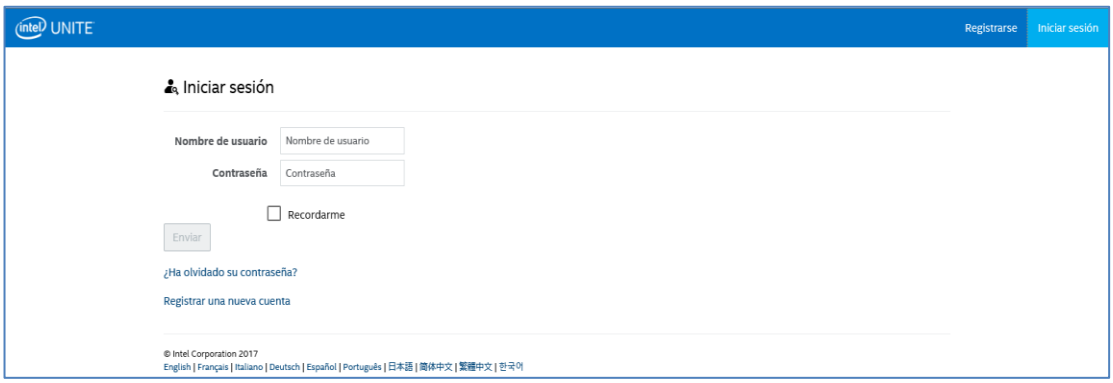
- Haga clic en el enlace para **Registrarse** que aparece en la parte superior derecha de la barra de navegación.
- Rellene el formulario con la dirección de correo electrónico y contraseña que desee, y haga clic en **Registrarse**.



- Como alternativa, puede agregar o registrar usuarios a través de la pestaña Administración una vez que haya iniciado sesión en el portal de administración.

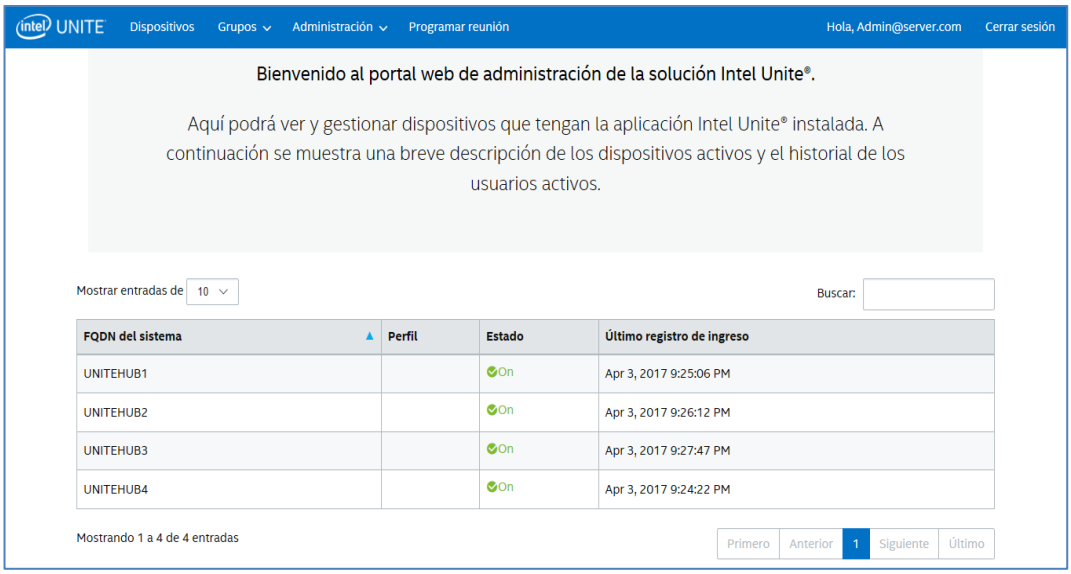
8.1.2 Iniciar sesión con una cuenta existente

Puede iniciar sesión con una cuenta registrada o utilizar la cuenta predeterminada creada durante la instalación. Como recordatorio, esta cuenta tiene acceso completo al portal de administración y se recomienda cambiar la contraseña para asegurarse de que se restringe el acceso a usuarios externos al portal.



8.2 Página de inicio del portal de administración

Esta página de inicio contiene un mensaje de bienvenida y ofrece una breve descripción general de todos los sistemas activos (clientes y hubs) que han accedido al servidor. La tabla muestra el nombre de cada **Sistema**, el **Perfil** asignado a cada uno, el estado de **Activado (ON)** o **Desactivado (OFF)**, y la fecha y hora del **último registro de ingreso**.



Las entradas de la tabla se pueden filtrar utilizando el cuadro de búsqueda con varias palabras clave; cada palabra clave buscará en todas las columnas. Puede seleccionar el número de entradas que desea mostrar en esta ventana haciendo clic en el Mostrar <número> entradas. Puede ver 10, 25, 50 o hasta 100 entradas.

8.2.1 Barra de navegación

Desde la barra de navegación se puede acceder a las diferentes secciones del portal web y se puede ver qué usuario ha iniciado sesión. Si ningún usuario ha iniciado sesión, aparecerá la opción **Registrarse** para hacerlo.

Las páginas y subpáginas son del portal web son:

- **Dispositivos**
- **Grupos**
  - Grupo de dispositivos
  - Perfiles
- **Administración**
  - Propiedades de servidor
  - Usuarios
  - Roles
  - Moderadores
  - PIN reservado
  - Telemetría
- **Programar reunión**

Para obtener más información, vaya a la sección asignada a cada tema en este capítulo del portal de administración.

8.2.2 Nomenclatura de iconos y enlaces

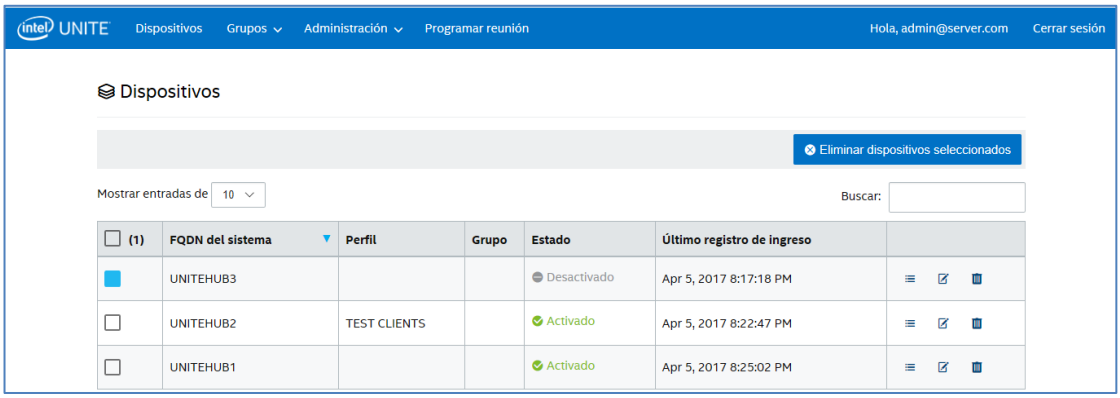
En el portal de administración, verá continuamente los siguientes iconos y enlaces:

	Editar
	Ver detalles
	Ver dispositivos
	Eliminar
	Cuadro de diálogo que contiene información acerca de un valor específico

Si coloca el cursor sobre el icono podrá consultar la información relativa a cada elemento.

8.3 Página Dispositivos

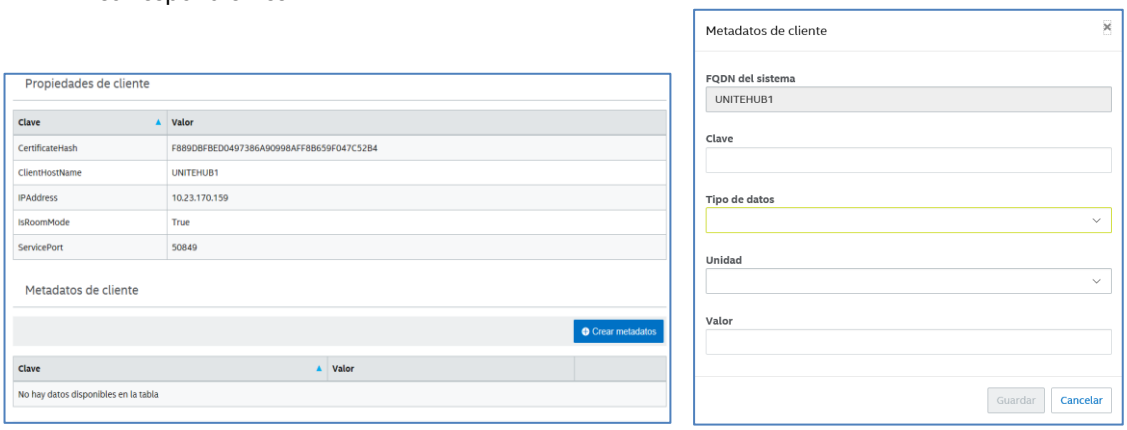
La página Dispositivos contiene todos los dispositivos que se encuentran actualmente en la base de datos. Puede seleccionar un dispositivo específico y **Ver**, **Editar**, **Actualizar** o **Eliminar** en consecuencia.



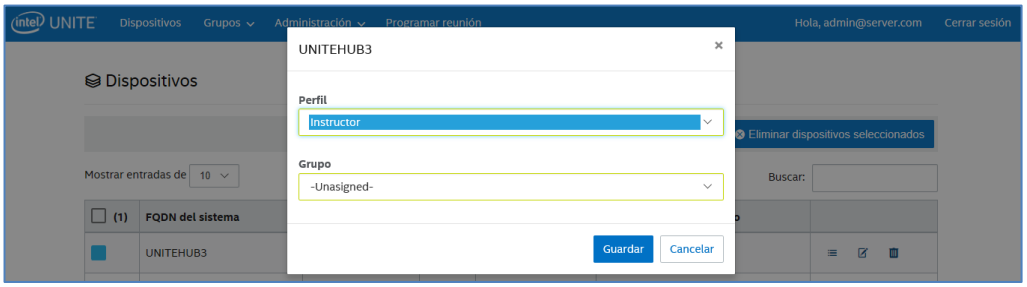
En la página **Dispositivos** encontrará:

- **FQDN de sistema** es el nombre de dominio completamente cualificado del cliente/hub
- **Perfil** dispone de ajustes de configuración que se aplican al dispositivo
- **Grupo** es el nombre del grupo al que se ha asignado el dispositivo
- **Estado** muestra si el dispositivo está encendido, ON (verde), o apagado, OFF (gris)
- **Último registro de ingreso** es la última vez que el dispositivo accedió al servidor
- **Detalles**: si hace clic en el enlace **Ver detalles**, aparecerá la ventana **Propiedades del cliente** con las propiedades del sistema y sus metadatos. Algunas de las claves en **Propiedades del cliente** son:
    - CertificateHash
    - ClientHostName
    - IPAddress
    - IsRoomMode
    - SevicePort

Para obtener más información acerca de los valores válidos para cada clave, vaya a la sección Configuración del perfil que proporciona detalles acerca de las claves y los valores correspondientes.



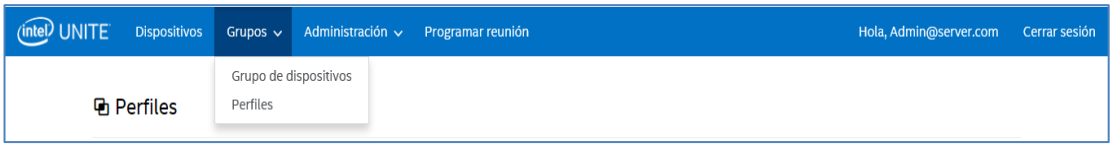
Editar enlace: hacer clic en el enlace Editar le permite editar el perfil de dispositivo y asignar el dispositivo a un grupo específico



Eliminar enlace: hacer clic en el enlace Eliminar eliminará el dispositivo desde el portal de administración. Antes de que se elimine el dispositivo, recibirá un mensaje de confirmación. Como alternativa, puede seleccionar en la columna izquierda uno o varios dispositivos y hacer clic en el botón **Eliminar dispositivos seleccionados.**

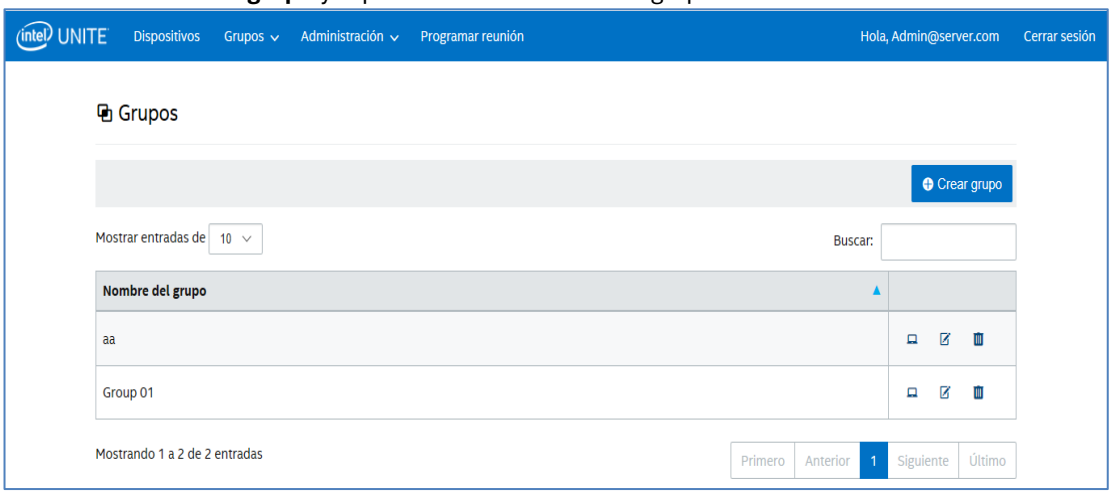
8.4 Página Grupos

La página **Grupos** ofrece dos opciones en el menú: **Grupo de dispositivos** y **Perfiles**.



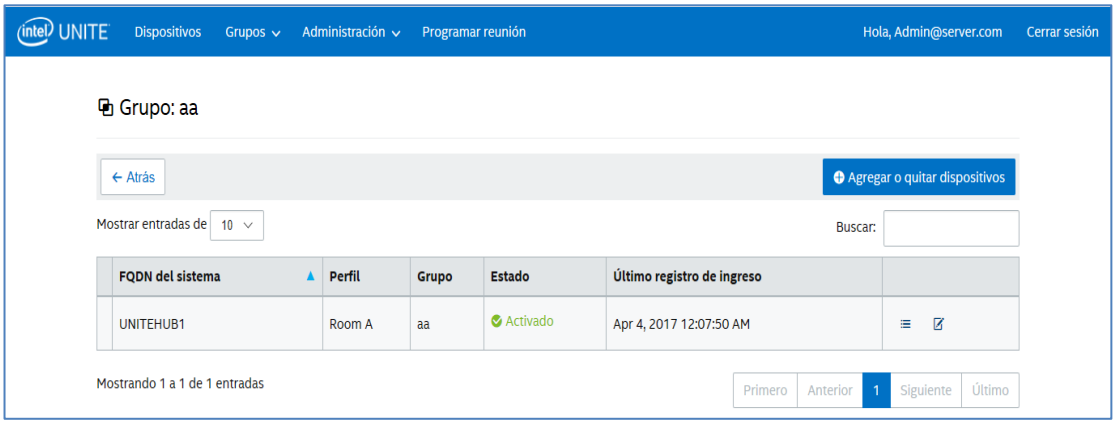
8.4.1 Grupos > Grupo de dispositivos

Grupo de dispositivos proporciona una forma de agrupar los dispositivos para su supervisión, funcionalidad o comodidad. Puede tener dispositivos asignados a un grupo con un perfil igual o diferente. Esta página le permite crear, ver, modificar y eliminar grupos y entradas para cada grupo. Puede crear un nuevo grupo haciendo clic en **Crear grupo** y especificando el nombre del grupo.



Una vez que haya creado el grupo, puede:

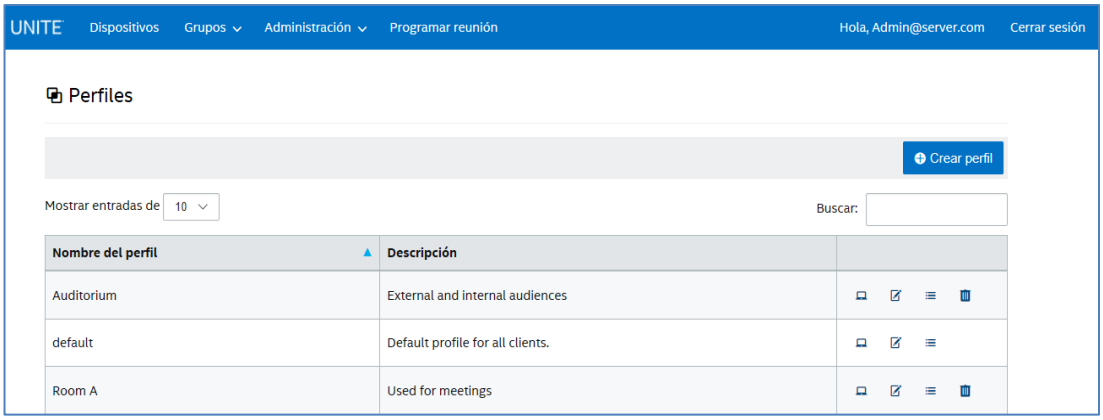
- Hacer clic en el enlace **Ver dispositivos** para agregar dispositivos al grupo seleccionado o eliminarlos, o puede hacer clic en el enlace **Detalles**, en la columna de la derecha, para ver las propiedades y los metadatos de los sistemas que pertenecen a este grupo.



- Hacer clic en el enlace **Editar** para actualizar o cambiar el **Nombre del grupo**.
- Si ha realizado algún cambio, haga clic en **Guardar** para conservar los cambios.

8.4.2 Grupos > Perfiles

En esta página se pueden crear, visualizar, eliminar y modificar los perfiles. Esta página tiene un diseño y funcionamiento parecidos a **Grupo de dispositivos**, pero se diferencia en que contiene perfiles. La diferencia entre **Grupos** y **Perfiles** es que el último contiene las opciones de configuración de dispositivos. Los dispositivos solo pueden pertenecer a un perfil, pero pueden estar incluidos en muchos grupos de dispositivos.



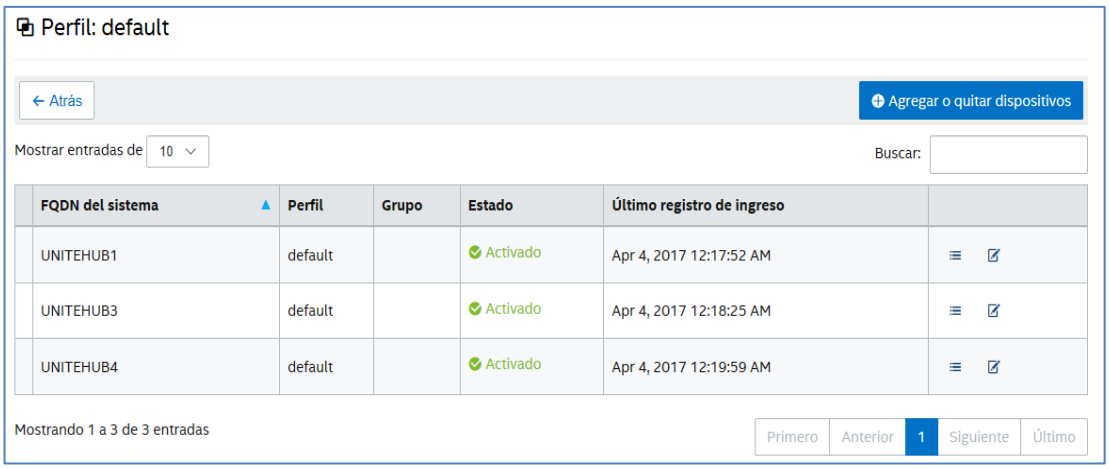
La página **Perfiles** muestra el **Nombre del perfil** y la **Descripción** de cada perfil disponible en el servidor. Los perfiles se aplican a todos los dispositivos que incorporan Servidor empresarial. Notará que el perfil **predeterminado** no se puede eliminar del portal de administración.

Al hacer clic en el enlace **Ver dispositivos**, verá los sistemas que se han asignado al perfil seleccionado. Al hacer clic en el enlace **Editar**, puede actualizar el nombre del perfil y su descripción.

Al hacer clic en el enlace **Ver detalles** de un perfil determinado, puede tener acceso y editar la configuración de la clave y el valor del perfil predeterminado o creado recientemente. Se mostrará una lista con todas las claves, su valor y el enlace **Editar** para actualizar o personalizar en consecuencia. Consulte la sección *Configuración del perfil* para obtener información detallada acerca de las claves y los valores correspondientes.

8.4.2.1 Perfil predeterminado

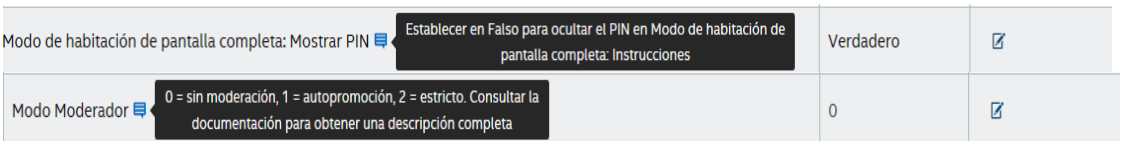
El perfil **predeterminado** no se puede eliminar del portal de administración. Puede crear otros perfiles, pero sepa que el predeterminado no se eliminará.



Claves y valores **predeterminados**:

Clave	Valor	
Permitir transferencia de archivos	Falso	
Asistencia de transmisión de audio y video	Verdadero	
Cambiar PIN durante la reunión	Verdadero	
Desactivar visualización remota	Falso	
Mostrar tamaño de PIN	48	
Mostrar transparencia de PIN	100	
Extensiones de archivo bloqueadas		
Tamaño máximo de archivo	2147483647	
Modo de habitación de pantalla completa	Verdadero	
Color de fondo de modo de habitación de pantalla completa		
Modo de habitación de pantalla completa: Expansión de imagen de fondo	Falso	
Modo de habitación de pantalla completa: URL de fondo		
Modo de habitación de pantalla completa: Instrucciones	{pin}	
Modo de habitación de pantalla completa: Color de PIN		
Modo de habitación de pantalla completa: Mostrar PIN	Verdadero	
Modo de habitación de pantalla completa: Color del texto		
Modo de habitación de pantalla completa: Fuente del texto		
Hub: Bloqueo de teclado	Falso	
Hub: Mostrar reloj	Verdadero	
Modo Moderador	0	
Enviar dirección de correo electrónico de envío de errores		
Puerto de escucha del servicio	0	
Compresión de mosaico	85	
Tamaño de mosaico	128	
Verificar hash del certificado de complemento	Verdadero	

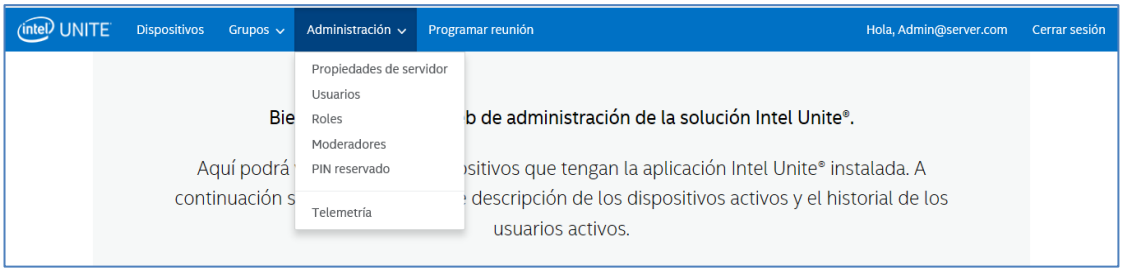
Tenga en cuenta que con cada clave aparece un cuadro de diálogo; si coloca el cursor en el cuadro de diálogo, podrá ver los valores y la información sobre cada clave, que le proporcionarán la información que necesita antes de editarla. Consulte los dos ejemplos siguientes:



También puede consultar la tabla proporcionada en Configuración del perfil para obtener información detallada sobre las claves y los valores correspondientes.

8.5 Página Administración

La página Administración se despliega en varias páginas secundarias:

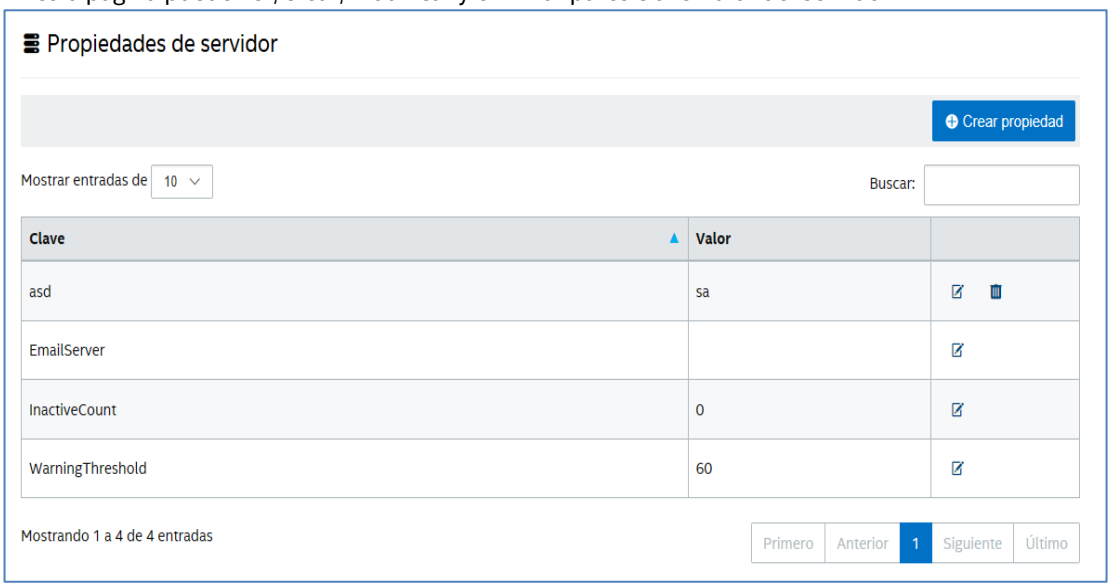


- **Propiedades de servidor**: es la interfaz para visualizar y modificar valores y claves del servidor.
- **Usuarios**: puede agregar, quitar o modificar manualmente cualquier cuenta en esta página.
- **Roles**: le permitirá crear nuevos roles, actualizar los existentes, asignar usuarios a los roles y editar los permisos para la administración de usuarios.
- **Moderadores**: esta función permite a los usuarios tomar el control de una reunión y agrupar las funcionalidades en roles. En esta sección puede eliminar o agregar moderadores con facilidad.
- **PIN reservado**: esta función permite a los administradores de TI asignar números PIN a ciertas aulas. El TI puede generar automáticamente o manualmente los números PIN según las necesidades de la sesión o la ubicación de la sala.
- **Telemetría**: para poder ver los datos de telemetría, se debe instalar el complemento de telemetría para la solución Intel Unite®. El complemento de telemetría de Intel permite que los administradores de TI recopilen información sobre el uso de la aplicación Intel Unite y los dispositivos cliente conectados a cada hub.

Consulte las secciones que aparecen a continuación para obtener más información sobre estas páginas secundarias.

8.5.1 Administración > Propiedades de servidor

En esta página puede ver, crear, modificar y eliminar pares clave-valor del servidor.



Las claves que utiliza el portal de administración son:

- **EmailServer:**: este es el correo electrónico donde el servidor envía las notificaciones.

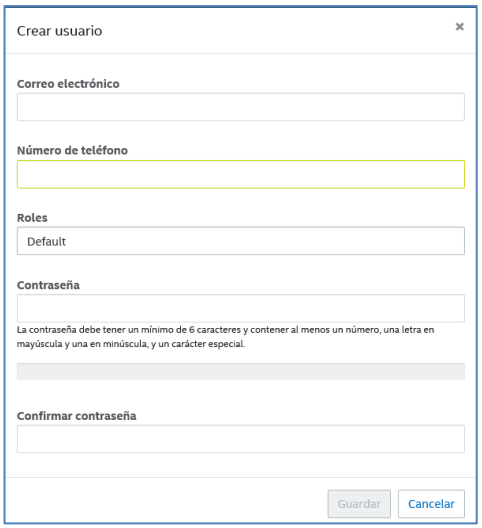
- **InactiveCount:** lo utiliza la herramienta de seguimiento de estado de la aplicación Intel Unite, que envía correos electrónicos a los usuarios con roles de Notificaciones asignados.
- **WarningThreshold**: se utiliza para determinar el umbral de cuando un dispositivo se considera inactivo, en minutos, con un valor predeterminado de 60.

Al hacer clic en el enlace **Editar**, puede actualizar las claves en consecuencia.

8.5.2 Administración > Usuarios

En la página **Usuarios** se mostrará una lista de todos los usuarios registrados en el portal de administración, si su cuenta ha sido bloqueada, y sus roles. También puede actualizar esta información haciendo clic en el enlace **Editar**.

Puede agregar un nuevo usuario haciendo clic en **Crear usuario** y proporcionando un correo electrónico, un número de teléfono y una contraseña. Al crear el usuario, también puede asignar un rol específico o dejar el valor predeterminado. Para asignar derechos de acceso al nuevo usuario, puede definir roles y asignar el usuario a un rol.



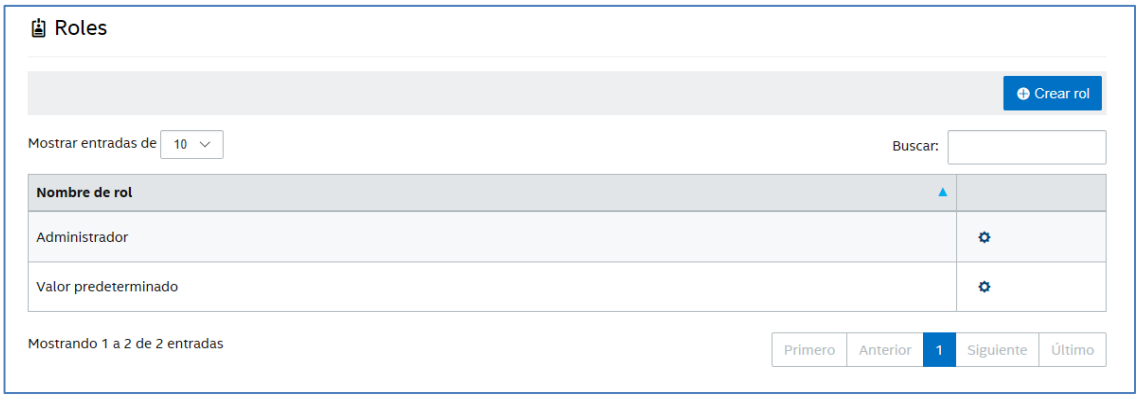
En esta misma página, al hacer clic en el rol (**Predeterminado** o **Administrador**) se abrirá la página **Roles**. Continúe con la siguiente sección para obtener más información acerca de **Roles**.

NOTA sobre la cuenta predeterminada: Si se añade una nueva cuenta de usuario iniciando sesión con la cuenta admin@server.com predeterminada, no se enviará una verificación automática de correo electrónico. Para verificar manualmente la dirección de correo electrónico, inicie sesión en la nueva cuenta,

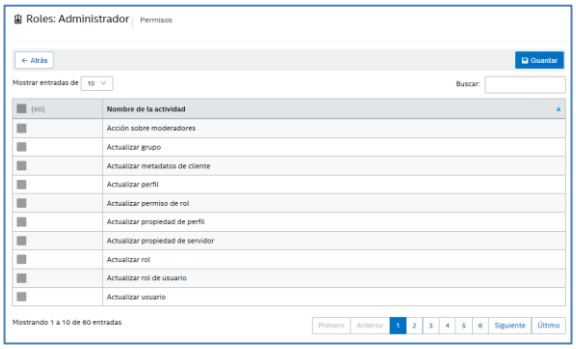
haga clic en la frase de bienvenida "Hola, <su nombre de usuario>" en la parte superior derecha de la barra de navegación y pulse el botón "**Enviar verificación de correo electrónico**" en la parte inferior de la página. Antes de hacer esto, debe cambiar la configuración de correo del servidor en el archivo xml web.config. Consulte la sección Configuración del servidor de correo electrónico.

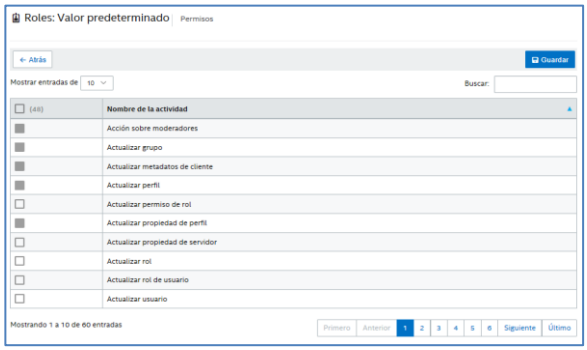
8.5.3 Administración > Roles

Esta página muestra los roles que están definidos actualmente, que son **Administrador** y **Predeterminado**. Puede agregar nuevos roles y editar los que ya existen. Los roles no regulan el acceso al portal por si solos, sino que las acciones en el portal (por ejemplo, crear un usuario) están restringidas a los roles que están asociados con un conjunto de usuarios.



Para ver las actividades y permisos asignados a cada rol, haga clic en el icono del engranaje en la columna de la derecha, y se mostrará la ventana **Permisos**. Las actividades asignadas se pueden personalizar para permitir que un conjunto de roles realicen la acción.





Para agregar un nuevo rol, haga clic en el botón **Crear rol** y edite el nombre del rol y, a continuación, en la página **Roles**, haga clic en el icono del engranaje y seleccione las actividades que desea que realice este rol. Esto le permitirá agregar o eliminar permisos.
Tenga en cuenta que los usuarios se pueden asignar a varios roles.

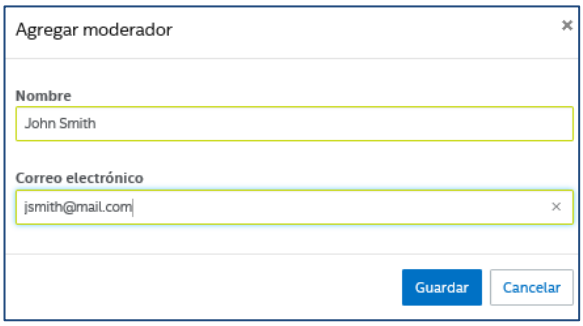
8.5.4 Administración > Moderadores

Esta página muestra los usuarios a los que se les ha asignado el rol Moderador. Para asignar un usuario como moderador, debe seguir unos pasos.

Hay dos maneras para agregar moderadores: puede hacer clic en **Agregar moderador** y rellenar los datos solicitados, o puede importar un archivo CSV con los nombres y los correspondientes correos electrónicos que desee agregar a la lista haciendo clic en **Importar moderadores de archivo CSV**. Si decide importar un archivo CSV con los nombres de los moderadores, asegúrese de que sigue el formato: **Nombre,Correo electrónico,Acción** o haga clic en el **Archivo de ejemplo** para ver el formato válido.

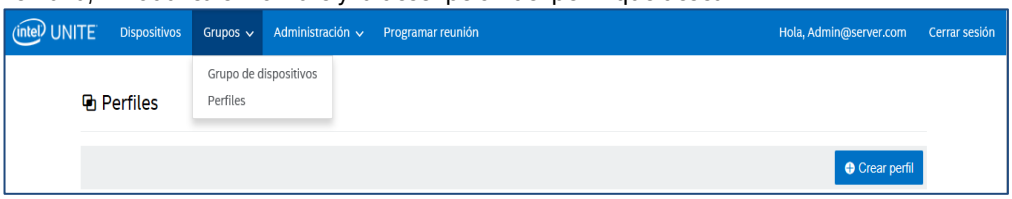
Ejemplo: John Smith,jsmith@aaa.com,Agregar
Sandra León,sleon@bbb.com,Eliminar

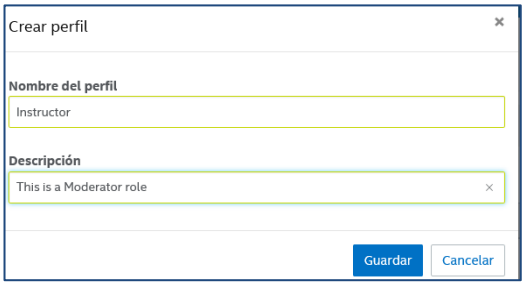
Haga clic en **Agregar moderador** para introducir manualmente el **Nombre** y **Correo electrónico** del moderador; haga clic en **Guardar** cuando haya terminado.



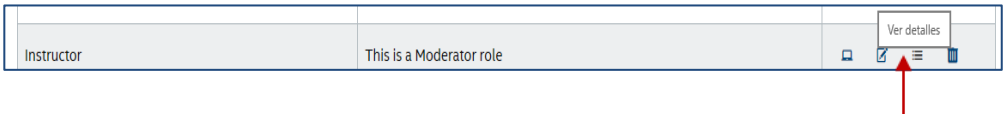
El modo de la funcionalidad del moderador debe establecerse en el perfil del hub, así puede tener un entorno mixto en sus sistemas. Para continuar, siga los siguientes pasos:

- Vaya a la página **Grupos** y seleccione **Perfiles**, haga clic en **Crear perfil** y, cuando se abra la ventana, introduzca el nombre y la descripción del perfil que desea.

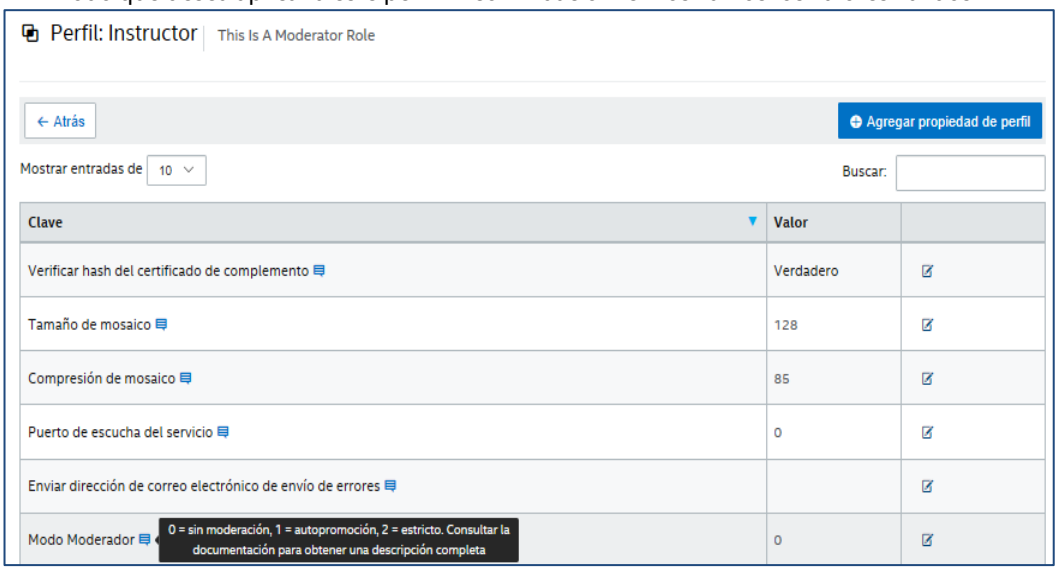




- Una vez ha creado el perfil, búsquelo en la lista y, en la columna de la derecha, haga clic en Ver detalles.



- En la columna **Clave**, busque la clave del **modo Moderador** e introduzca el **valor** deseado para el modo que desea aplicar a este perfil. A continuación le mostramos los valores válidos:



Descripción y valores del moderador:

0- **No administrado**: es el modo predeterminado, no hay moderadores en las reuniones/sesiones, todos los participantes tienen los mismos derechos para ver y presentar. Las versiones anteriores de este software Intel Unite (hasta la v3.1) utilizan este modo.

1- **Autopromocionado**: no se administra la reunión o sesión hasta que alguien se autopromociona a moderador. En este caso, solo el moderador puede asignar a otro participante como moderador. El moderador también puede asignar quién presenta durante la sesión.

2- **Estricto**: la reunión o sesión solo la administra el moderador. Cuando un moderador se une a la sesión, se promociona automáticamente a este rol.

Notas:

a. La lista de moderadores la gestiona el administrador de TI a través del portal de administración. Los moderadores se autentican con una clave asociada a su dirección de correo electrónico. Cuando se promociona un usuario a moderador, el portal de administración le envía un mensaje de correo electrónico que contiene un URI que, al hacer clic, instala el token de moderador en su cliente. Los usuarios solo tienen que pasar por este proceso una vez para cada sistema.

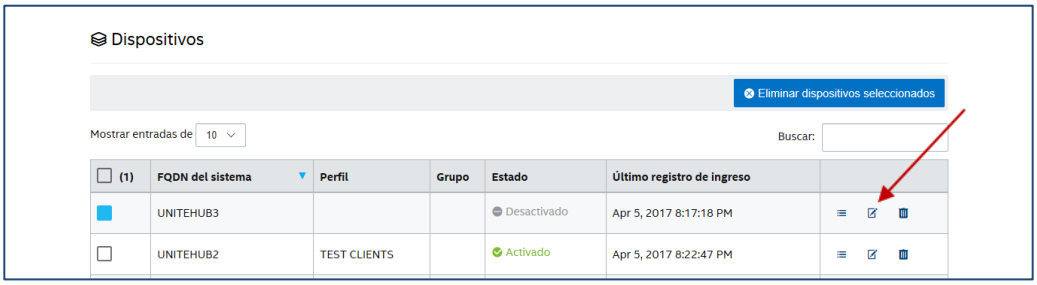
b. El administrador de TI puede revocar los derechos del moderador si elimina el token del usuario desde el portal de administración.

c. Para enviar correos electrónicos de registro a los moderadores, el equipo de TI necesita configurar un relé SMTP para que funcione.

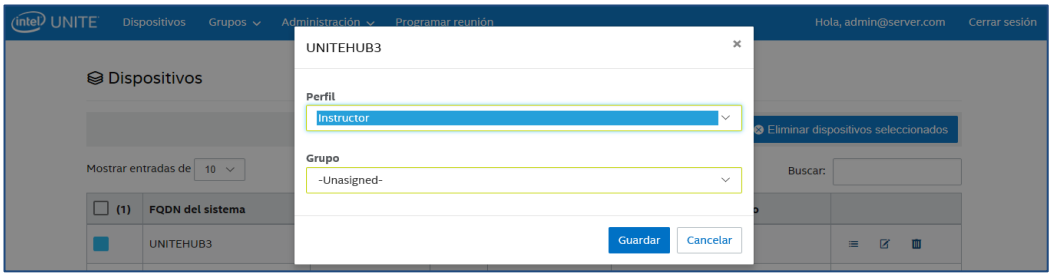
d. Si no dispone de un relé SMTP y tiene que generar manualmente el URI que se envía en el mensaje, realice lo siguiente:

Vaya a la pestaña **Administración** y seleccione **Propiedades del servidor**, haga clic en el enlace **Editar**, junto a **EmailServer**, e introduzca el relé SMTP, por ejemplo: smtp.example.com:22
Solo se puede configurar un relé SMTP que no requiera autenticación. También es posible obtener e instalar manualmente el token de moderador para un usuario; vaya a la sección **Instalación de token manual en modo Estricto** si desea más detalles.

- Para activar el perfil de moderador en un hub seleccionado, vaya a la página **Dispositivos**, seleccione de la lista el hub que desea configurar y haga clic en el enlace **Editar** situado en la columna de la derecha.



- Cuando se abra la ventana, seleccione el perfil creado para el moderador en la sección Perfil, y el grupo al que pertenece, si hay alguno, y seleccione **Guardar**.



Una vez que haya rellenado la lista de los moderadores, puede eliminar a cualquiera si selecciona uno (recuadro azul) y hace clic en **Eliminar**. Para enviar al moderador una URL para unirse a la reunión/sesión como moderador, seleccione su nombre y haga clic en **Enviar token**.

8.5.4.1 Instalación de token manual en modo Estricto

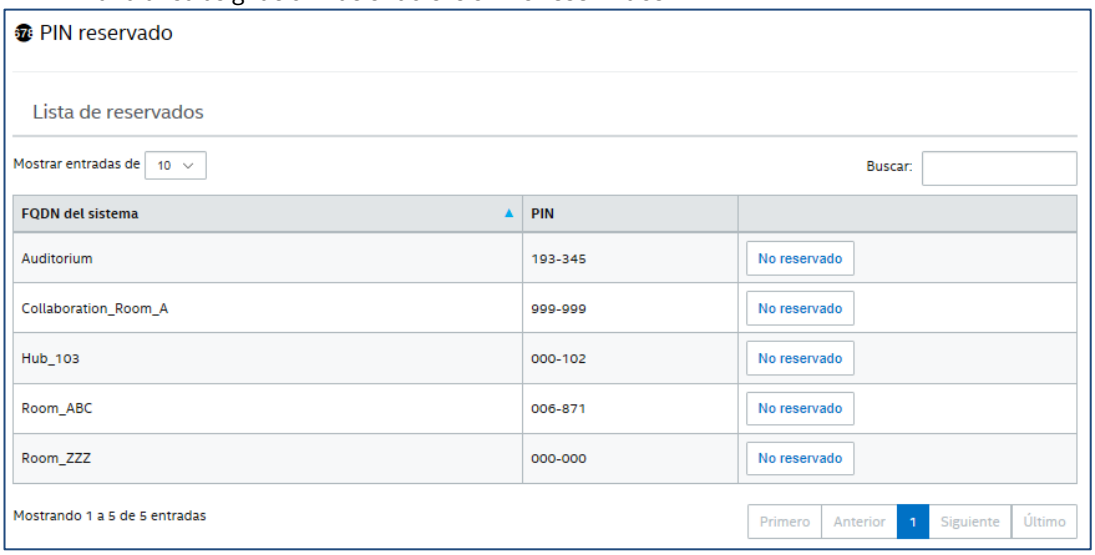
Si no dispone de un relé SMTP, es posible obtener e instalar manualmente el token de moderador para un usuario que se ha añadido como moderador. Para hacerlo, necesitará tener instalado Microsoft SQL Server Management Studio.
Para obtener el token:

- Agregue un moderador
- Abra Microsoft SQL Server Management Studio y conéctese al servidor de la bases de datos mediante las credenciales de administrador que utilizó durante la instalación del Servidor empresarial.
- Expanda "Bases de Datos", a continuación, "UniteServer", y después, "Tablas"
- Haga clic con el botón derecho en "dbo.Moderators" y en "Seleccionar hasta 1000"
- En los resultados, busque el "Nombre de usuario" que coincida con el que agregó en el paso anterior
- Haga clic con el botón derecho y copie el token en el portapapeles
- Abra el bloc de notas y cree el URI: intelunite://localhost/SetModerationToken?Token=<pegue el token que obtuvo en el paso anterior>
- Abra Intel Unite
- En dispositivos Windows: abra Windows Explorer, copie/pegue el URI completo y pulse Intro
- En dispositivos Mac: abra Safari, copie/pegue el URI completo y pulse Intro

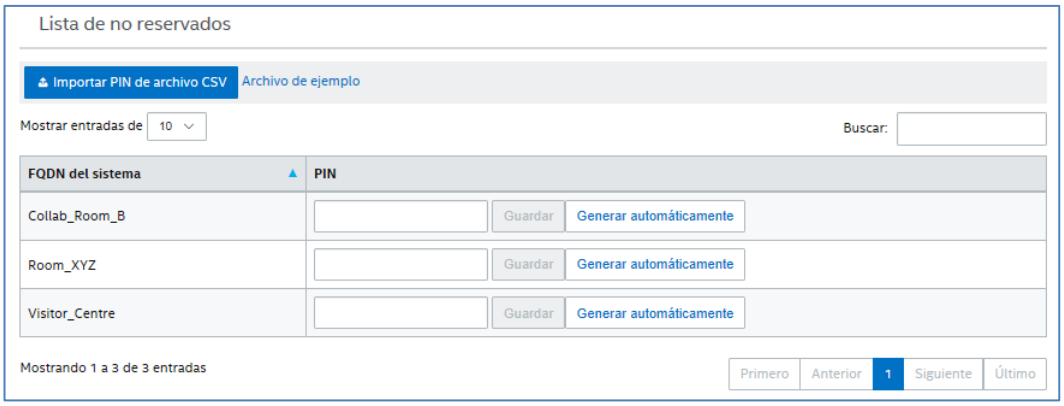
8.5.5 Administración > PIN reservado

Esta página le muestra dos secciones, la lista de sistemas **Reservados** y **No reservados** en las que se mostró el PIN durante la reunión/sesión, ya sea estática como no. Los administradores de TI pueden asignar sistemas en algunas salas, donde los usuarios podrán introducir el mismo PIN durante la reunión o sesión, o podrán tener un PIN de rotación, que es el valor predeterminado.

- **Lista de reservados**: esta es la lista de reservas que el equipo de TI ya ha configurado. Puede anular su asignación haciendo clic en **No reservados**.



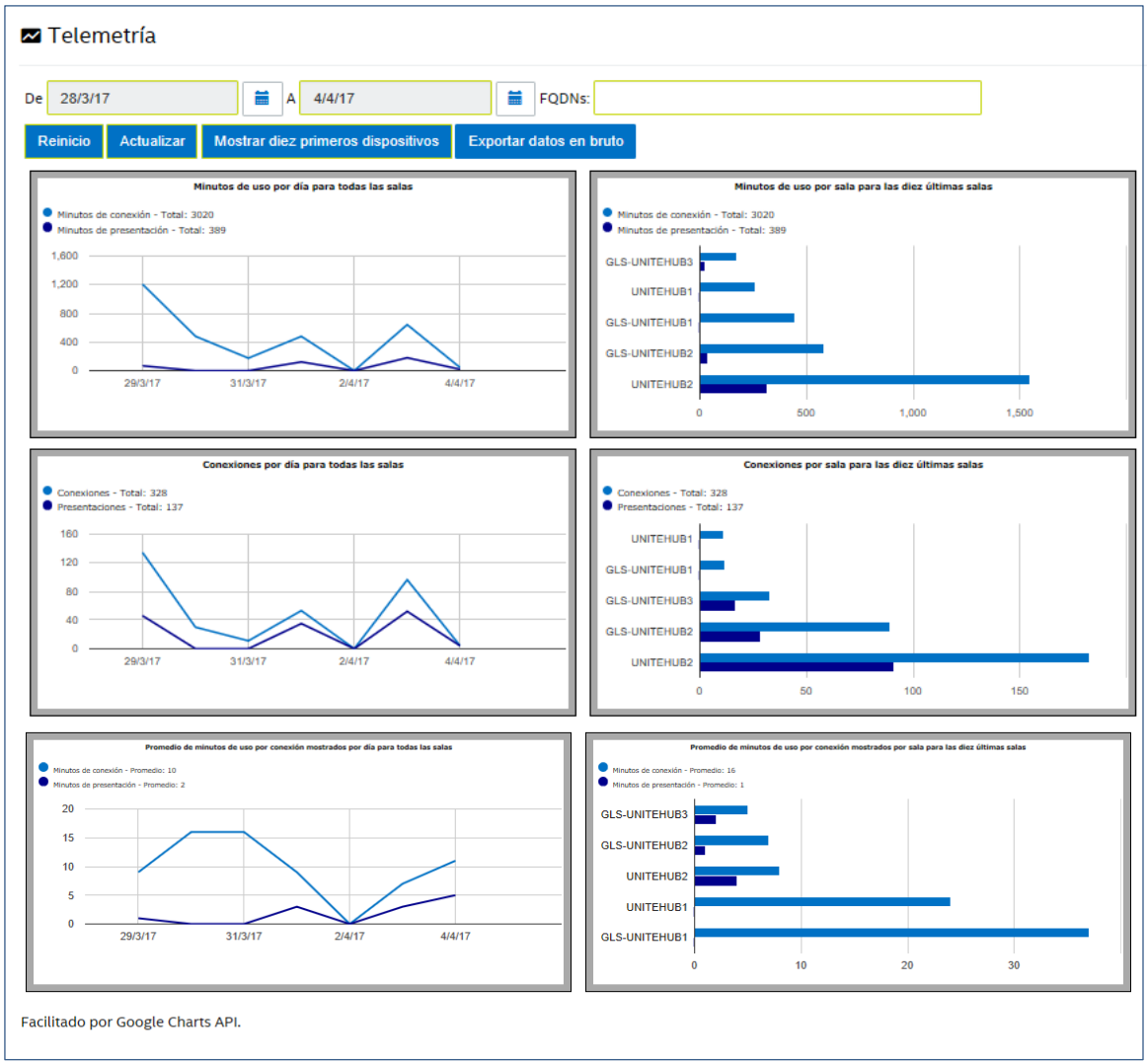
- **Lista de no reservados**: esta es la lista de los sistemas que no tienen reservas de PIN estáticos. Los PIN se pueden introducir manualmente, se pueden generar automáticamente o pueden importarse desde un archivo CSV.



Cuando asigne PIN, haga clic en **Guardar** para conservar los valores.

8.5.6 Administración > Telemetría

Esta página muestra los datos de telemetría recopilados por el portal de administración. Para poder verlos, debe tener instalado el complemento de la solución Intel Unite®. El complemento de telemetría de Intel permite que los administradores de TI recopilen información sobre el uso de la aplicación Intel Unite y los dispositivos cliente conectados a cada hub. El administrador de TI podrá consultar información diversa, como un número de conexiones en cada habitación, las conexiones por día, el tiempo medio usado por conexión, etc. Consulte la **Guía del complemento Intel Unite® de telemetría** para obtener más información e implementar el complemento en su sistema.



8.6 Página Programar reunión

La página Programar reunión es una función que creará una URL de reunión para los participantes de una reunión o sesión que no pueden instalar ni utilizar el complemento Intel Unite existente para Microsoft Office. Cualquier participante podrá ver esta página.

Simplemente haga clic en el botón **Generar nueva reunión** para crear la dirección URL y enviarla a los usuarios que participarán en la reunión o sesión.

8.7 Otras opciones de configuración para el portal de administración

8.7.1 Configuración del perfil

Los perfiles se pueden configurar accediendo a **Grupos** > **Perfiles** y haciendo clic en **Detalles**, en el perfil del portal de administración. Esto muestra los ajustes de configuración en forma de pares clave-valor. Puede cambiar los valores para personalizar la aplicación y la experiencia del espacio de reuniones o sesiones. Algunos ejemplos de ajustes que se pueden personalizar son las imágenes de fondo en la pantalla del hub, el tamaño de PIN, el color de la fuente y el contenido.
Tras personalizar los valores en un perfil, es necesario asignar dispositivos al perfil para aplicar los ajustes de configuración del perfil. Para aplicar el perfil a los dispositivos, haga clic en el enlace **Ver dispositivos** y, a continuación, en **Actualizar lista de dispositivos**. Aparecerá la lista de dispositivos; haga clic en la casilla de verificación que aparece junto al dispositivo para aplicar los ajustes de configuración.

La siguiente tabla muestra las **Claves** disponibles, su descripción, los tipos de datos y los valores predeterminados de las claves.

Clave	Descripción	Tipo de datos	Valor predeterminado
Permitir transferencia de archivos	Indicador para activar y desactivar la capacidad de un hub o cliente para transferir un archivo.	Booleano	Falso
Asistencia de transmisión de audio y video	Indicador para que los usuarios de Windows puedan presentar su escritorio con la experiencia audiovisual al completo (1080p a 20-30 fps)	Booleano	Verdadero
Cambiar PIN durante la reunión	Bloquee el PIN para una reunión o sesión; el PIN no se cambiará hasta que todos los usuarios se desconecten Verdadero = Permite que el PIN cambie durante la sesión	Booleano	Verdadero

	Falso = Bloquea el PIN durante la sesión		
Desactivar visualización remota	Cuando se haya establecido la opción de desactivar la vista remota desde algunas de las salas, si un usuario intenta ver el contenido mediante la vista remota, verá una imagen que indica que esta funcionalidad no está disponible Verdadero = Desactiva la vista remota Falso = Permite la vista remota	Booleano	Falso
Mostrar tamaño de PIN	Tamaño en píxeles. El valor es la altura en píxeles del PIN en pantalla (los valores más altos permiten leer el PIN más fácilmente desde cualquier parte de la sala)	Enteros	48
Mostrar transparencia de PIN	Controla la transparencia alfa del PIN que aparece en el monitor 100 = Visible al 100 % 1-99 = El PIN es visible dentro del cuadro que lo rodea; la opacidad cambia dependiendo del valor utilizado 0 = El PIN es transparente	Enteros	100
Las extensiones de archivo bloqueadas se muestran como Extensiones de archivo bloqueadas	Lista separada por comas de las extensiones de archivo bloqueadas (por ejemplo exe, bin, msi)	Cadena	Blanco
El tamaño máximo de archivo se muestra como Tamaño máximo de archivo	El tamaño de archivo máximo para las transferencias de archivos.	Enteros	2147483647 bytes (rango válido: 0-2147483647)
Modo de habitación de pantalla completa	Activa/desactiva el modo de pantalla completa del hub. Falso: solamente aparece el PIN en la parte superior derecha Verdadero: aparece el PIN en la parte superior derecha y un fondo de pantalla completa	Booleano	Falso
Color de fondo de modo de habitación de pantalla completa	Color de fondo utilizado en el hub. Colores HTML (hexadecimales). Ejemplos de valores válidos (valores RGB, formato #000000): Rojo: #FF0000 Amarillo: #FFFF00 Verde: #00FF00 Azul claro: #00FFFF Azul oscuro: #0000FF Negro: #000000 Blanco: #FFFFFF Gris: #808080	Cadena	Blanco (aparece en negro)
Modo de habitación de pantalla completa: Expansión de imagen de fondo	Indicador para establecer que la imagen de fondo se expanda en toda la pantalla	Booleano	Falso
Modo de habitación de pantalla	Establece el fondo del hub en la URL	Cadena	Blanco

completa: URL de fondo	o imagen (jpg/png) indicada. Establezca el valor en Verdadero si desea activar esta función. Ejemplo: http://myserver.com/background.jpg		
Modo de habitación de pantalla completa: Instrucciones	Instrucciones de texto que aparecerán en el hub. Se pueden usar {pin} y {host} como sustitutos La URL para descargas del cliente. Este elemento se muestra en pantalla en el modo de pantalla completa de la sala.	Cadena	{pin}
Modo de habitación de pantalla completa: Color de pin	Color del PIN mostrado	Cadena	Blanco (aparece en blanco)
Modo de habitación de pantalla completa: Mostrar pin	Muestra las instrucciones. Establezca el valor en Verdadero si desea activar esta función.	Booleano	Falso
Modo de habitación de pantalla completa: Color del texto	Color del texto mostrado en el hub	Cadena	Blanco (aparece en blanco)
Modo de habitación de pantalla completa: Fuente del texto	El nombre de la fuente de las instrucciones.	Cadena	Blanco
Hub: Bloqueo de teclado	Bloquea lo siguiente: Ctrl-Esc, Alt-Tab, barra de accesos, teclas de Windows y Alt-F4 en el hub. Si se establece en True, se activa el bloqueo en el hub. Se puede anular con la contraseña establecida en la máquina de la clave de registro (valor de la clave de registro)	Booleano	Falso
Hub: Mostrar reloj	Muestra un reloj en la esquina inferior derecha.	Booleano	Verdadero
Modo Moderador	Para asignar el modo Moderador en reuniones o sesiones, utilice los siguientes valores: 0 = Sin Moderación 1 = Autopromocionado 2 = Estricto	Enteros	0
Enviar dirección de correo electrónico de envío de errores	Asignar una dirección de correo electrónico a la que el hub deberá enviar los mensajes de error	Cadena	Blanco (aparece en blanco)
Puerto de escucha del servicio	Un puerto para que el hub reciba las conexiones entrantes	Enteros	0 (0 = Puerto asignado automáticamente)
Compresión de mosaico	Permite ajustar la relación de compresión para poder compartir contenido no audiovisual. El porcentaje de compresión que se debe aplicar a una parte modificada de la pantalla (panel) que se está transmitiendo a través de la red. (El valor más alto utiliza más ancho de banda)	Enteros	85 (Rango válido: 5-100)

Tamaño de mosaico	Permite ajustar el tamaño del mosaico para poder compartir contenido no audiovisual. El tamaño de mosaico en los que se puede dividir la pantalla. El tamaño de mosaico, en píxeles de cada panel.	Enteros	128 (Rango válido: 32-512)
Verificar hash del certificado de complemento	Los complementos necesitan verificación Verdadero = Verifica el hash del certificado Falso = No verifica el hash del certificado	Boolean o	Verdadero

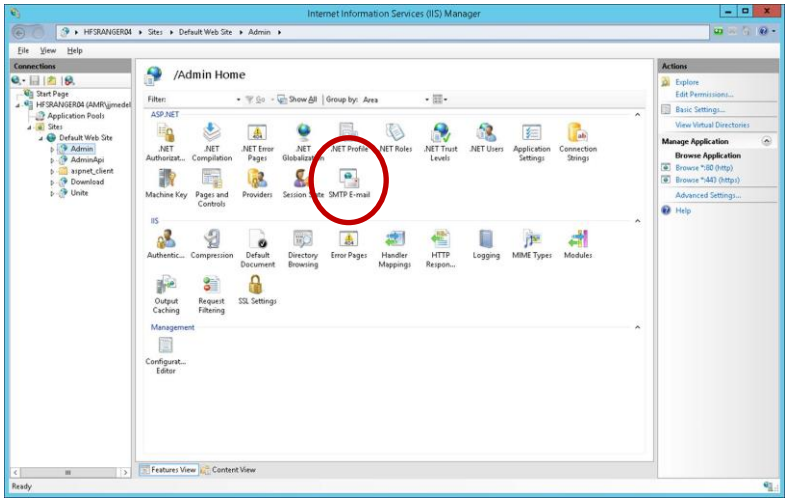
8.7.2 Intervalo de actualización de PIN

El intervalo predeterminado de actualización del PIN es de 5 minutos, es decir, el PIN que aparece en el hub cambia cada 5 minutos. Puede cambiarse en incrementos de 1 minuto de 2 a 60 minutos, modificando el archivo **web.config** en la raíz del directorio virtual del sitio del servicio web. Se puede acceder utilizando el administrador de IIS. También es posible acceder al archivo yendo al directorio Intel Unite\PinServer. Por defecto, está instalado en C:\Program Files (x86)\Intel\Intel Unite\PinServer.
Modifique el valor en la etiqueta <add key="**PinExpireTimeInMinutes**" value="5"></add> para que indique el intervalo de actualización que desee.

8.7.3 Configuración del servidor de correo electrónico

El portal de administración define el servidor SMTP en el archivo xml web.config que se crea cuando la aplicación Intel Unite está instalada en el servidor. Habrá que modificar **mailSettings** en el archivo xml web.config, en función del lugar donde esté configurado el servidor SMTP, para que el host apunte al servidor SMTP. (Por defecto, el archivo xml Web.config se encuentra en C:\Program Files (x86)\Intel\Intel Unite\PinServer).
Compruebe que el servidor de correo electrónico SMTP está configurado en IIS y que la configuración es correcta para trabajar con la aplicación en la instalación previa del Servidor empresarial.
La configuración del archivo es la siguiente:

```
<mailSettings>
    <smtp from="noreply@uniteserver.com" deliveryMethod="Network">
        <network enableSsl="false" host="smtp.myco.com" port="25"
        userName="noreply@uniteserver.com" password="pass" />
    </smtp>
</mailSettings>
```



8.7.4 Alertas y supervisión

El servidor empresarial ofrece servicios de alerta y supervisión. Se trata de un servicio que requiere darse de alta y se configura en el portal de administración.
Cualquier dispositivo que tenga las alertas configuradas será supervisado y, si no ha entrado en el umbral de advertencia, se enviará un mensaje de correo electrónico a los usuarios indicados.
Para recibir correos electrónicos sobre los dispositivos inactivos, asegúrese de que el usuario del portal de administración tiene asignado el rol **Notifications**. Para elegir que se supervise un dispositivo, añada la clave **EnableReporting** a sus metadatos y establezca el valor en **True**.
El umbral de advertencia se configura en **Administración** > **Propiedades de servidor**, y el valor predeterminado es de 60 minutos.
Recuento inactivo: si el usuario desea recibir un correo electrónico inmediatamente en la siguiente comprobación, deberá ajustarse en una cifra baja.
La dirección de correo electrónico (smtp from) y el servidor de correo electrónico (host) se deben especificar en el archivo **clocktower.exe.config**, que se encuentra en: /productfiles/release/clocktower.exe.config. (De forma predeterminada, la ubicación del archivo de configuración xml clocktower.exe es C:\Program Files (x86)\Intel\Intel Unite\ClockTower)

La configuración del archivo es la siguiente:

```
<mailSettings>
    <smtp from="noreply@uniteserver.com" deliveryMethod="Network">
        <network enableSsl="false" host="smtp.myco.com" port="25"
        userName="noreply@uniteserver.com" password="pass" />
    </smtp>
</mailSettings>
```

9 Controles de seguridad del sistema operativo y equipo

9.1.1 Estándares mínimos de seguridad (MSS)

Se recomienda que todos los dispositivos con la aplicación Intel Unite cumplan los estándares mínimos de seguridad predeterminados de su empresa, tengan un agente instalado para parches y un antivirus / IPS / IDS y otros controles necesarios según la especificación de MSS (se ha probado la compatibilidad del paquete McAfee contra malware, IPS e IDS).

9.1.2 Endurecimiento del equipo

La interfaz de firmware ampliable unificada (UEFI) de su equipo podría estar bloqueado para que solo arranque el cargador de arranque de Windows (de manera que no sea posible arrancar desde un disco USB / DVD), el bit de desactivación de ejecución podría estar activado, la tecnología de ejecución de confianza Intel® podría estar activada y los ajustes se podrían bloquear mediante contraseña.

Endurecimiento del sistema operativo Windows: como punto de partida, el sistema se ejecuta con derechos de usuario al mismo nivel. También se recomienda desinstalar del sistema operativo el software que no utilice, incluyendo el software preinstalado no necesario y componentes de Windows (PowerShell, servicios de impresión y documentos, proveedor de ubicación de Windows y servicios XPS).

Bloqueo de subsistema GUI: puesto que el sistema solo emplea una pantalla no táctil sin teclado ni ratón, resulta más difícil salir del subsistema GUI. Para impedir que un atacante conecte un dispositivo HID (ratón/teclado USB), se recomienda bloquear sistemáticamente **Alt+Tab**, **Ctrl+Shift+Esc** y la **barra de accesos**.

9.1.3 Otros controles de seguridad

Se recomienda bloquear la cuenta del usuario del equipo según la cuenta específica del equipo en Active Directory. Si la implementación consta de un número elevado de unidades, las cuentas de usuario se pueden bloquear según una planta designada o un edificio específico.

Propiedad del equipo: recomendamos que cada equipo tenga un propietario identificado. En caso de que el equipo se desconecte durante un periodo de tiempo largo, se notificará de ello a su propietario identificado.
Aparte de los mecanismos de seguridad que proporciona la plataforma Intel vPro y el propio software Intel Unite, se recomienda endurecer el sistema operativo Microsoft* Windows* según las directrices de Microsoft relativas al endurecimiento del equipo. Como referencia, consulte el administrador de cumplimiento de normas de seguridad de Microsoft* (SCM) en el siguiente enlace:
https://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx
Nota: La información que proporciona el enlace contiene una herramienta de endurecimiento mediante asistente que incluye el endurecimiento de las prácticas recomendadas y la documentación pertinente.

10 Mantenimiento

Su empresa y su administrador de TI deberán decidir un programa de mantenimiento frecuente. Se recomienda realizar las siguientes tareas de mantenimiento:

10.1 Reinicio nocturno

Se recomienda reiniciar los hubs a diario (preferiblemente por la noche). Antes de este reinicio, realice tareas de mantenimiento como las indicadas a continuación: borrar los archivos temporales en caché e iniciar el procedimiento de parches estándar.

10.2 Estrategia de parches

Si está disponible, ejecute su mecanismo de parches estándar en modo desatendido (sin mensajes de GUI) y preferiblemente antes de que se produzca el mencionado reinicio nocturno.

10.3 Informes

Recopile los indicadores de tiempo de actividad del equipo y cree un informe adaptado a las necesidades de su empresa.

10.4 Monitorización

Utilice un sistema de seguimiento de estado basado en la actividad de otros equipos y realice análisis backend de tiempo de actividad según sea necesario.

10.4.1 Monitorización backend:

Utilice herramientas de supervisión de servidor virtual estándar para generar y enviar alertas al soporte de segundo nivel.

11 Solución Intel Unite para macOS

11.1 Antecedentes

El software Intel Unite para macOS es un paquete de aplicaciones primarias y puede aprovechar los valores de las preferencias específicas de TI. De esta manera, la aplicación admite gran cantidad de instalaciones habituales, desde técnicas y software de gestión generales de Mac, hasta la instalación y configuración de preferencias de forma manual.

11.2 Flujo de trabajo de conexión general

Por defecto, la aplicación utilizará la detección automática de DNS (p. ej., registros de servicio DNS) para determinar el servidor empresarial adecuado al que conectarse. El flujo de trabajo general es el siguiente:

- Servidor empresarial según lo definido en las preferencias (opcional)
- Detección automática de los siguientes dominios:
  - _uniteservice._tcp
  - _uniteservice._tcp.yourSubDomain.yourDomain.yourTLD
    i. Ejemplo: _uniteservice._tcp.corp.acme.com
  - _uniteservice._tcp.yourDomain.yourTLD
    i. Ejemplo: _uniteservice._tcp.acme.com
  - Intento de conexión a HTTPS seguido de HTTP si no se realiza con éxito
- uniteservice.yourDomain.yourTLD

11.3 Valores de las preferencias

El equipo de TI puede modificar y personalizar la aplicación Intel Unite para que se adapte a su propia infraestructura y requisitos de seguridad. Para ello, deben configurar los ajustes siguientes en el archivo com.intel.Intel-Unite.plist que se encuentra en la capeta ~/Biblioteca/Preferencias de cada usuario:

- **Definir un servidor empresarial predeterminado**
  defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD

- **Definir una clave pública de servidor empresarial para la asignación de certificados**
  defaults write com.intel.Intel-Unite EnterpriseServerPublicKey "cadena de clave pública"

- **Forzar a un cliente a permitir únicamente certificados de servidores de confianza**
  defaults write com.intel.Intel-Unite ClientOnlyAllowsTrustedCertificates -bool true

- **Forzar a un cliente a conectarse en modo independiente**
  defaults write com.intel.Intel-Unite Standalone -bool true

Cada uno de estos ajustes se puede establecer o modificar manualmente abriendo el terminal macOS (/Aplicaciones/Utilidades) e introduciendo el comando seguido de un retorno. A continuación, podrá encontrar más información sobre cada uno de los comandos:

- **Definir un servidor empresarial predeterminado**
  Establecer un servidor empresarial predeterminado hará que el proceso de detección automática no tenga lugar. Si sus clientes Mac viven exclusivamente en su propia red, puede ser una buena opción para "asignar" la aplicación Intel Unite a su servidor empresarial por motivos de seguridad o para la solución de problemas.

- **Definir una clave pública de servidor empresarial para la asignación de certificados**
  Si desea "asignar" la aplicación cliente al servidor empresarial, puede hacerlo configurando la "Cadena de clave pública" en cada cliente, independientemente de si se está utilizando o no la detección automática. Para obtener este valor:
  - En su red corporativa, abra Safari en cualquier Mac
  - Vaya a la dirección HTTPS de su servidor empresarial
  - Haga clic en el icono de candado en la barra de direcciones
  - Haga clic en el botón **Mostrar certificado** en la hoja de certificados
  - Haga clic en el triángulo desplegable **Detalles** para expandirlo
  - Avance hacia abajo hasta que encuentre el campo **Información de clave pública** > **Clave pública**
  - Haga clic en el campo de datos, que comienza con "256 bytes:"
  - El campo de datos se ampliará
  - Seleccione todos los datos de este campo utilizando el ratón o CMD+A
  - Copie los datos al portapapeles seleccionando **Copiar** desde el menú contextual o **CMD+C**
  - En el comando de valores predeterminados, sustituya la **Cadena de clave pública** por los datos del portapapeles. Nota: Debe poner los datos entre comillas.

  Al igual que sucede al definir un servidor empresarial predeterminado, configurar esta opción dificultará a su base de usuarios la tarea de conectarse a las instalaciones de soluciones Intel Unite de otros partners/instalaciones.

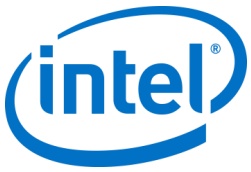
- **Forzar a un cliente a permitir únicamente certificados de servidores de confianza**
  Además de definir un servidor empresarial específico o de asignar la clave pública de certificado, también puede decirle a la aplicación Intel Unite que solo permita conexiones a servidores/certificados que estén plenamente autorizados por su cadena de confianza de certificados. Al hacerlo, debe asegurarse de que su certificado de servidor empresarial se remonte al servidor de raíz pública según lo definido por Apple en las llaves, o de que ha instalado su propio certificado de servidor raíz y cualquier certificado intermedio que se necesite en cada cliente.

- **Forzar a un cliente a conectarse en modo independiente**
  Configurar este modo cambiará el flujo de trabajo de conexión para realizar la detección automática UDP de un hub que ha generado un PIN en un entorno sin servidor empresarial. En este caso, el sistema equipado con procesador Intel Core vPro actuará como host principal y resultará útil en un entorno de pequeña y mediana empresa donde puede que no haya un departamento de TI para instalar la infraestructura del Servidor empresarial. Este modo solo funciona en sistemas que pertenezcan a la misma subred, donde los paquetes UDP no estén bloqueados.

11.4 Metodologías de distribuciones comunes

Si está utilizando la detección automática, la distribución puede ser tan fácil como arrastrar la aplicación Intel Unite a la carpeta de aplicaciones. En entornos más complejos o que requieren ajustes de seguridad adicionales, puede que le interese configurar preferencias específicas junto con la distribución de paquetes de aplicaciones. Hay muchas maneras de hacerlo y aquí le presentamos algunas de las más habituales:

- Secuencias bash
  - Puede definir la configuración de sus preferencias en una secuencia bash que se puede distribuir a los usuarios junto con el paquete de aplicaciones.
- Paquete de instalación personalizada con PackageMaker
  - Puede definir la configuración de preferencias mediante una secuencia de comandos "preflight" o "postflight".
- Instalación personalizada con Apple Remote Desktop



- Utilizando Apple Remote Desktop, puede instalar el paquete de aplicaciones Intel Unite y definir cualquier ajuste de preferencias mediante el menú **Enviar comando UNIX...**

- Instalación personalizada mediante el software de gestión de Mac para empresas
  - Puede generar una instalación push o pull personalizada utilizando las soluciones de gestión de Mac para empresas más habituales, incluidas:
    - Casper / Bushel
    - Puppet
    - Munki
    - Chef
    - Etc.

12 Solución de problemas

12.1 No se puede acceder a la página del portal de administración tras instalar la aplicación Intel Unite en el servidor

Solución/método alternativo: asegúrese de que se hayan añadido las características y los roles necesarios del servidor web al servidor.

- Agregue roles y características al servidor usando el Administrador del servidor
    - Roles del servidor: servidor web
        - Incluya las herramientas de gestión
    - Añada las características de .NET Framework 3.5
    - Añada las características de .NET Framework 4
        - ASP .NET
            - Servicios de WCF
            - Activación de HTTP
        - Roles de servidores web:
            - Servidor web, características HTTP comunes y documento predeterminado.

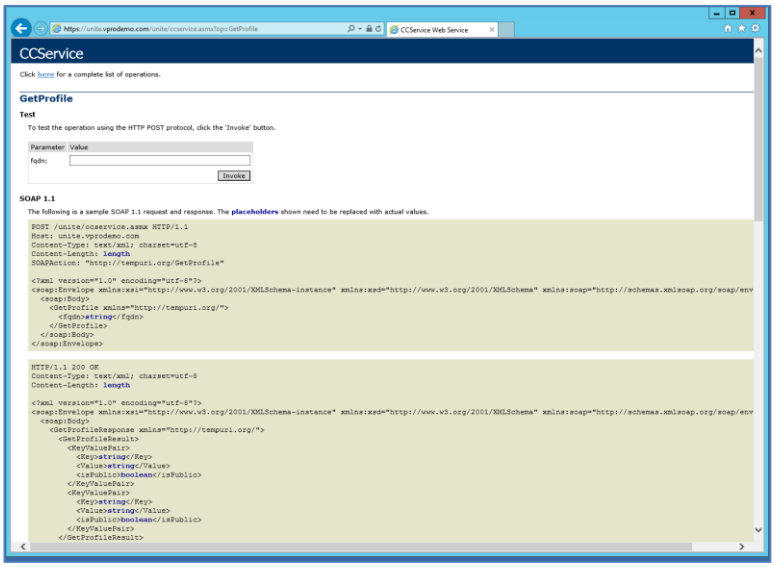
12.2 No se puede acceder al portal de administración

Si aparece una página de error al acceder al portal de administración en la que se habla de una etiqueta xml específica en Web.config, elimine la etiqueta de Web.config en el nivel superior del directorio virtual del portal (accesible desde la consola de administración de IIS).

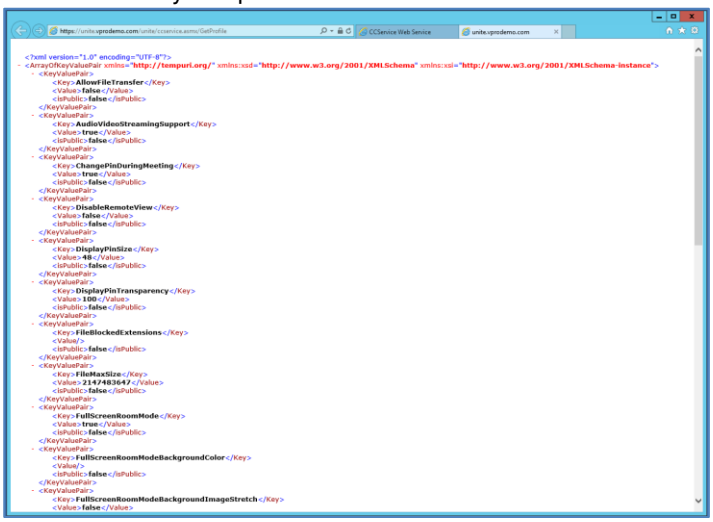
- Para comprobar que la instalación del servicio web se ha realizado correctamente, siga este enlace:

    https://<yourservername>/unite/ccservice.asmx

    - Seleccione **GetProfile** (Finalizar).
    - En el campo **Value** (Valor), introduzca **test** y pulse la opción Invoke (Invocar).



- Compruebe que puede ver el perfil predeterminado en el archivo xml como se muestra a continuación. Esto indica que el servicio de PIN puede acceder a la base de datos y recuperar datos correctamente.



12.3 Error al iniciar la aplicación del hub

Una ventana emergente indica el ID de error. La naturaleza del error se puede determinar según el ID.

12.3.1 Fallo de comprobación de la plataforma con el error ID333333

Este error indica que el hub realizó una comprobación de la plataforma, pero no se pudo validar el certificado de firma de código. Esto normalmente se debe a que el sistema operativo no cuenta con un certificado raíz actualizado, por lo que no se puede validar el certificado de firma de código público de Intel Unite.
Compruebe que el sistema está conectado a Internet, abra un explorador y vaya a https://www.microsoft.com (esto obliga al sistema a actualizar los certificados raíz).

12.3.2 Fallo de comprobación de la plataforma con el error ID666666

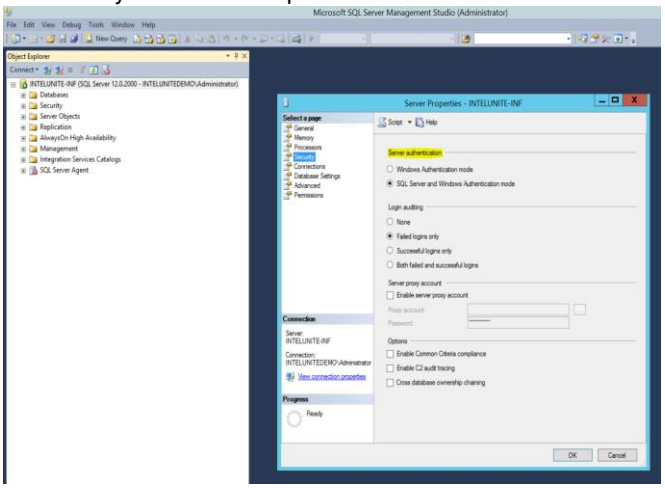
Este error indica que la plataforma no es compatible con la aplicación Intel Unite. Consulte a su proveedor OEM para asegurarse de contar con una plataforma compatible para ejecutar la aplicación.

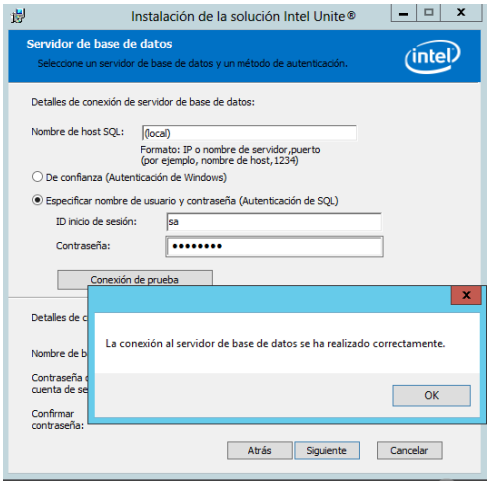
12.4 El hub no obtiene un PIN del servidor PIN - Aparecen guiones al desplazarse

Arranque la aplicación Intel Unite en el hub con un modificador Debug, es decir, navegue desde el símbolo del sistema hasta la carpeta donde está guardada la aplicación y ejecute: **IntelUnite.exe** /debug
Esto abrirá una ventana de depuración y aparecerá la información de conexión. A continuación se enumeran algunos de los errores más comunes con sus soluciones alternativas. Si aparece alguno de los errores siguientes en la información de depuración, siga la solución o método alternativo para resolverlo y obtener un PIN en el hub.

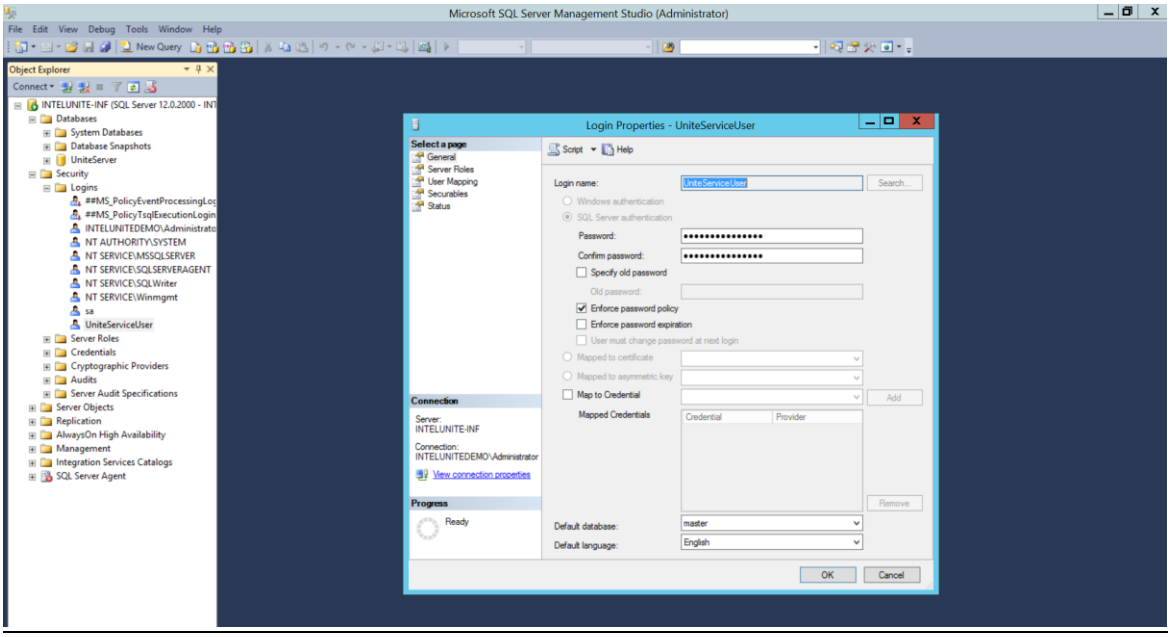
12.4.1 El servidor no puede procesar la solicitud; error de inicio de sesión del usuario "UniteServiceUser"

Este podría ser el caso si los datos de inicio de sesión de SQL no coinciden o si la contraseña de la base de datos se daña porque el usuario intenta instalar el servidor empresarial varias veces.
Solución/método alternativo:
Verifique los modos de autenticación utilizados durante la instalación de MS SQL. Para cambiar el tipo de autenticación/inicio de sesión, vaya a Microsoft SQL Management Studio y conéctese al SQL Server; haga clic con el botón derecho del ratón en SQL Server y seleccione Propiedades. Seleccione la página Seguridad y compruebe que el modo de **autenticación de Windows y SQL Server** está seleccionado cuando vaya a instalar la aplicación Intel Unite en el servidor.





Si sigue apareciendo el error, restablezca la contraseña para **UniteServiceUser**. Utilice Microsoft SQL Management Studio y conéctese al SQL Server; vaya a **Seguridad** > **Inicios de sesión** y haga clic con el botón derecho del ratón en **UniteServiceUser** para que se abra la ventana **Propiedades de inicio de sesión**. Introduzca una nueva contraseña y haga clic en **Aceptar** para guardar los cambios.



12.4.2 No aparece ningún servidor. Probando el registro de servicio DNS: _uniteservice._tcp

Solución/método alternativo:

Este podría ser el caso si el hub no puede encontrar el registro DNS. Como paso de depuración, abra la ventana de línea de comandos y ejecute el comando nslookup. Compruebe que el hub puede hacer ping al servidor en el que se está ejecutando el servicio DNS y que se ha creado un registro de servicio DNS para la solución Intel Unite. El registro de servicio debe tener los valores siguientes: **Servicio (Service)**: _uniteservice, **Protocolo (Protocol)**: _tcp, **Número de puerto (Port number)**: 443 y **Host que ofrece el servicio (Host offering this service):** FQDN del servidor empresarial.

12.4.3 No se puede establecer una relación de confianza para el canal seguro SSL/TLS con la autoridad 'uniteserverfqdn'

La versión más reciente de la solución Intel Unite solo acepta certificados SHA-2 o posteriores. Consulte a su departamento de TI para asegurarse de que el certificado de servidor web de confianza sea un certificado SHA-2 y de que la ruta de certificado sea válida.
Para realizar una comprobación del entorno, obtenga un certificado SHA-2 o desactive el cifrado de su entorno.

- Para usar Intel Unite sin cifrado, omita los siguientes pasos que proporcionan información sobre enlaces de sitios para el puerto seguro 443, continúe con la instalación de MS SQL Server y prepare el registro de servicio DNS. También debe asegurarse de que el servicio se encuentre en el puerto 80 cuando se cree un registro de servicio DNS.
- Otra manera de omitir la comprobación del certificado consiste en añadir el registro en la cuenta de la máquina del hub y del cliente.
  HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 si se debe omitir la comprobación de algoritmos del certificado, 0 si no es así. (si el valor es 0, el certificado empresarial debe ser un SHA2)]

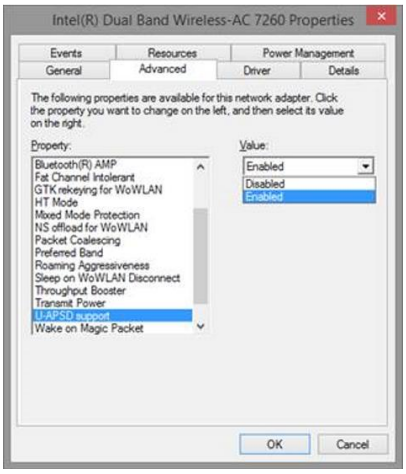
12.5 La aplicación cliente se bloquea al iniciarla o conectarla

Ejecute la aplicación del cliente con un modificador Debug y guarde la información en un archivo de registro.
(Ejecute Intel Unite.exe /debug >logfile.txt)
Si el archivo de registro muestra un mensaje de "EXCEPCIÓN: Clave no válida para utilizar en el estado especificado.", cierre la aplicación y elimine el archivo
C:\Users\eaviles\AppData\Roaming\Microsoft\Crypto\RSA\[sid]\d046df

12.6 Zona de precaución: el usuario puede experimentar tiempos de conexión más largos de lo habitual o actualizaciones de pantalla periódicas lentas.

Causa principal:

Se trata de un error que se puede dar en algunos puntos de acceso inalámbricos cuando U-APSD (modo de ahorro de energía automático no programado) está activado. Consulte
http://www.intel.es/content/www/es/es/support/network-and-i-o/wireless-networking/000005615.html.
Método alternativo: este problema se puede solucionar actualizando el firmware del punto de acceso inalámbrico. Sin embargo, en la mayoría de las empresas, esto no resulta fácil. Como último recurso puede deshabilitar U-APSD en el cliente, en las propiedades avanzadas del controlador inalámbrico.



12.7 Zona de precaución: el servidor PIN va lento

Solución/método alternativo: El servidor empresarial administra la asignación de pines y la búsqueda de pines para conectarse a habitaciones. Como medida de seguridad, la frecuencia con la que un usuario puede solicitar pines y consultar pines de la base de datos está limitada por un algoritmo de tiempo de espera exponencial. Este mecanismo de tiempo de espera efectúa un seguimiento en función de la dirección IP del usuario y el número de intentos.

Los servidores de producción pueden utilizar equilibradores de carga para ayudar a gestionar la carga y mantener la redundancia en el entorno. Los equilibradores de carga redirigen el tráfico a los servidores web apropiados. De esta manera, puede parecer que el servidor web está recibiendo todas las solicitudes de la misma dirección IP, con lo que se desencadenan los algoritmos de tiempo de espera.

La base de datos contiene un procedimiento almacenado (*spGetPinBackoffTime*), que devuelve el retraso calculado en segundos al servidor web. Esta funcionalidad se ha desactivado, por lo que el procedimiento almacenado siempre devuelve el valor 0. Esto desactiva el algoritmo de tiempo de espera de seguridad.

12.8 Solución de problemas de clientes Mac

Inicie la aplicación Intel Unite (/Aplicaciones/Utilidades) desde el terminal para ver los mensajes de depuración.
/pathToUnite/Intel\ Unite.app/Contents/MacOS/Intel\ Unite
La aplicación se iniciará y aparecerá toda la información de depuración en el terminal.

12.8.1 Error de conexión al servidor empresarial -1003: no se ha podido encontrar un servidor con el nombre de host especificado.

Solución/método alternativo: Compruebe que el dominio de búsqueda DNS está correctamente definido. Si un usuario define un servidor DNS, pero no especifica ningún dominio de búsqueda, no habrá ningún sufijo de dominio DNS en el que realizar la búsqueda cuando el equipo MAC intente hacer una detección automática. Si no hay ningún dominio de búsqueda DNS definido, la aplicación Intel Unite no puede agregarlos a la detección automática ni a la entrada "estática" de *uniteservice*. Así pues, salvo que la detección automática funcione en *_uniteservice._tcp*, el cliente no podrá encontrar el servidor empresarial. La solución más sencilla consiste simplemente en agregar un dominio de búsqueda DNS (que debe coincidir con el registro de servicio DNS), pero también se podría optar por definir el servidor empresarial en la configuración de los archivos *plist*.

Utilice el comando del terminal:
defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD

12.8.2 Error de conexión al servidor empresarial -1001: tiempo de espera agotado para esta solicitud

Solución/método alternativo: Este error podría deberse a uno de los dos motivos siguientes.

1. Hay un posible problema con el servicio web en el Servidor empresarial.
2. El equipo MAC no se puede conectar al servidor por problemas de red.

Lo primero que se debe hacer para intentar solucionar el problema es buscar el servicio web en el registro de depuración. Busque https://yourserver/Unite/CCService.asmx.
Copie y pegue esta URL en Safari y confirme que el equipo MAC puede acceder al servicio web. De esta forma podrá ver si hay un problema de red que impida la conexión al servidor y si el servicio web del servidor empresarial está funcionando.

12.8.3 Error de conexión del servidor empresarial 1200: se ha producido un error de SSDL y no se puede establecer una conexión segura al servidor.

Póngase en contacto con su departamento de TI para obtener los certificados SHA-2 válidos para la solución Intel Unite.

12.9 La aplicación Intel Unite para Mac OS se elimina/desinstala del dispositivo cliente y se instala una versión alternativa o más reciente de la aplicación Intel Unite. No obstante, se conservan las propiedades de instalación anteriores.

La aplicación Intel Unite para dispositivos de clientes Mac sigue las convenciones generales de OS X, por lo tanto, la configuración del usuario no se borra cuando se elimina la aplicación.

Solución/método alternativo:
Desinstale la aplicación Intel Unite del dispositivo cliente. Hay dos formas de eliminar estos ajustes y volver a un estado limpio.

1. Acceda al terminal (/Aplicaciones/Utilidades) e introduzca el siguiente comando:

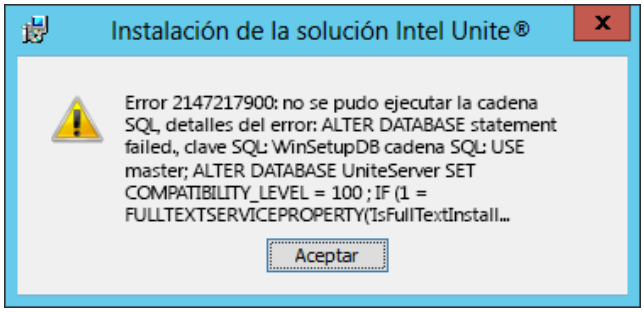
   defaults delete com.intel.Intel-Unite

2. En Finder, borre el archivo de ~/Biblioteca/Preferencias/com.intel.Intel-Unite.plist.

   Vuelva a iniciar el sistema. Actualmente, los archivos plist suelen tener una gran cantidad de caché en los sistema operativo, por lo tanto, no se pueden eliminar y conseguir que el sistema operativo detecte el cambio, normalmente.

12.10 Error 2147217900: error al ejecutar la cadena SQL.

Este error se genera cuando se ejecuta el instalador de servidor Intel Unite y la base de datos Unite ya existe, pero el nombre del servidor está en blanco.



Solución/método alternativo:
El instalador genera un error si ya existe la base de datos en el clúster. Para resolver este error, elimine la base de datos, asegúrese de que tiene derechos de DBAdmin y vuelva a ejecutar el instalador.

12.11 Mensaje de error: "Error de la base de datos"

Si un administrador de TI elige la opción "Enviar token" desde la consola de administración y le aparece el mensaje de error "Error de la base de datos", es probable que la configuración del servidor SMTP sea errónea. Deberá comprobar la configuración del servidor de correo electrónico SMTP.

12.12 El portal web de administración no se muestra correctamente (faltan componentes)

El portal web de la administración no se muestra por completo, faltan componentes como cuadros de texto, opciones o iconos después de actualizar el software Intel Unite. Esto se debe a los tipos MIME bloqueados por la opción de filtrado de solicitudes en IIS.

Solución/método alternativo:

1. Abra el administrador de IIS.
2. Muestre las propiedades del servidor IIS.
3. Haga clic en **Tipos MIME** y, a continuación, agregue la extensión JSON:
    - Extensión de nombre de archivo: .json.
    - Tipo MIME: application/json.
4. Vuelva a las propiedades del servidor ISS.
5. Haga clic en **Asignaciones de controlador**.
    - Añada una asignación de script
    - Ruta de solicitud: *.json
    - Ejecutable: C:\WINDOWS\system32\inetsrv\asp.dll
    - Nombre: JSON
6. En el panel **Conexiones**, vaya a la conexión, sitio, aplicación o directorio para el que desee modificar la configuración de filtrado de solicitud.
7. En el panel **Inicio**, haga doble clic en **Filtrado de solicitud**.
8. Busque la opción para permitir la extensión de nombre de archivo
9. Agregue estas 4 extensiones:
    - .json
    - .less
    - .woff
    - .woff2

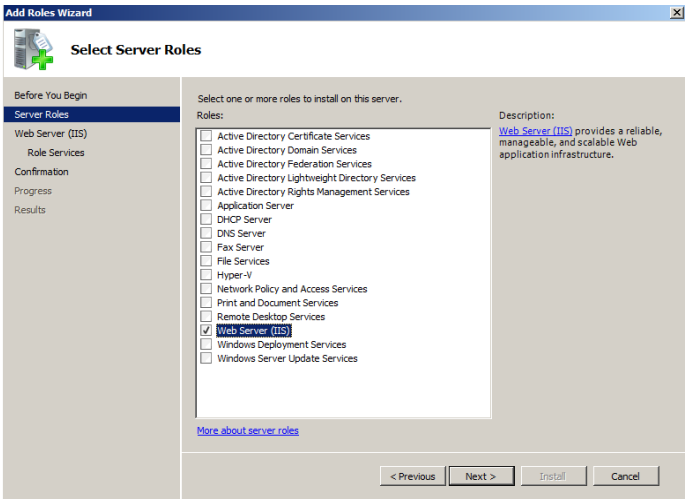
Apéndice A. Preparación del servidor empresarial

Activando IIS

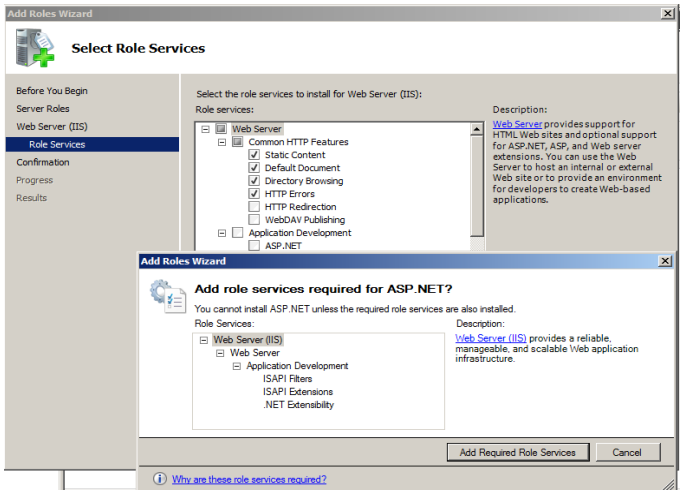
Para Windows 2008:

En Windows Server 2008, tendrá que descargar la actualización de .NET Framework 4.5 (https://www.microsoft.com/en-us/download/details.aspx?id=40779)

- Haga clic en **Start (Inicio)**, elija **Administrative Tools (Herramientas administrativas**) y, a continuación, haga clic en **Server Manager (Administrador del servidor**).
- En **Roles Summary (Resumen de roles)**, haga clic en **Add Roles (Agregar roles)**.
- Utilice el **Add Roles Wizard (Asistente para agregar roles)** para añadir el rol de **Web Server (Servidor web) (IIS)** (marque la casilla).



- Haga clic en **Next (Siguiente)** hasta que llegue a la ventana **Select Role Services (Seleccionar servicios de rol**).
- En la sección **Application Development (Desarrollo de aplicaciones)**, compruebe que ASP.NET está marcado y, de no ser así, selecciónelo. Tenga en cuenta que, de forma predeterminada, ASP.NET no está seleccionado. Haga clic en **Add Required Role Services (Agregar servicios de rol requeridos)** para ASP.NET. También necesita ASP.NET 4.5.



- Una vez haya creado el rol, en el menú **Roles**, vaya a **Web Server (Servidor web) (IIS)**, en el lado derecho del panel, acceda al **Internet Information Services (IIS) Manager (Administrador de Internet Information Services) (IIS)** y seleccione su servidor en el panel izquierdo de **Conections (Conexiones)**.

  Referencia: enlace a la biblioteca de Windows Server Instalar IIS en Windows Server 2008.

  Nota: La versión más reciente de la solución Intel Unite solo acepta certificados SHA-2 o posteriores. Consulte a su departamento de TI para asegurarse de que el certificado de servidor web de confianza sea un certificado SHA-2 y de que la ruta de certificado sea válida.

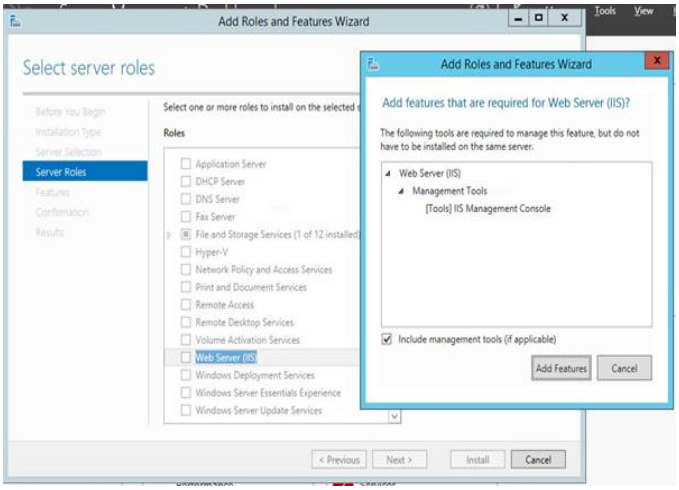
  Para realizar una prueba del entorno, póngase en contacto con su equipo de certificación autorizado para obtener un certificado SHA-2 o desactivar el cifrado.
  - Para usar Intel Unite sin cifrado, omita los siguientes pasos que proporcionan información sobre enlaces de sitios para el puerto seguro 443, continúe con la instalación de MS SQL Server y prepare el registro de servicio DNS. También debe asegurarse de que el servicio se encuentre en el puerto 80 cuando se cree un registro de servicio DNS.
  - Otra manera de omitir la comprobación del certificado consiste en añadir la clave de registro en la cuenta de la máquina del hub y del cliente. HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 si se debe omitir la comprobación de algoritmos del certificado, 0 si no es así. (si el valor es 0, el certificado empresarial debe ser un SHA2)]

- Para asignar el certificado, vaya al panel izquierdo de **conexiones**, amplíe los sitios y haga clic en la opción **Sitio web predeterminado**.
- En el panel de la derecha **Actions (Acciones)**, seleccione **Bindings (Enlaces)** (debajo de Editar sitio).
- En la ventana **Site Bindings (Enlaces de sitios)**, haga clic en **Add (Agregar)**.
- Utilice la siguiente información:
  - Tipo: https (no http)
  - Dirección IP: todas sin asignar
  - Puerto: 443
  - Nombre de host: (déjelo en blanco).
  - Certificado SSL: use el certificado SSL que se instaló en los pasos anteriores.
  - Haga clic en **OK (Aceptar)**.

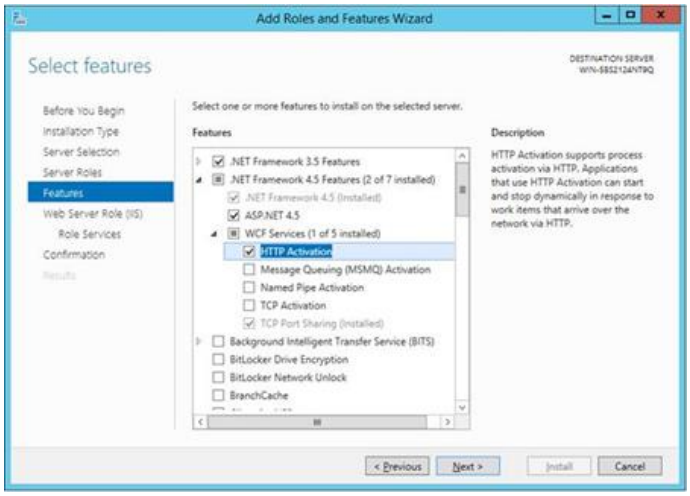
Windows 2012:

- Abra el **Administrador del servidor**.
- En el menú **Manage (Administrar)**, seleccione **Add Roles and Features (Agregar roles y características)**.
- Seleccione **Role-based or Feature-based Installation (Instalación basada en roles o basada en características).**
- Seleccione el servidor pertinente ("local" está seleccionado de forma predeterminada).
- Seleccione **Web Server (Servidor web) (IIS)** y **Add Features (Agregar características)** para añadir las características que se necesitan para el servidor web (IIS) y haga clic en **Next (Siguiente)**.

NOTA: Si necesita información adicional para solicitar un Certificado de Servidor de Internet en el Servidor de Unite, acceda al siguiente enlace web de Microsoft https://technet.microsoft.com/en-us/library/cc732906.aspx y siga los pasos indicados por el proveedor de certificados SSL para obtener un certificado firmado.

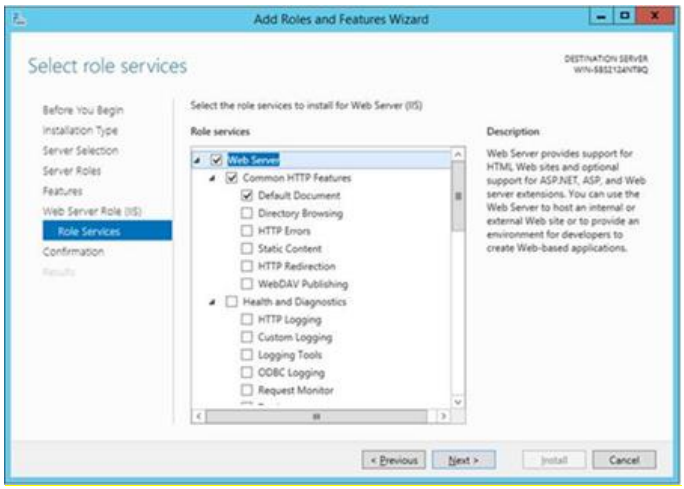


- En Características, añada las siguientes características de IIS (puesto que no son opciones predeterminadas):
  - Características de .NET Framework 3.5
  - ASP.NET 4.5
  - Servicios de WCF
  - Activación HTTP (añada las funciones necesarias para la activación HTTP cuando se le solicite) y haga clic en **Next (Siguiente)**.



Note (Nota): .NET 3.5 podría dar un error durante el proceso de instalación. Especifique una ruta de acceso de origen alternativa si el equipo de destino no tiene acceso a Windows Update. Haga clic en el enlace **Specify an alternate source path (Especifique una ruta de acceso de origen alternativa)** para especificar una ruta para acceder a la carpeta **\sources\sxs** en el medio de instalación.
Referencia: https://technet.microsoft.com/en-us/library/dn482071.aspx

- En la página Servicios de rol, agregue **Rol de servidor web (IIS)** como rol a su servidor o acepte el valor predeterminado.
- Seleccione los siguientes servicios de rol para instalar en el servidor web:
    - Características HTTP comunes
    - Documento predeterminado



- Haga clic en **Next (Siguiente)** para continuar y en **Intall (Instalar)**, en la ventana siguiente, para instalar las características y los roles seleccionados.
- Una vez haya creado el rol, en el menú **Roles**, vaya a **Rol de servidor web (IIS)**, en el lado derecho del panel, acceda al **Administrador de Internet Information Services (IIS)** y seleccione su servidor en el panel izquierdo de **Conexiones**.

Nota: La versión más reciente de la solución Intel Unite solo acepta certificados SHA-2 o posteriores. Consulte a su departamento de TI para asegurarse de que el certificado de servidor web de confianza sea un certificado SHA-2 y de que la ruta de certificado sea válida.

Para realizar una prueba del entorno, desactive el cifrado o cree un certificado SHA 2 autofirmado.

- Para usar Intel Unite sin cifrado, omita los siguientes pasos que proporcionan información sobre enlaces de sitios para el puerto seguro 443, continúe con la instalación de MS SQL Server y prepare el registro de servicio DNS. También debe asegurarse de que el servicio se encuentre en el puerto 80 cuando se cree un registro de servicio DNS.
- Ejecute el siguiente comando de PowerShell como administrador.
  - New-SelfSignedCertificate –dnsname "su_nombre_de_servidor" –CertStoreLocation cert:\LocalMachine\My ; donde "su_nombre_de_servidor" es el FQDN del servidor empresarial.
- Otra manera de omitir la comprobación del certificado consiste en añadir la clave de registro en la cuenta de la máquina del hub y del cliente. HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 si se debe omitir la comprobación de algoritmos del certificado, 0 si no es así. (si el valor es 0, el certificado empresarial debe ser un SHA2)]

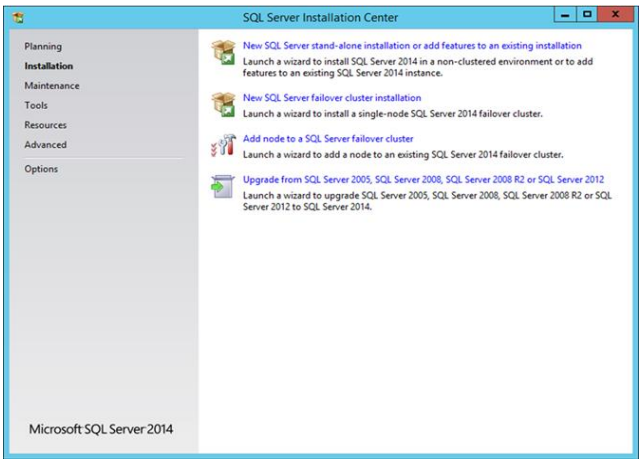
- Para asignar el certificado, vaya al panel izquierdo de **conexiones**, amplíe los sitios y haga clic en la opción **Sitio web predeterminado**.
- En el panel de la derecha **Actions (Acciones)**, seleccione **Bindings (Enlaces)** (debajo de Editar sitio).
- En la ventana **Site Bindings (Enlaces de sitios)**, haga clic en **Add (Agregar)**.
- Utilice la siguiente información:
  - Tipo: https (no http)
  - Dirección IP: todas sin asignar
  - Puerto: 443
  - Nombre de host: (déjelo en blanco).
  - Certificado SSL: elija el que haya instalado en los pasos anteriores.
  - Haga clic en **OK (Aceptar**).
- Seleccione **Close (Cerrar)**.

Referencia: enlace a la biblioteca de Windows Server Instalar IIS en Windows Server 2012.
Nota sobre el puerto 443: El servicio web de la aplicación Intel Unite se comunica con los clientes y los hubs a través del puerto 443, por lo que es importante comprobar que este puerto está activado tal y como se indica más arriba.

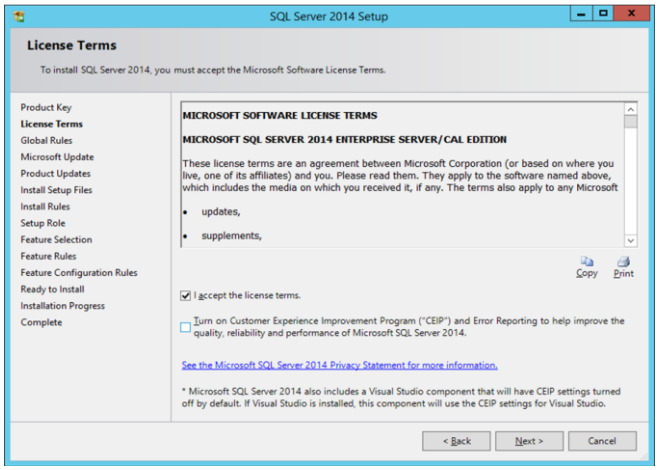
Instalación de Microsoft SQL Server

Para poder ejecutar el Servidor empresarial, se necesita MS SQL, como mínimo, necesita la versión 2008 R2 o posterior. Puede instalar un nuevo SQL Server específico si desea ejecutar un "entorno de prueba" y familiarizarse con la aplicación, aunque no es obligatorio. La aplicación Intel Unite creará su propia base de datos, tablas de datos e índices en la base de datos existente sin interferir con las demás tablas o datos existentes.
Consulte a continuación cómo se instala MS SQL 2014

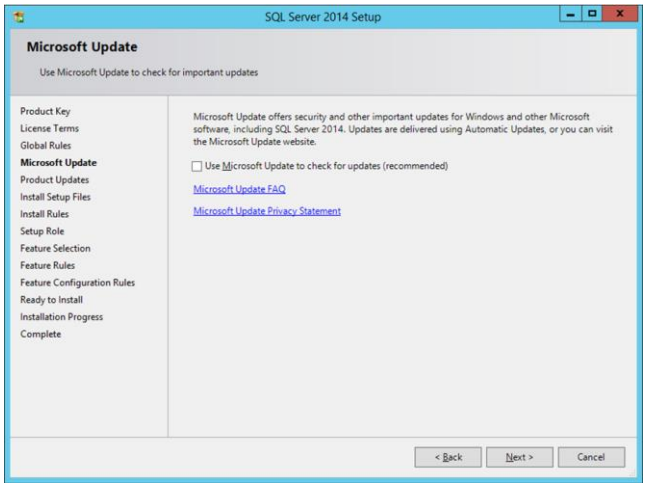
- Ejecute el programa de instalación de SQL Server y abra el Centro de instalación de SQL Server. Haga clic en **Instalación** en el panel izquierdo y seleccione **Nueva instalación independiente de SQL Server o agregar características a una instalación existente (New SQL Server stand-alone installation or add features to an existing installation)**



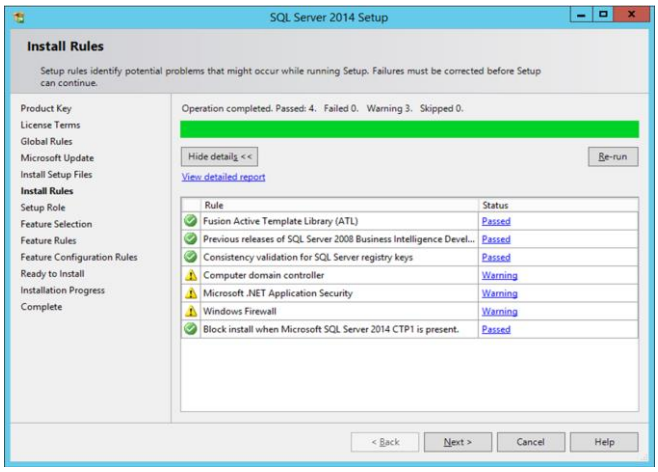
- Introduzca la clave del producto, acepte los términos de licencia y haga clic en **Next (Siguiente)**.



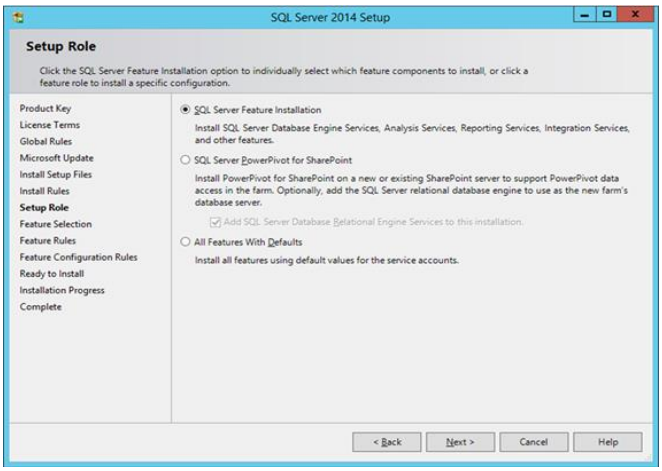
- Seleccione **Use Microsoft Update to check for updates (recommended) (Usar Microsoft Update para buscar actualizaciones) (opción recomendada)** para comprobar si hay actualizaciones y haga clic en **Next (Siguiente)**. En la siguiente ventana, el programa de instalación buscará actualizaciones del producto e instalará las actualizaciones pertinentes. Para continuar, haga clic en **Next (Siguiente)**.



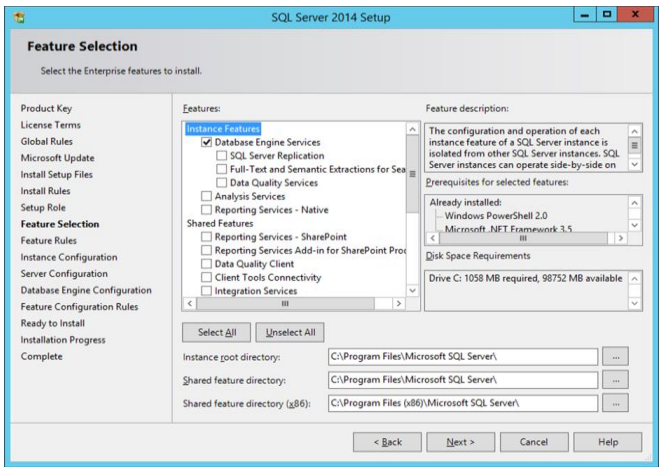
- El programa de instalación de SQL busca posibles fallos y comprueba qué requisitos se deben cumplir antes de proceder con la instalación. Haga clic en **Next (Siguiente)** para continuar.



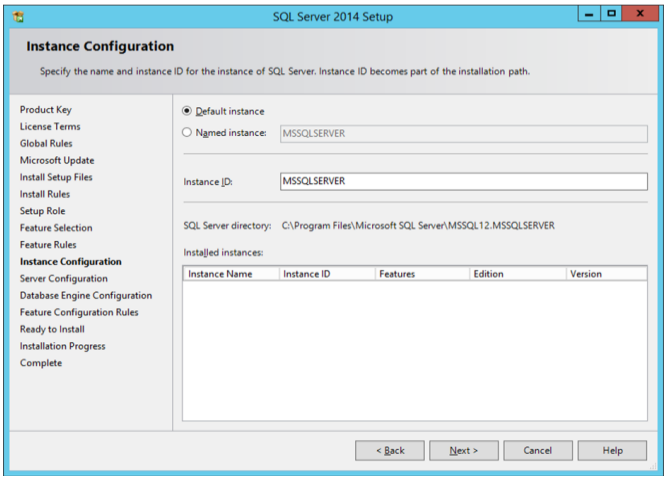
- Seleccione **SQL Server Feature Installation (Instalación de características de SQL Server)** y haga clic en **Next (Siguiente)**.



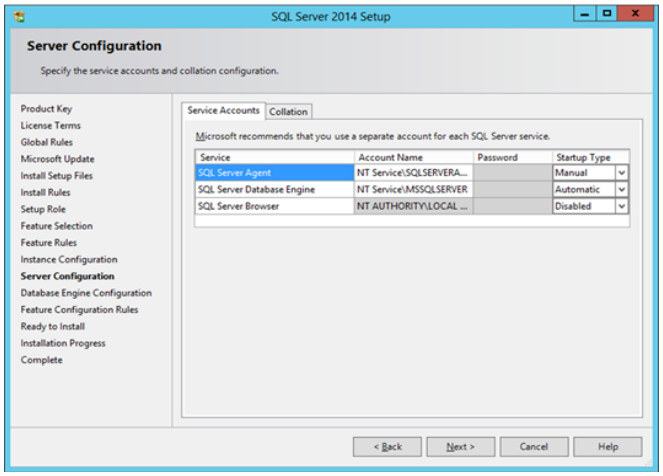
- En la **Selección de características (Feature Selection)**, elija **Servicios de motor de base de datos (Database Engine Services)**, **Herramientas de administración- Completa (Management tools-Complete)** y haga clic en **Next (Siguiente)**.



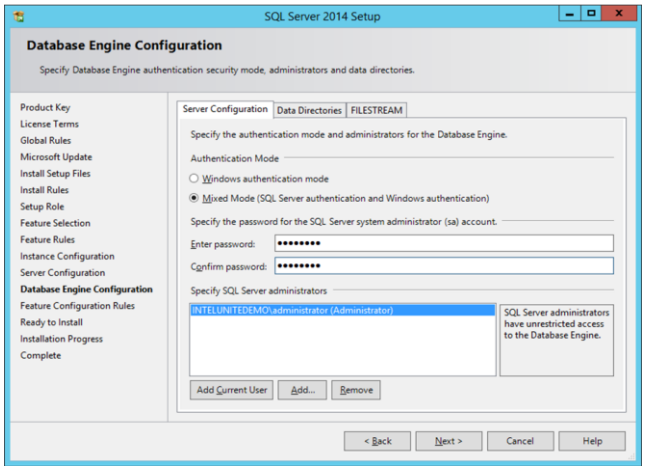
- Especifique el nombre y el identificador de instancia de SQL Server y haga clic en **Next (Siguiente)**.



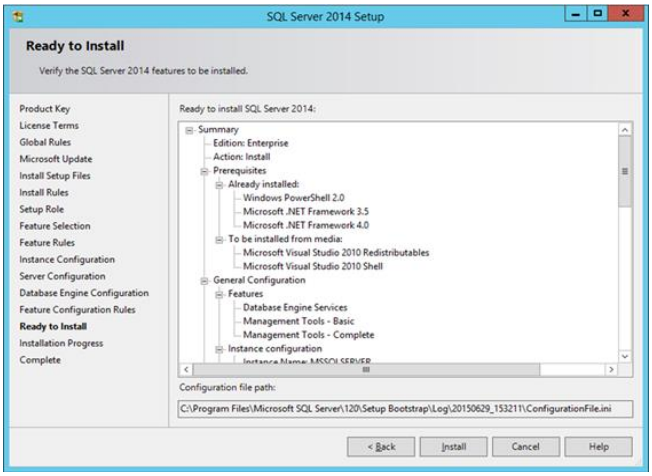
- Especifique las cuentas de servicio de cada servicio y haga clic en **Next (Siguiente)** para continuar.



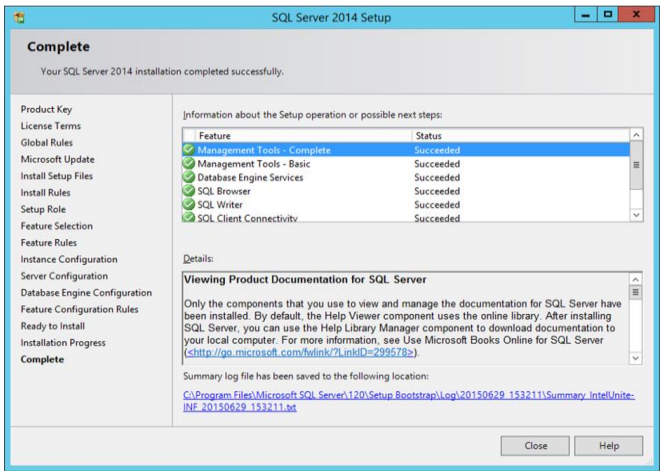
- Seleccione Autenticación de modo mixto (que incluye la autenticación de SQL Server y de Windows), especifique los administradores de SQL Server y haga clic en **Next (Siguiente)**.



- Compruebe las características que se van a instalar y haga clic en **Install (Instalar)**.



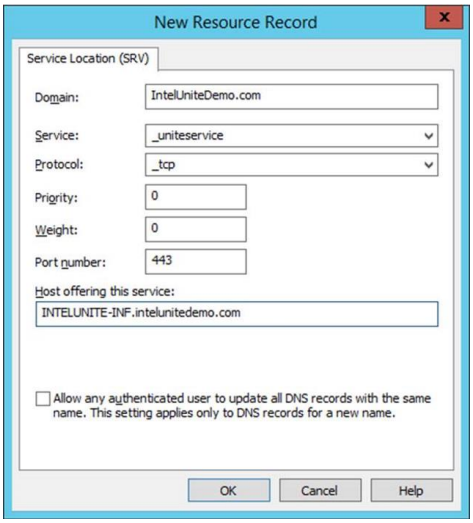
- **Cierre** el cuadro de diálogo una vez terminada la instalación.



Creación de un registro de servicio DNS

El hub o los clientes localizarán el servidor empresarial usando el servicio DNS durante una búsqueda automática del servidor empresarial. También puede utilizar la búsqueda manual, pero es altamente recomendable usar DNS. Si tiene pensado asignar el nombre de host del servidor empresarial de forma manual durante la instalación del hub y del cliente, puede ignorar esta sección.
Si se utiliza un registro de servicio DNS, el hub o el cliente buscará el servicio denominado _uniteservice._tcp en los registros de servicio DNS _uniteservice._tcp.example.com 86400 IN 0 5 443 uniteserver.example.com.
Para agregar un registro de servicio DNS en Microsoft Windows:

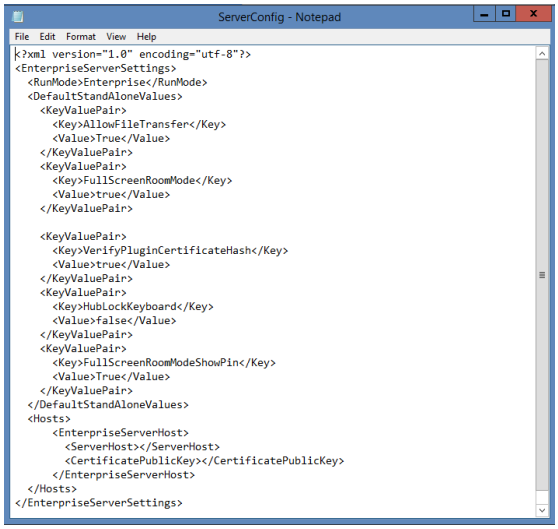
- Abra el Administrador de DNS en su servidor DNS.
- Expanda las zonas de búsqueda directa (panel izquierdo).
- Haga clic con el botón derecho del ratón en la zona y seleccione la opción "Otros registros nuevos...".
    - En **Select a resource record type (Seleccione el tipo de registro del recurso):** elija **Service Location (Ubicación de servicio) (SRV)** y después **Create Record (Crear registro)**.
    - En el campo **Service (Servicio)**, introduzca: _uniteservice
    - En el campo **Protocol (Protocolo)**, introduzca: _tcp
    - En el campo **Port (Puerto)**, introduzca: 443
    - Para el host que ofrece el servicio: escriba el nombre de host o IP de los servidores empresariales.



NOTA: Acceda al siguiente enlace de Microsoft para obtener más información sobre cómo configurar un servidor DNS para poder utilizar reenviadores: https://technet.microsoft.com/en-us/library/cc754941.aspx

Apéndice B. Ejemplo de archivo ServerConfig.xml

El archivo ServerConfig.xml se crea al instalarse los componentes del hub y del cliente del software Intel Unite. La ubicación predeterminada del archivo xml es C:\Archivos de programa (x86)\Intel\Intel Unite\Hub o C:\Archivos de programa (x86)\Intel\Intel Unite\Cliente, para el hub y el cliente respectivamente.
Este archivo se modifica si se elige **Especificar servidor** y se introduce el nombre de host del servidor o si se introduce la **Clave pública** de forma manual al instalar el software Intel Unite en el hub o el cliente.
Si desea modificar el archivo serverconfig.xml tras la instalación, vaya a la carpeta donde está el archivo y realice los cambios correspondientes.



Si hay un servidor definido en ServerConfig.xml, tendrá prioridad sobre el registro de servicio DNS.

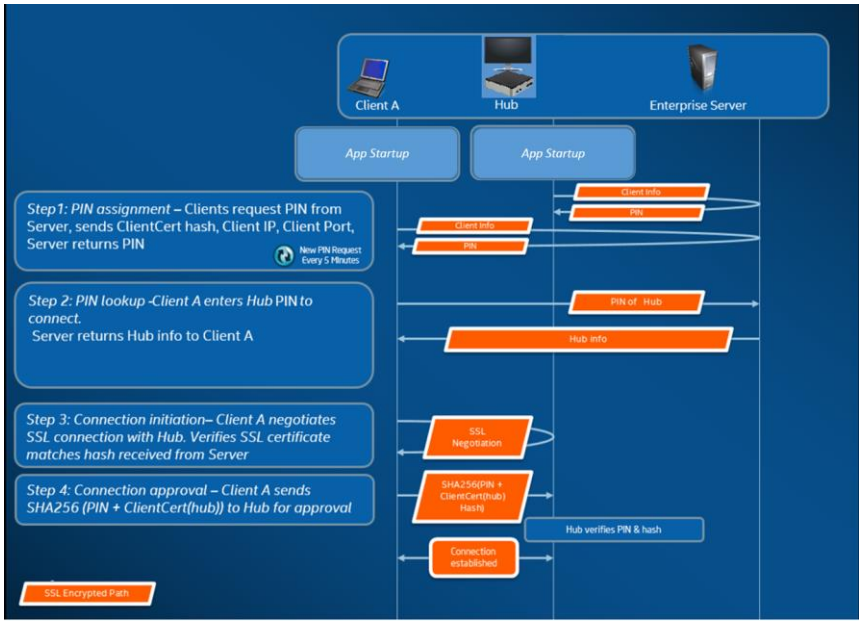
Apéndice C. Solución Intel Unite: descripción de la seguridad

Software Intel Unite - Flujo de seguridad

En esta sección se ofrece una breve descripción de los aspectos relativos a la seguridad de la aplicación Intel Unite. Se exponen con relación a los cuatro pasos siguientes:

1. Asignación de PIN
2. Búsqueda de PIN
3. Inicio de la conexión
4. Aprobación de la conexión

La siguiente imagen contiene una vista general de alto nivel del modo en que las aplicaciones del cliente (con tecnología Intel vPro) y del hub reciben códigos PIN de forma segura del servidor empresarial, los asignan y establecen una conexión.



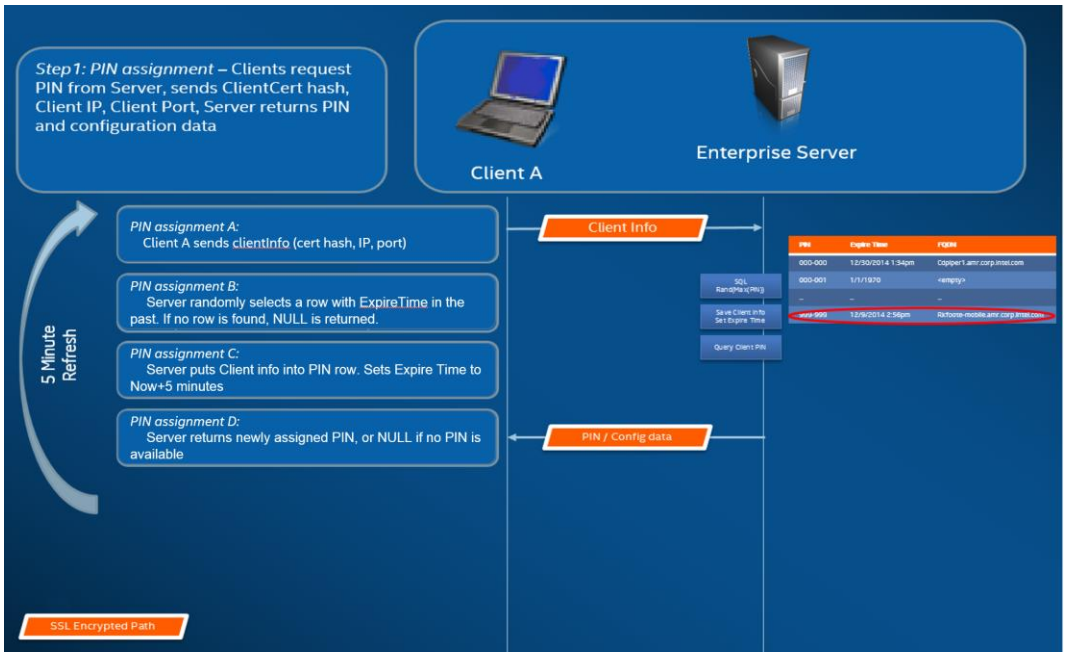
Paso 1: asignación de PIN

La imagen de abajo describe cómo se asignan los PIN. Todas las comunicaciones de red durante este proceso se cifran con SSL a través de un servicio web (TCP 443).
Además de recibir códigos PIN, el hub y el cliente también registran su información de conexión y una clave pública en el servidor. La clave pública se utiliza durante la conexión para validar que cada componente está estableciendo comunicación con el destino deseado.

Nota: La asignación de PIN para el cliente (con tecnología Intel vPro) y el hub siguen el mismo proceso.

Tenga también en cuenta lo siguiente:

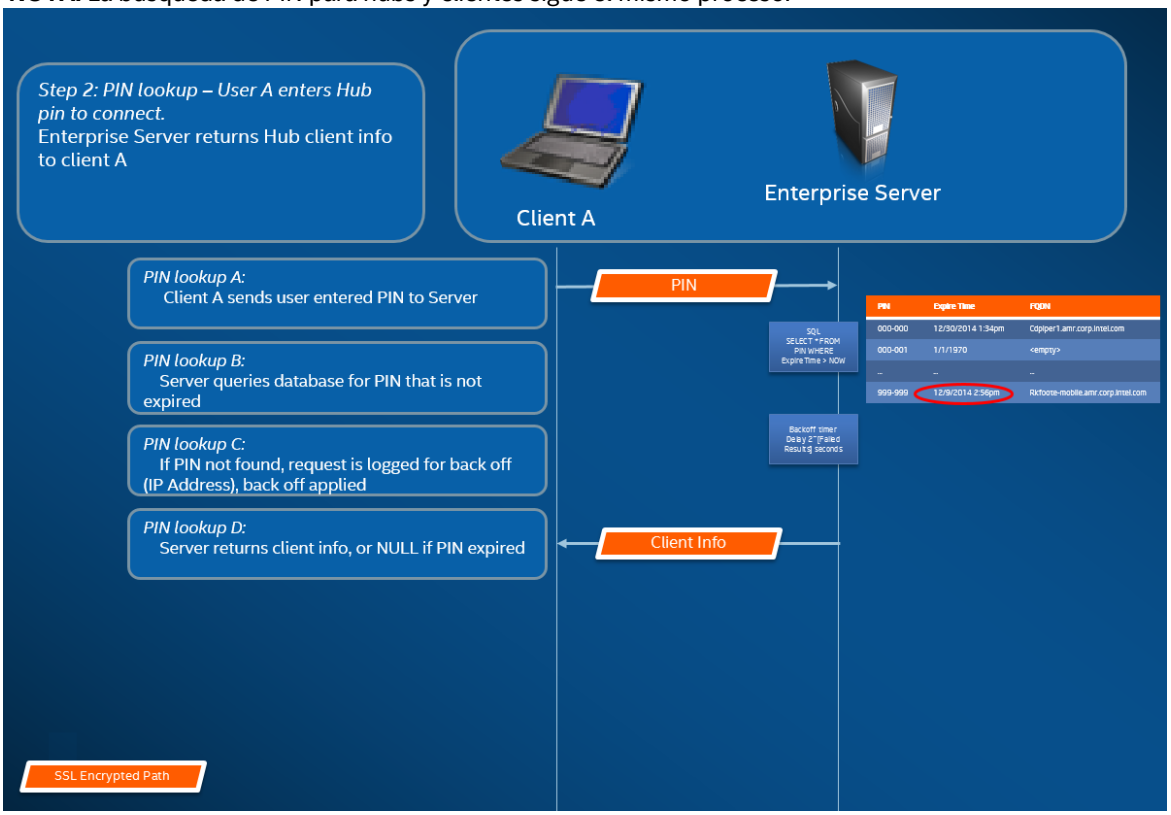
- El intervalo de actualización del PIN se puede configurar.
- Cuando el hub o el cliente envían información de conexión, se ignoran las direcciones IP del host local (127.0.0.0/8) y los intervalos 169.254.0.0/16.
- El puerto TCP se puede configurar por cliente o hub, o a través de un perfil desde el portal de administración. El comportamiento predeterminado es permitir que el sistema operativo asigne un puerto.
- Los códigos PIN caducados podrán acceder durante un máximo de 15 segundos.
- Los PIN caducados no se volverán a asignar hasta pasados 5 minutos desde su caducidad para garantizar que los usuarios no se conectan por error a una pantalla equivocada.



Paso 2: búsqueda de PIN

La imagen que aparece a continuación describe cómo resuelve los PIN el servidor empresarial. Todas las comunicaciones de red durante los procesos de búsqueda de PIN se cifran con SSL a través de un servicio web (TCP 443).
Cuando un usuario introduce un PIN del destino en el cliente, este envía el PIN al servidor empresarial para obtener la información de conexión. Si la búsqueda se completa correctamente, el servidor empresarial devuelve la información de conexión válida al destino. El destino puede ser un hub o un cliente (con tecnología Intel vPro) que ejecute el software Intel Unite.
Además de recibir información de conexión, también se facilita la clave pública del destino para que la aplicación cliente pueda validar que se está comunicando con el destino correcto.

NOTA: La búsqueda de PIN para hubs y clientes sigue el mismo proceso.

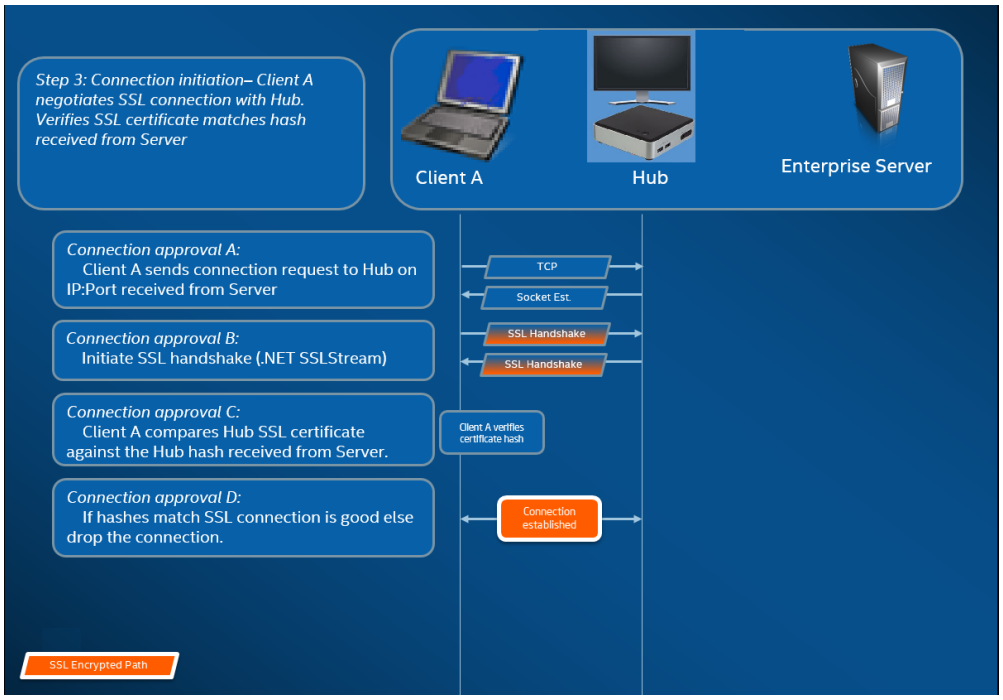


Protección de búsqueda de PIN

Para evitar que los atacantes intenten obtener códigos PIN del servidor empresarial, se registran los intentos fallidos. Los usuarios pueden tener hasta 3 intentos fallidos en un periodo de 10 segundos antes de que el mecanismo de protección empiece a aplicar un retardo en las respuestas (2^x segundos, donde x=número de intentos fallidos en un periodo de 5 minutos).

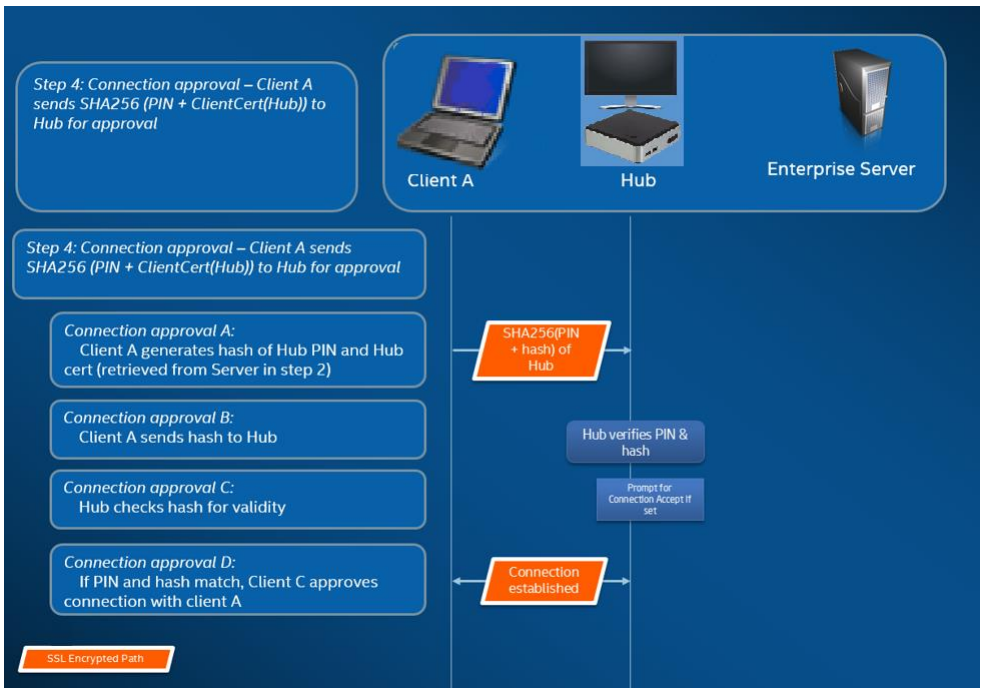
Paso 3: establecimiento de la conexión

La imagen de abajo describe cómo se establece la conexión. El cliente establece una conexión TCP par a par con el destino (un hub o un cliente con tecnología Intel vPro que se ejecuta en el software Intel Unite) e inicia el protocolo de enlace SSL. El certificado que proporciona el destino pasa por el proceso de hash y se compara con el hash del cliente que se recibe en el paso 2. Este tipo de validación evita los ataques y también las situaciones en las que las direcciones IP de los clientes DHCP pueden cambiar.



Paso 4: aprobación de la conexión

La imagen que aparece a continuación muestra cómo se establece la conexión entre el cliente y el objetivo, que podría ser un hub o un cliente (con tecnología Intel vPro) que se ejecuta en el software Intel Unite. Una vez que el objetivo verifica el PIN y el certificado de cliente, acepta la conexión y se establece una conexión entre el cliente y el objetivo.



Apéndice D. Solución Intel Unite: equilibrador de carga

En esta sección se describe brevemente el método para evitar el tiempo de espera del PIN del equilibrador de carga/proxy.
Si el valor está por debajo del equilibrador de carga, asegúrese de que el procedimiento SQL almacenado (dbo.spGetPinBackoffTime) **siempre devuelve un valor igual a 0.**
Pasos:

- Alterne el procedimiento almacenado dbo.spGetPinBackoffTime. Puede omitir todo y utilizar únicamente "seleccionar 0" al final.
- Ejecute el script.

Si el valor no está por debajo del equilibrador de carga, asegúrese de que el procedimiento almacenado está configurado con los valores predeterminados.