Guía del administrador de HP ThinPro 7.2

RESUMEN

Esta guía es para administradores de thin clients HP basados en el sistema operativo HP ThinPro.

Información legal

AMD y ATI son marcas comerciales de Advanced Micro Devices, Inc. Citrix y XenDesktop son marcas comerciales registradas de Citrix Systems, Inc. y/o una o más de sus subsidiarias, y es posible que estén registradas en la Oficina de Patentes y Marcas Registradas de los Estados Unidos y en otros países. Linux es una marca comercial registrada de Linus Torvalds en los Estados Unidos y en otros países. Microsoft, Windows, Windows Vista y Windows Server son marcas comerciales o marcas registradas de Microsoft Corporation en los Estados Unidos y/o en otros países. NVIDIA es una marca comercial registrada de NVIDIA Corporation en los EE. UU. y en otros países. UNIX es una marca comercial registrada de The Open Group. VMware, Horizon y View son marcas comerciales o marcas comerciales registradas de VMware, Inc. en Estados Unidos y/o en otras jurisdicciones.

Software confidencial para equipos. Se necesita una licencia válida de HP para su propiedad, uso o copia. Según lo dispuesto en las disposiciones FAR 12.211 y 12.212, el software informático comercial, la documentación de software informático y los datos técnicos para elementos comerciales se otorgan según la licencia comercial estándar del fabricante al gobierno de EE.UU.

La información contenida en el presente documento está sujeta a cambios sin previo aviso. Las únicas garantías de los productos y servicios HP son las que se establecen en las declaraciones expresas de garantía que se incluyen con tales productos y servicios. Ninguna información contenida en este documento se debe interpretar como una garantía adicional. HP no se hará responsable de los errores técnicos o de edición ni de las omisiones contenidas en el presente documento.

Segunda edición: noviembre de 2021

Primera edición: abril de 2021

Número de referencia del documento: M53784–E52

Software de código abierto

Este producto incluye software licenciado bajo una licencia de software de código abierto, como la Licencia Pública General de GNU y la Licencia Pública General Reducida de GNU u otra licencia de código abierto. En la medida en que HP tenga la obligación o, a su exclusivo criterio, decida poner a disposición el código fuente de dicho software de acuerdo con la licencia de software de código abierto aplicable, el código fuente del software puede obtenerse en el siguiente lugar: https://ftp.hp.com/pub/tcdebian/pool/ThinPro7.2

Clave de sintaxis de entrada de usuario

El texto que debe introducir en una interfaz de usuario se indica con una `fuente con ancho fijo`.

Tabla Clave de sintaxis de entrada de usuario

Elemento	Descripción
`Texto sin corchetes ni llaves`	Los elementos que debe escribir exactamente como se muestra
`<Texto dentro de corchetes angulares>`	Un marcador de posición para un valor que debe proporcionar; omita los corchetes
`[Texto dentro corchetes cuadrados]`	Elementos opcionales; omita los corchetes
`{Texto dentro de llaves}`	Un conjunto de elementos de los cuales solo debe elegir uno; omita los corchetes
`|`	Un separador para los elementos de los cuales solo debe elegir uno; omita la barra vertical
`...`	Elementos que se pueden o se deben repetir; omita los puntos suspensivos

Tabla de contenido

1 Pasos iniciales

Esta guía se destina a los administradores de thin clients HP basados en el sistema operativo HP ThinPro y presupone que usted iniciará sesión en el sistema como administrador al modificar las configuraciones del sistema o usar herramientas administrativas según se describe en esta guía.

NOTA: HP ThinPro cuenta con dos configuraciones de SO posibles: ThinPro y Smart Zero. Los thin clients basados en HP ThinPro se pueden comprar con cualquiera de las dos configuraciones de SO como versión predeterminada y usted puede alternar entre las configuraciones mediante el Panel de control.

Para obtener más información sobre cada configuración de SO, consulte Elección de una configuración de SO en la página 1. Para obtener más información sobre la alternación entre las configuraciones de SO, consulte Centro de personalización en la página 79.

Obtener más información

Los recursos de información para ThinPro y otros programas de software están disponibles en línea.

NOTA: La información en los sitios web indicados en esta tabla podría estar disponible solo en inglés.

Tabla 1-1

Recurso	Contenido
Sitio web de soporte de HP http://www.hp.com/support	Guías del administrador, guías de referencia de hardware, libros blancos y otra documentación ▲ Busque el modelo de thin client y, a continuación, consulte la sección **Guías de usuario** de la página de soporte de ese modelo. **NOTA:** HP Device Manager y el software HP Remote Graphics tienen una página de soporte dedicada a cada uno; por lo tanto, busque el nombre de la aplicación y, a continuación, consulte la sección **Guías de usuario**.
Sitio web de soporte de Microsoft http://support.microsoft.com	Documentación de software de Microsoft
Sitio web de soporte de Citrix http://www.citrix.com/support	Documentación de software de Citrix
Sitio web de soporte de VMware http://www.vmware.com/support	Documentación de software de VMware

Elección de una configuración de SO

HP ThinPro incluye dos configuraciones de SO, cada una de ellas a la medida de diferentes escenarios de implementación del thin client:

- La configuración de SO **ThinPro** es la versión completa del sistema operativo y es la más adecuada para entornos con múltiples fines que requieren administración avanzada o personalización del usuario final. Las características de esta configuración de SO incluyen:
  - Se inicia en el escritorio ThinPro o en la pantalla de inicio de sesión de Active Directory
  - Tiene más tipos de conexión que Smart Zero
  - Permite configurar y ejecutar simultáneamente varias conexiones (de cualquier tipo compatible)
- La configuración de SO **Smart Zero** es una versión más simple y más segura del sistema operativo y es la más adecuada para entornos al estilo quiosco y con un fin único que requieren administración mínima y muy poca o ninguna personalización del usuario final. Las características de esta configuración de SO incluyen:
  - Se inicia directamente en una sesión virtual y oculta el escritorio, un recurso también conocido como "modo quiosco"
  - Tiene menos tipos de conexión que ThinPro
  - Admite que se configure y ejecute solo una conexión a la vez
  - No admite la autenticación de Active Directory ni el inicio de sesión único

NOTA: Puede alternar entre las configuraciones del SO mediante el Panel de control (consulte Centro de personalización en la página 79).

También puede personalizar algunos de los valores predeterminados de cada configuración de SO; por ejemplo, para cambiar los tipos de conexión que están disponibles, permitir el modo quiosco para ThinPro o iniciar en el escritorio para Smart Zero.

Para obtener más información sobre el modo quiosco, consulte Modo quiosco en la página 14.

La siguiente tabla enumera los tipos de conexión disponibles predeterminados para cada configuración de SO.

Tabla 1-2 Configuraciones de OS

Configuración de OS	Tipos de conexión disponibles predeterminados
ThinPro	• Citrix® • RDP • VMware® Horizon® View™ • Web Browser (Firefox) • XDMCP • Secure Shell • Telnet • Personalizada
Smart Zero	• Citrix • RDP • VMware Horizon View • Web Browser (Firefox)

Elección de un servicio de administración remota

Independientemente de la configuración de SO, hay dos servicios de administración remota diferentes que puede usar para administrar los thin clients basados en HP ThinPro:

- **HP Device Manager (HPDM)** es ideal para entornos grandes con diversos entornos operativos, incluida una mezcla de thin clients basados en HP ThinPro y en Windows®. HPDM brinda más variedad de opciones de administración que HP Smart Client Services. Para obtener más información o para descargar HPDM, vaya a http://www.hp.com/go/hpdm.
- **HP Smart Client Services** puede administrar solo thin clients basados en HP ThinPro y está optimizado para el uso con Smart Zero y un escenario de "administración cero". Para obtener más información, consulte HP Smart Client Services en la página 82.

HP recomienda evaluar ambos servicios y elegir el que sea mejor para su implementación.

Iniciar el thin client por primera vez

Cuando inicia por primera vez un nuevo thin client basado en HP ThinPro, se ejecuta automáticamente un programa de configuración. El Asistente de configuración inicial le permite seleccionar un idioma, seleccionar la asignación del teclado, seleccionar una conexión de red y configurar la fecha y la hora.

SUGERENCIA: Si desea modificar la configuración de un único thin client y luego copiar e implementar la configuración en otros thin clients, use primero el Asistente de configuración inicial y el Panel de control para alterar la configuración. Luego, implemente la configuración con HPDM o HP ThinState. Para obtener más información, consulte Descripción general de la GUI en la página 8 o Panel de control en la página 57. Para obtener más información sobre HP ThinState, consulte HP ThinState en la página 70.

Alternar entre el modo administrador y el modo usuario

Siga las instrucciones que se describen a continuación para alternar entre el modo de administrador y el modo de usuario.

▲ Haga clic derecho en el escritorio o seleccione **Inicio** y luego seleccione en el menú **Cambiar a Administrador**.

Para obtener más información sobre el escritorio, consulte Escritorio en la página 8.

Para obtener más información sobre el Panel de control, consulte Barra de tareas en la página 8 y Panel de control en la página 57.

NOTA: La primera vez que pase al modo administrador, se le solicitará que configure una contraseña de administrador. La contraseña de administrador se deberá introducir cada vez que pase al modo administrador. Cuando se habilita la autenticación de Active Directory, también puede pasar al modo de administrador introduciendo las credenciales del dominio de una persona del grupo de administradores del dominio.

Cuando se encuentra en el modo administrador, la pantalla tiene un borde rojo.

2 ThinPro PC Converter

A partir de ThinPro 7.1, puede usar ThinPro en hardware que no sean thin clients HP mediante HP ThinPro PC Converter Deployment Tool. El sistema debe cumplir con estos requisitos mínimos:

- CPU: cualquier CPU x86 de 64 bits.
- Memoria: 4 GB de memoria RAM, con al menos 1 GB libre para el uso del sistema operativo.
- Almacenamiento: 8 GB o más de almacenamiento interno para la instalación.
- Gráficos: Intel®, ATI™/AMD® o NVIDIA®. Si la tarjeta gráfica no es reconocida, puede utilizar el modo VESA de rendimiento limitado.
- Audio: la compatibilidad de audio es opcional.
- Redes: un adaptador de red cableado o inalámbrico reconocido.
- USB: HP recomienda unidades flash USB Type-C® de alto rendimiento.
- Licencias: el software ThinPro debe tener una licencia adecuada.

La primera vez que un sistema se inicia con ThinPro, aparece una ventana de verificación de compatibilidad que muestra el estado de compatibilidad del sistema de cada uno de estos requisitos.

Herramienta de implementación

HP ThinPro PC Converter Deployment Tool le permite ejecutar ThinPro en un equipo que ejecuta Microsoft Windows y que cumple con los requisitos mínimos. Esta herramienta permite la creación de una unidad flash USB que contiene la imagen de ThinPro. Puede iniciar y ejecutar la imagen de ThinPro desde la unidad flash USB creada o puede instalar la imagen de ThinPro directamente en el equipo. También tiene la opción de crear una imagen de implementación masiva mediante herramientas de administración remota.

Para obtener más detalles, consulte la *Guía del administrador de HP ThinPro PC Converter Deployment Tool*.

Verificación de la compatibilidad e instalación

La primera vez que ThinPro se inicia desde una unidad flash USB, aparece la ventana de Verificación de compatibilidad. La herramienta Verificación de compatibilidad evalúa el hardware del sistema para ver si cumple con los requisitos mínimos y si el software ThinPro ha reconocido el dispositivo y ha asignado un controlador de dispositivo. Si el sistema no cumple con los requisitos mínimos, o si no se encuentra el hardware necesario, la herramienta Verificación de compatibilidad mostrará una advertencia e información adicional.

NOTA: La herramienta Verificación de compatibilidad solo hace un examen superficial del estado del hardware y del controlador. No realiza comprobaciones detalladas de la funcionalidad, como el envío de paquetes de red, la reproducción de archivos de audio, la prueba de bloques de memoria erróneos o la evaluación del rendimiento. HP no puede garantizar que todos los componentes de hardware del equipo funcionen bien con ThinPro, incluso si la herramienta Verificación de compatibilidad determina que el equipo es compatible.

Si ThinPro se está ejecutando desde una unidad flash USB y si Verificación de compatibilidad aprueba todas las comprobaciones necesarias, aparecen dos botones en la parte inferior de la ventana. El primer botón permite que el software ThinPro se instale directamente en el almacenamiento interno. El segundo botón le permite ejecutar ThinPro desde la unidad flash USB sin instalación directa en el equipo.

NOTA: El botón de instalación solo aparecerá con una unidad flash USB creada con la opción Installer Flash Drive de Deployment Tool. La opción Bootable Flash Drive no permite la instalación.

Al instalar ThinPro en el equipo, tiene la opción de guardar las configuraciones establecidas al ejecutar ThinPro desde la unidad flash USB. Si no se guardan las configuraciones, se instalará la imagen de fábrica predeterminada de ThinPro.

La herramienta Verificación de compatibilidad también se puede iniciar manualmente desde la lista de herramientas de administrador, debajo del botón de Inicio.

Licencias

Los thin clients HP admitidos tienen licencia automática y no necesitan archivos de licencia. Si un sistema tiene licencia automática, muchas de las fuentes de información de licencias que aparecen a continuación no serán visibles.

Todos los demás sistemas necesitan archivos de licencia válidos para ejecutar ThinPro. Los archivos de licencia se obtienen en el Depósito de software de HP Inc.

Deployment Tool le solicitará que navegue hasta los archivos de licencia válidos. Los archivos que seleccione se copiarán automáticamente cuando cree una unidad flash USB de inicio e instalación de ThinPro, y cuando cree una imagen de implementación masiva.

Si Deployment Tool y las licencias válidas se utilizan para instalar ThinPro en un dispositivo, no es necesario instalar manualmente los archivos de licencia. Sin embargo, si instala ThinPro por otros medios, es posible que tenga que copiar archivos de licencia en el directorio `/persistent/licenses` del dispositivo. Puede utilizar HP Device Manager (o algún otro mecanismo) para realizar esta implementación.

Tipos de licencia

Hay tres tipos de archivos de licencia:

- Una licencia de prueba le permite ejecutar ThinPro por un periodo de tiempo corto sin pagar las tarifas de licencia.
- Una licencia de unidad le permite ejecutar una versión específica de ThinPro indefinidamente. También denota que los royalties se han pagado y desbloquea cualquier software que implique royalties.
- Una licencia de soporte brinda acceso a los parches y mejoras del sistema y permite que el sistema se actualice a versiones más recientes de ThinPro.

Según la combinación de las licencias presentes en el sistema, varias funciones estarán visibles, ocultas o deshabilitadas.

Icono de la bandeja del sistema

Un icono de la bandeja del sistema indica el estado de licencia del sistema.

Tabla 2-1 **Icono de la bandeja del sistema**

Icono	Descripción
	Licencia válida.
	La licencia expirará próximamente.
	Licencia inválida (como una licencia de prueba expirada).

Al pasar el cursor sobre el icono de la bandeja del sistema, aparece información sobre las licencias activas que se encuentran en el sistema. Al hacer clic con el botón derecho, se iniciará la aplicación System Info con la ficha **License** seleccionada.

Notificaciones

Es posible que aparezcan notificaciones por encima del icono de la bandeja del sistema periódicamente.

Las notificaciones de cortesía avisan cuando una licencia de soporte o una licencia de prueba se aproxima a la fecha de expiración. Puede deshabilitar las notificaciones de cortesía mediante ciertas configuraciones del registro. Consulte Claves de registro en la página 102 para obtener más información.

Otras notificaciones advierten sobre los errores de licencia, como los archivos de licencia expirados, faltantes o inválidos. No puede deshabilitar este tipo de notificaciones.

Información del sistema

La ficha Software License de la aplicación System Information muestra tanto el estado general de licencia del sistema como los detalles de cada archivo de licencia que se encuentra en el sistema, incluidas las fechas de inicio y fin, la cantidad de licencias, el número de serie de la licencia y otra información.

Marca de agua en el segundo plano del escritorio

El texto de la marca de agua se muestra en el fondo del escritorio con una licencia de prueba o con una combinación de licencias expiradas o inválidas. No puede deshabilitar este texto de marca de agua.

Herramientas de actualización del sistema

Si un sistema no tiene licencia automática y no cuenta una licencia de soporte activa, los parches y actualizaciones mostrados por Easy Update y otras herramientas de actualización del sistema serán limitados.

Software con royalties

Algunos programas de software utilizados por ThinPro tienen royalties. Un ejemplo es cualquier función que utilice la decodificación de video H.264. Si el sistema no tiene licencia automática y no se encuentra ninguna

licencia de unidad válida en el sistema, se deshabilitará el software con royalties. Las licencias de prueba no permiten software con royalties.

Conexiones

Si no se encuentra ninguna combinación de licencia válida en el sistema, la capacidad de crear conexiones remotas a otros sistemas podría estar limitada o deshabilitada.

3 Descripción general de la GUI

Escritorio

La sección describe la interfaz gráfica de usuario del escritorio.

NOTA: La siguiente imagen demuestra el escritorio de ThinPro con una configuración local para los EE. UU. En el caso de Smart Zero, la barra de tareas es vertical y viene alineada a la derecha de forma predeterminada; además, el tema del escritorio varía según el tipo de conexión. El formato de la pantalla de cierta información de la barra de tareas varía según la configuración local.

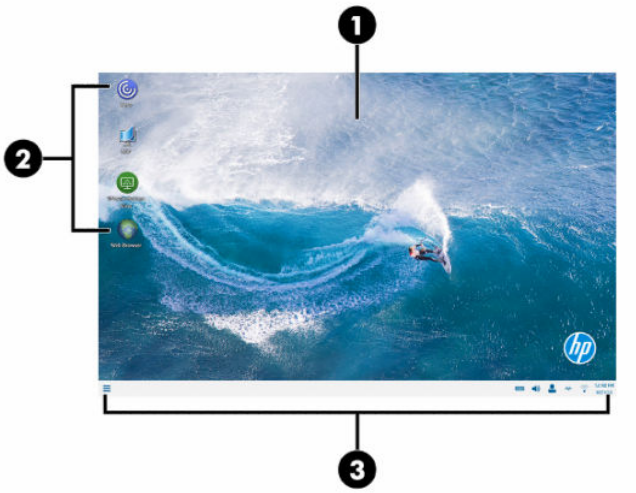

Tabla 3-1

Elemento		Descripción
(1)	Escritorio	En ThinPro, puede organizar accesos rápidos a la conexión en el área del escritorio y personalizar el tema de fondo. En Smart Zero, el escritorio se sustituye por una pantalla de inicio de sesión personalizable con un tema específico para el tipo de conexión elegido.
(2)	Accesos directos a la conexión	Haga doble clic en el acceso directo de una conexión para iniciarla. Haga clic derecho en el icono para mostrar un menú de acciones relacionadas con la conexión actual y selecciónelo para arrastrarlo a una nueva ubicación.
(3)	Barra de tareas	Brinda acceso rápido a programas y funciones del sistema (consulte Barra de tareas en la página 8 para obtener más información).

Barra de tareas

La sección describe la barra de tareas.

NOTA: La siguiente imagen demuestra la barra de tareas de ThinPro con una configuración local para los EE. UU. En el caso de Smart Zero, la barra de tareas es vertical y está alineada a la derecha de forma predeterminada. El formato de la pantalla de cierta información de la barra de tareas varía según la configuración local.

Tabla 3-2

Elemento		Descripción
(1)	Inicio	Muestra un menú principal. Para obtener más información, consulte Menú de Inicio en la página 55.
(2)	Área de aplicación	Muestra los iconos de las aplicaciones abiertas en el momento. **SUGERENCIA:** Puede mantener presionadas las teclas Ctrl+Alt y luego presionar Tab varias veces para seleccionar una aplicación y que aparezca en primer plano.
(3)	Bandeja del sistema	Brinda acceso rápido o información acerca de ciertas funciones y servicios. Coloque el cursor sobre un elemento de la bandeja del sistema para mostrar el texto explicativo (solo en algunos elementos). Seleccione para iniciar una acción de configuración y haga clic derecho para mostrar un menú. Entre los elementos de la bandeja del sistema pueden incluirse los siguientes (es posible que algunos elementos no aparezcan según la configuración del sistema): • Mezclador de audio • Teclado: seleccione este icono para cambiar la disposición del teclado, abra el teclado virtual o cambie la disposición del teclado. Haga clic derecho para abrir el teclado virtual. Para mostrar el nombre de la disposición actual del teclado, pase el cursor sobre el icono. • Estado de la red por cable: haga clic derecho sobre este icono para mostrar más información sobre una red conectada. • Estado de la red inalámbrica: seleccione este icono para ver una lista de redes inalámbricas disponibles y conectarse a una de ellas mediante la creación de un perfil inalámbrico para esa red. • Opciones de Automatic Update: el icono de Automatic Update aparece cuando Automatic Update busca actualizaciones o actualiza el equipo. Para ver más información, seleccione el icono. Si ThinPro no puede encontrar un servidor de actualización automática o está deshabilitada la clave de registro para mostrar el icono, éste no aparece. • Intelligent Input Bus (Ibus): Ibus es un marco de método de entrada (IM) para la entrada multilingüe en sistemas operativos similares a Unix. • Icono de la batería: para abrir el Administrador de energía, haga clic derecho en este icono y seleccione **Ajustar configuraciones de energía**. • Icono del usuario: indica que está habilitada la autenticación de Active Directory. Selecciónelo para bloquear la pantalla o actualizar la contraseña del dominio. Para mostrar al usuario actual, pase el cursor sobre el icono.

Tabla 3-2 (continúa)

Elemento		Descripción
		• Icono de licencia: indica el estado de las licencias de ThinPro. Pase el cursor sobre el icono para ver los detalles de las licencias actualmente activas y haga clic derecho para ir a la página de System Info y ver más detalles sobre las licencias. Esto no es visible en los thin clients HP actuales, ya que tienen licencia automática.
(4)	Fecha y Hora	Muestra la fecha y la hora actuales y abre las configuraciones de fecha y hora.

4 Configuración de la conexión

La administración de conexiones se puede realizar directamente desde el escritorio, así como a través del Administrador de conexión heredado o el menú de Inicio. De forma predeterminada, el escritorio muestra un icono como un acceso directo para cada conexión configurada.

Cuando inicia el equipo por primera vez, aparecen varios iconos de conexión en el escritorio. Puede crear un acceso directo de conexión nuevo, genérico, para cualquiera de los tipos de conexiones que admite ThinPro.

Para obtener más información sobre el Administrador de conexión heredado, consulte Administrador de conexiones (solo en ThinPro) en la página 12.

Crear un nuevo acceso directo de conexiones

Para Crear un nuevo acceso directo de conexiones:

- Haga clic con el botón derecho en el escritorio y seleccione **Crear**.

Administración de iconos del escritorio

Todos los iconos se colocan automáticamente en una cuadrícula. Puede hacer clic y arrastrar un icono a cualquier otra posición de la cuadrícula en el escritorio. Después de que un icono se ha movido a una posición de la cuadrícula, se fija en esa posición. Se mantiene en esa posición incluso si se agregan, eliminan o reacomodan otros accesos directos de conexión.

Los iconos que no se fijan en una posición de la cuadrícula quedan flotando. Pueden moverse automáticamente cuando se agregan, eliminan o reacomodan accesos directos de conexión. Para que un icono fijo se transforme en un icono flotante, haga clic derecho y elimine **Fijar posición**.

Administración de conexiones del escritorio

La administración de conexiones se puede realizar directamente desde el escritorio, así como a través del Administrador de conexión heredado o el menú de Inicio. De forma predeterminada, el escritorio muestra un icono como un acceso directo para cada conexión configurada.

Cuando inicia el equipo por primera vez, aparecen varios iconos de conexión en el escritorio. Puede crear un acceso directo de conexión nuevo, genérico, para cualquiera de los tipos de conexiones que admite ThinPro.

Para obtener más información sobre el Administrador de conexión heredado, consulte Administrador de conexiones (solo en ThinPro) en la página 12.

Puede iniciar, detener, editar, copiar, renombrar o eliminar cada conexión. Si no está habilitada la edición del usuario, los usuarios que no son administradores solo pueden iniciar o detener una conexión.

- Para administrar una conexión en el escritorio, haga clic derecho en el icono de conexión y seleccione una acción.

NOTA: Si la edición del usuario no está habilitada, debe cambiar al modo de administrador para administrar una conexión.

- **Iniciar/Detener**: inicia una conexión o detiene una conexión activa. También puede hacer doble clic en el icono de conexión. Cuando la conexión está activa, aparece un círculo verde en el icono de conexión y éste aparece en la barra de tareas. Cuando se inicia una conexión, si falta cualquier parámetro de la conexión, un cuadro de diálogo solicita los parámetros faltantes. Por ejemplo, como ninguno de los iconos de inicio tiene un servidor remoto definido, un cuadro de diálogo solicita la dirección o el nombre del servidor remoto cuando se inicia la conexión.
- **Editar**: abre el editor de la conexión completa.
- **Copiar**: crea una copia de la conexión con todos los parámetros de la conexión original y un nombre único.
- **Renombrar**: le permite renombrar la conexión. También puede hacer doble clic en el texto debajo del icono de la conexión o usar el editor de conexión.
- **Eliminar**: elimina la conexión.

Administrador de conexiones (solo en ThinPro)

Esta sección identifica los componentes del Administrador de conexiones (Connection Manager) y explica cómo abrirlo.

NOTA: HP recomienda el uso de los accesos directos de conexión. No obstante, puede usar la interfaz del Administrador de conexión heredado.

La siguiente imagen demuestra el Administrador de conexión con una configuración local para los EE. UU.

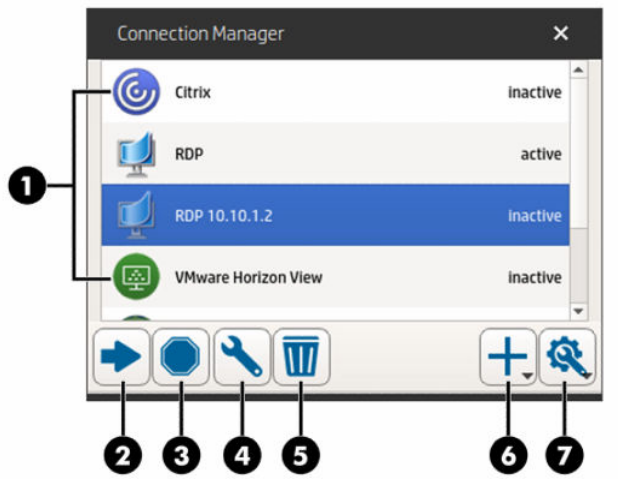

Tabla 4-1

Elemento		Descripción
(1)	Lista de conexiones	Enumera las conexiones configuradas y especifica si cada conexión está activa o inactiva.
(2)	Inicio	Inicia la conexión seleccionada.
(3)	Detener	Detiene la conexión seleccionada.
(4)	Editar	Le permite editar la conexión seleccionada.
(5)	Delete (Eliminar)	Elimina la conexión seleccionada.

Tabla 4-1 (continúa)

Elemento		Descripción
(6)	Agregar	Le permite agregar una nueva conexión. NOTA: Consulte Elección de una configuración de SO en la página 1 para ver una lista de los tipos de conexión disponibles.
(7)	Configuración	Le permite editar los ajustes generales de las conexiones Citrix. Estos ajustes se aplican a todas las conexiones de ese tipo.

Para abrir el Administrador de conexión:

1. En el modo de administrador, seleccione **Inicio** y luego escriba `Administrador de conexión` en el cuadro de búsqueda.
2. Seleccione **Administrador de conexión**.

Para obtener más información sobre cómo configurar las conexiones, consulte las siguientes opciones:

- Configuración de la conexión en la página 11
- Tipos de conexión en la página 16

Ajustes de conexión avanzada

La siguiente tabla describe las configuraciones disponibles en la categoría Avanzado al editar una conexión de cualquier tipo.

NOTA: Estos ajustes afectan solo la conexión que está configurando en ese momento.

Tabla 4-2 Ajustes de conexión avanzada

Opción	Descripción
Conexión alternativa	Especifica la conexión alternativa. Si la conexión no se inicia, la conexión alternativa intentará iniciarse en su lugar. NOTA: Esta opción no está disponible para el tipo de conexión VMware Horizon View.
Prioridad de inicio automático	Determina en qué orden se iniciarán las conexiones de manera automática. **0** significa que el inicio automático está desactivado. Los otros valores determinan el orden de inicio. La prioridad más alta es **1**.
Compartir credenciales con protector de pantalla	Permite que los usuarios desbloqueen el protector de pantalla local usando sus credenciales para esa conexión. NOTA: Esta opción solo está disponible para los tipos de conexión Citrix, RDP y VMware Horizon View.
Reconexión automática	Si la opción está activada, y la conexión se interrumpe, esta conexión intentará volverse a conectar de forma automática. NOTA: Si detiene una conexión mediante el Administrador de conexión no funcionará la reconexión automática.
Espere por red antes de conectar	Desactive esta opción si su conexión no necesita una red para iniciarse o si no desea esperar a la red para iniciar la conexión.
Mostrar icono en el escritorio	Si está habilitada, se crea un icono de escritorio para esta conexión. Esta opción está habilitada de forma predeterminada.

Tabla 4-2 **Ajustes de conexión avanzada (continúa)**

Opción	Descripción
	Si está deshabilitada, la conexión no es visible en el escritorio, pero es visible en el menú de Inicio y en el Administrador de conexión.
Permitir que el usuario inicie esta conexión	Si está activada, un usuario final puede iniciar esta conexión.
Permitir que el usuario edite esta conexión	Si está activada, un usuario final puede modificar esta conexión.
Opciones del cuadro de diálogo de inicio de sesión	Active o desactive estas opciones para configurar el cuadro de diálogo de inicio de sesión para la conexión. **NOTA:** Esta opción solo está disponible para los tipos de conexión Citrix, RDP y VMware Horizon View. Se encuentran disponibles las siguientes opciones: • **Mostrar el campo del servidor** • **Mostrar el campo nombre de usuario** • **Mostrar el campo contraseña** • **Mostrar el campo dominio** • **Mostrar la casilla de verificación 'recordarme'** **NOTA:** Esta opción guarda el nombre de usuario y el dominio, pero la contraseña debe introducirse cada vez.

Modo quiosco

Cuando un thin client está configurado en el modo quiosco, inicia sesión automáticamente en la conexión predeterminada en el inicio mediante las credenciales de usuario predefinidas. Si la conexión se pierde debido a un cierre de sesión, desconexión o fallo de la red, se vuelve a conectar automáticamente tan pronto como se restaure.

SUGERENCIA: Es posible configurar el host remoto para iniciar los recursos automáticamente en el inicio de sesión. Esto hace que el modo quiosco sea una experiencia impecable.

La forma más fácil de configurar un thin client para el modo quiosco es cambiarlo a Smart Zero (consulte Centro de personalización en la página 79) y configurar una conexión. Una vez hecho esto, los siguientes ajustes se definen automáticamente:

- Ocultar la barra de tareas de forma automática.
- Iniciar la conexión de forma automática.
- Volver a conectar la conexión de forma automática
- La conexión comparte las credenciales de usuario con el protector de pantalla local.
- El tema del escritorio se ajusta de acuerdo al tema predeterminado de ese tipo de conexión.
- El protocolo de redirección USB en el Administrador de USB está configurado conforme al protocolo de ese tipo de conexión.

Si desea configurar un thin client para el modo quiosco en ThinPro (por ejemplo, si desea utilizar un tipo de conexión disponible solo con ThinPro), configure manualmente los siguientes ajustes para la conexión deseada:

- En el Centro de personalización, establezca la opción **Ocultar automáticamente** para la barra de tareas.
- En los ajustes de la conexión, haga lo siguiente:
  - Establezca **Prioridad de inicio automático** en **1**.
  - Active la **Reconexión automática**.
  - Active **Compartir credenciales con el protector de pantalla**, si está disponible.
  - Para una conexión Web Browser únicamente, seleccione la opción **Activar el modo Quiosco**.
- En el Administrador de USB, defina el protocolo adecuado de redirección USB, si es necesario.

SUGERENCIA: Cuando se encuentra en el modo quiosco, para minimizar la conexión y volver al escritorio local, presione Ctrl+Alt+Fin.

5 Tipos de conexión

Citrix

La siguiente tabla describe los backends admitidos de Citrix XenApp.

Tabla 5-1 Backends de Citrix XenApp

Tipo de acceso	Versión de XenApp
PNAgent (heredado)	7.6 LTSR y 7.15 LTSR y 7.16 o posterior
Navegador Web	7.6 LTSR y 7.15 LTSR y 7.16 o posterior
StoreFront	7.6 LTSR y 7.15 LTSR y 7.16 o posterior
Workspace	7.6 LTSR y 7.15 LTSR y 7.16 o posterior

La siguiente tabla describe los backends admitidos de Citrix XenDesktop®.

Tabla 5-2 Backends de Citrix XenDesktop

Tipo de acceso	Versión de XenApp
PNAgent (heredado)	7.6 LTSR y 7.15 LTSR y 7.16 o posterior
Navegador Web	7.6 LTSR y 7.15 LTSR y 7.16 o posterior
StoreFront	7.6 LTSR y 7.15 LTSR y 7.16 o posterior
Workspace	7.6 LTSR y 7.15 LTSR y 7.16 o posterior

Administrador de conexión Citrix

La siguiente sección describe las configuraciones disponibles en las diversas categorías al editar la conexión Citrix.

NOTA: La conexión, la configuración y los ajustes avanzados afectan solo la conexión que está configurando en el momento. Los ajustes generales afectan todas las conexiones Citrix.

Conexión

La siguiente tabla describe las configuraciones disponibles en la categoría Conexión al editar los ajustes generales de Citrix.

Tabla 5-3 Conexión

Opción	Descripción
Nombre	El nombre de la conexión.

Tabla 5-3 Conexión (continúa)

Opción	Descripción
Modo de conexión	Establece el modo de conexión en una de las siguientes opciones: • **PNAgent** • **StoreFront** • **Workspace** **NOTA:** Las opciones de autenticación se muestran después de esta opción y varían según el modo de conexión que seleccionó. Consulte la documentación de Citrix para obtener más información. **NOTA:** Puede probar los ajustes de conexión al seleccionar el botón **Probar la conexión**.
URL	Nombre de host del o dirección IP del servidor de Citrix. Si está configurando una conexión a un servidor en un sitio HTTPS, introduzca el FDQN del sitio y el certificado raíz local en el almacén de certificados de Citrix. Si se marca, la casilla de verificación que está al lado de esta opción fuerza una conexión de HTTPS.
Ignorar verificación del certificado	Omite la verificación del certificado del servidor Citrix. **NOTA:** El modo Workspace no puede ignorar la verificación de certificado.
Credenciales	Establece el modo de autenticación en una de las siguientes opciones: • **Inicio de sesión anónimo**: para los servidores StoreFront que permiten a usuarios no autenticados (anónimos). • **Usar credenciales de inicio de sesión único**: las credenciales usadas en el inicio de sesión también se usan para empezar la conexión. • **Pedir credenciales en el inicio de la conexión**: no hay componentes de credencial suministrados previamente. • **Usar usuario, contraseña y/o dominio predefinidos**: algunas o todas las credenciales se almacenan y suministran para la conexión. • **Usar smart card predefinida**: se espera que se use la conexión con una smart card para la autenticación.
Usuario	El nombre de usuario de esta conexión.
Contraseña	La contraseña de esta conexión.
Dominio	El nombre de dominio de esta conexión (opcional).
Probar la conexión	Verifica la URL y las credenciales.

Configuración

La siguiente tabla describe las configuraciones disponibles en la categoría Configuración al editar los ajustes generales de Citrix.

Tabla 5-4 Configuración

Opción	Descripción
Auto Reconnect Applications on Login (Reconexión automática de aplicaciones en el inicio de sesión)	Con esta opción seleccionada, los recursos que estaban abiertos la última vez que el usuario terminó la sesión se vuelven a abrir cuando se inicia sesión nuevamente. **SUGERENCIA:** Si no está utilizando el recurso SmoothRoaming de Citrix, desactive esta opción para aumentar la velocidad de su conexión.
Modo de inicio automático	Le permite establecer que un escritorio o una aplicación específica se inicien de forma automática cuando se inicia la conexión de Citrix. Si se establece en **Iniciar automáticamente un único recurso** y, hay un único recurso publicado, ese recurso de inicia de forma automática. **NOTA:** Esta opción queda sin efecto si se selecciona **Reconectar automáticamente aplicaciones al iniciar sesión** y hay aplicaciones a las que es posible reconectarse. Si seleccionó Iniciar automáticamente la aplicación o Iniciar automáticamente el escritorio, seleccione el botón **Enumeración** para recuperar una lista de recursos (aplicaciones o escritorios) y mostrarlos en Citrix Connection Manager, lo que le permite seleccionar los recursos automáticamente tras la conexión. Si seleccionó Inicio automático de un solo recurso, seleccione el botón **Enumeración** para recuperar la cantidad de recursos. Si hay un único recurso, se inicia automáticamente tras la conexión.
Mostrar los recursos	Con esta opción seleccionada, debe seleccionar dónde mostrar los recursos: • **En una ventana**: muestra los recursos en una ventana. • **Directamente en el escritorio**: muestra los recursos en el escritorio.
Mostrar los recursos en el menú de Inicio	Con esta opción seleccionada, los recursos remotos de la conexión se muestran en el menú de Inicio.
Mostrar solo los recursos suscritos	Si se selecciona, solo se muestran los recursos suscritos durante una conexión de Citrix. **NOTA:** Esta opción no es compatible cuando utiliza la interfaz de usuario de Citrix Self-Service.

Configuración General

Para editar los ajustes generales:

▲ En el Administrador de conexión Citrix, seleccione la ficha **Ajustes generales** y luego seleccione **Administrador de configuraciones generales de la conexión Xen**.

NOTA: Estos ajustes afectan todas las conexiones de Citrix.

Opciones

La siguiente tabla describe las configuraciones disponibles en la categoría Opciones al editar los ajustes generales de Citrix.

Tabla 5-5 Opciones

Opción	Descripción
Activar HDX MediaStream	Activa HDX MediaStream.
Habilitar MultiMedia	Activa multimedia
Habilitar la barra de conexión	Activa la barra de conexión.

Tabla 5-5 Opciones (continúa)

Opción	Descripción
Activar Auto Reconexión	Permite la reconexión automática de conexiones interrumpidas.
Activar Session Reliability	Activa el recurso Session Reliability de Citrix. Consulte la documentación de Citrix para obtener más información.
Habilitar el canal de la smart card	Habilita el recurso del canal de la smart card. **NOTA:** Si quiere usar una smart card en la sesión de Citrix pero no está usando una conexión de smart card, habilite esta opción.
Tiempo de espera de confiabilidad de la sesión (en segundos)	Especifica el tiempo de espera de confiabilidad de la sesión en segundos. El valor predeterminado es 180 segundos.
Activar la redirección del portapapeles	Activa la redirección del portapapeles.
Utilizar Compresión de Datos	Utiliza compresión de datos para esta conexión.
Activar compresión de H264	Activa la compresión de H264. Consulte la documentación de Citrix para determinar si este método de compresión de datos es el mejor para sus casos de uso.
Permitir Pegar con el Botón Central	Habilita la función de pegar del botón central del mouse.
Secuencia de User Agent	Especifica una secuencia de User Agent que se utilizará para las solicitudes enviadas al servidor Citrix. Esta opción es útil para la configuración de Netscaler.
Sonido	Establece la calidad del sonido o desactiva por completo el sonido.
Protocolo de transporte	Especifica el protocolo de transporte para la conexión y si se usa un protocolo de transporte para fallback. • **Desactivado** (predeterminado): usar TCP. • **Activado**: usar UDP y no usar TCP como alternativa en caso de falla. • **Preferido**: probar primero UDP y usar TCP como alternativa en caso de falla.
Usar paquetes de encriptación obsoletos	Especifica si se permiten o no los paquetes de encriptación obsoletos: TLS_RSA, RD4–MD5, RC4_128_SHA.

Recursos Locales

La siguiente tabla describe las configuraciones disponibles en la categoría Recursos Locales al editar los ajustes generales de Citrix.

Tabla 5-6 Recursos Locales

Opción	Descripción
Estado de redirección de USB Citrix	Para configurar, seleccione **Administrador de USB**. Consulte Redirección de dispositivos USB en la página 77. • **Habilitado**: la redirección de USB se admite para la conexión Citrix. • **Deshabilitado**: la redirección de USB está deshabilitada para la conexión Citrix.
Impresoras	Controla la forma en que se maneja la redirección de la impresora.

Tabla 5-6 **Recursos Locales (continúa)**

Opción	Descripción
Entrada de cámara web/audio	Controla la forma en que se maneja la redirección de la entrada de audio y la cámara web local.
Asignación/redirección de unidades	Especifica el método usado para acceder a la unidad local. **NOTA:** Seleccione solo un método de redirección de la unidad. • **Redirección de USB**: habilita la redirección de USB. Para ver más opciones, abra el **Administrador de USB**. • **Asignación dinámica de unidad**: habilita la asignación de unidad dinámica. • **Asignación estática de unidad (heredada)**: habilita la asignación de unidad estática, lo que le permite especificar las asignaciones de unidad a rutas locales. Para especificar estas rutas, seleccione **Configurar carpetas de asignación**.

Ventana

La siguiente tabla describe las configuraciones disponibles en la categoría Ventana al editar los ajustes generales de Citrix.

Tabla 5-7 **Ventana**

Opción	Descripción
Modo TWI	Le permite mostrar una única ventana continua en el escritorio local de ThinPro, como si fuera una aplicación nativa.
Tamaño Predeterminado de Ventana	Cuando el **Modo TWI** se establece en **Forzar la desactivación del modo continuo** se controla el tamaño predeterminado de la ventana.
Colores Predeterminados de Ventana	Establece la profundidad de color predeterminada.
Monitor izquierdo Monitor derecho Monitor superior Monitor inferior	Cuando está desactivado **Mostrar el escritorio virtual en todos los monitores**, estos campos le permiten especificar cómo aparece el escritorio virtual en monitores específicos.

Autoservicio

La siguiente tabla describe las configuraciones disponibles en la categoría Autoservicio al editar las configuraciones generales de Citrix (solo para el modo Workspace).

Tabla 5-8 **Autoservicio**

Opción	Descripción
Opción 1 Habilitar el Modo quiosco	Configura un dispositivo de usuario para que se inicie en el modo quiosco, en el que el autoservicio se inicia en modo de pantalla completa.
Opción 1.1 Mostrar la barra de tareas	Especifica si la barra de tareas se muestra o no. Customization Center cuenta con más opciones para personalizar la barra de tareas.

Tabla 5-8 **Autoservicio (continúa)**

Opción	Descripción
Opción 1.2 Habilitar el modo de usuario compartido	Varios usuarios podrían compartir el dispositivo.
Opción 2 Deshabilitar Citrix Workspace - Preferences	Deshabilita el elemento de menú de Citrix - Preferences en la interfaz de usuario de autoservicio.
Opción 3 Deshabilitar Citrix Connection Center	Deshabilita el elemento de menú de Citrix – Connection Center en la interfaz de usuario de autoservicio.

Firewall

La siguiente tabla describe las configuraciones disponibles en la categoría Firewall al editar los ajustes generales de Citrix.

Tabla 5-9 **Firewall**

Opción	Descripción
Tipo de Proxy	Especifica el tipo de proxy.
Dirección de Proxy	La dirección IP del servidor proxy.
Puerto de Proxy	El puerto para conexión al servidor proxy.
Nombre de usuario	El nombre de usuario a utilizar para conexión al servidor proxy.
Contraseña	La contraseña a utilizar para conexión al servidor proxy.
Utilice Dirección Alterna para Conexión Firewall	El Citrix ICA Client solicitará la dirección alterna definida para el servidor cuando se esté contactando servidores dentro de la firewall. La dirección alterna debe especificarse para cada servidor en una red de servidores.

Accesos Directos de Teclado

La siguiente tabla describe las configuraciones disponibles en la categoría Accesos directos del teclado al editar los ajustes generales de Citrix.

Tabla 5-10 **Accesos Directos de Teclado**

Opción	Descripción
Activar UseLocalIM	Utiliza el método de entrada local para interpretar la entrada de teclado. Esto solo es compatible con los idiomas europeos.
Usar número EUKS	Controla el uso de Extended Unicode Keyboard Support (EUKS) en servidores Windows. Las opciones válidas se describen a continuación: • 0: no se usa EUKS. • 1: EUKS se usa como alternativa. • 2: EUKS se utiliza cuando es posible.
Archivo de asignación del teclado	Especifica el archivo de asignación del teclado. Seleccione **Automático** para permitir que se seleccione el archivo automáticamente. De lo contrario, seleccione un archivo de asignación específico. **NOTA:** Para usar su propio archivo de asignación del teclado, guárdelo en la carpeta: `/usr/lib/ICAClient/keyboard/`.

Tabla 5-10 **Accesos Directos de Teclado (continúa)**

Opción	Descripción
Administración de accesos directos del teclado	Especifica cómo deben manejarse los accesos directos del teclado. Las siguientes configuraciones están disponibles: • **Traducido**: los accesos directos del teclado se aplican al escritorio local (lado del cliente). • **Directo solo en escritorios con pantalla completa**: los accesos directos del teclado se aplican al escritorio remoto (lado del servidor), pero solo para una sesión de ICA que no sea continua en modo de pantalla completa. • **Directo**: los accesos directos del teclado se aplican al escritorio remoto (lado del servidor) para las sesiones de ICA continuas y no continuas cuando sus ventanas tienen el enfoque del teclado.
Detener administración de tecla Directa	Especifica la combinación de teclas que desactiva el manejo directo de accesos directos del teclado.
Alt+F1 ... Alt+F12	Le permite agregar accesos directos del teclado que puede manejar.

Sesión

La siguiente tabla describe las configuraciones disponibles en la categoría Sesión al editar los ajustes generales de Citrix.

Tabla 5-11 **Sesión**

Opción	Descripción
Demora al cerrar sesión de forma automática antes de iniciar la aplicación	Cuando utiliza un servidor Citrix con varios recursos publicados, esta opción especifica el número de segundos que un usuario tiene para iniciar una aplicación después de iniciar sesión antes de que el sistema cierre la sesión automáticamente y regrese a la pantalla de inicio de sesión original.
Demora al cerrar sesión de forma automática después de cerrar la aplicación	Cuando utiliza un servidor Citrix con varios recursos publicados, esta opción especifica el número de segundos entre el cierre del último recurso Xen publicado y el momento en que se saca al usuario de la sesión automáticamente y se vuelve a la pantalla de inicio de sesión original.
Intervalo de espera de verificación del servidor	Para realizar una verificación de la conectividad básica del puerto y el servidor seleccionados, configure esta opción con un valor diferente del predeterminado **–1**.
SUGERENCIA: Si cualquiera de estos valores se establece en menos de 0 se desactivará el cierre de sesión automático.	
NOTA: Los retrasos de procesamiento de Citrix pueden aumentar el tiempo de cierre de sesión automático.	

Avanzado

Esta sección menciona dónde puede encontrar información sobre las configuraciones de conexión avanzada, en la categoría Avanzado, al editar una conexión.

NOTA: Consulte Ajustes de conexión avanzada en la página 13 para obtener información sobre los ajustes disponibles en la categoría Avanzado al editar una conexión.

RDP

El cliente RDP se basa en FreeRDP 1.1 y cumple con los siguientes requisitos para RDP:

- RemoteFX acelerado por hardware
- MMR compatible cuando se conecta a hosts de Windows con el recurso Desktop Experience activado
- USBR compatible cuando se conecta a servidores RDP que lo activen

Ajustes por conexión RDP

La siguiente sección describe las configuraciones disponibles en las diversas categorías al editar la conexión RDP.

NOTA: Estos ajustes afectan solo la conexión que está configurando en ese momento.

Red

La siguiente tabla describe los ajustes disponibles en la categoría Red al editar una conexión RDP.

Tabla 5-12 Red

Opción	Descripción
Nombre de la conexión	Un nombre personalizado para esta conexión.
Nombre/dirección del servidor	El nombre del servidor o la dirección IP de esta conexión o la URL de alimentación de RD Web Access. Si es necesario, se puede adjuntar el puerto al servidor después de dos puntos (de forma predeterminada, el puerto es 3389 para una conexión RDP directa). **NOTA:** La URL de alimentación de RD Web Access debe empezar con `https://`. De forma predeterminada, esto se agrega automáticamente tal y como lo especifica la clave de registro de `rdWebFeedUrlPattern`, que define el patrón de la URL.
Credenciales	• **Usar credenciales de inicio de sesión único**: las credenciales usadas en el inicio de sesión también se usan para empezar la conexión. • **Pedir credenciales en el inicio de la conexión**: no hay componentes de credencial suministrados previamente. • **Usar usuario, contraseña y/o dominio predefinidos**: algunas o todas las credenciales se almacenan y suministran para la conexión. • **Usar smart card predefinida**: se espera que se use la conexión con una smart card para la autenticación.
Usuario	El nombre de usuario de esta conexión.
Contraseña	La contraseña de esta conexión.
Dominio	El nombre de dominio de esta conexión (opcional).
Usar RD Gateway	Activa las opciones adicionales de RD Gateway, como la dirección, el puerto y las credenciales de gateway.
Exploración del servidor	Abre la exploración del servidor, que puede utilizarse para determinar cuáles recursos de RDP admite el servidor de RDP.

Servicio

La siguiente tabla describe los ajustes disponibles en la categoría Servicio al editar una conexión RDP.

Tabla 5-13 Servicio

Opción	Descripción
Servicio	Establece el servicio de RDP para una de las siguientes opciones: • **Equipo remoto**: al usar este servicio, se crea una conexión RDP directa a un equipo remoto. Una aplicación remota o un shell alternativo pueden iniciarse opcionalmente tras la conexión. Las siguientes opciones adicionales están disponibles para un servicio de equipo remoto: – Si se establece el **Modo** en **Aplicación remota**, el campo **Aplicación** especifica la ruta de la aplicación que se va a ejecutar. – Si se establece el **Modo** en **Alternar shell**, el campo **Comando** especifica el comando que ejecuta la aplicación que se va a ejecutar en el shell alternativo. Por ejemplo, para ejecutar Microsoft® Word, escriba `Word.exe`. Si se establece el **Modo** en **Shell alternativo**, el campo **Directorio** especifica la ruta del directorio de trabajo del servidor para los archivos de programa de la aplicación. Por ejemplo, el directorio de trabajo de Microsoft Word es `C:\Program Files\Microsoft`. • **RD Web Access**: al usar este servicio, se recupera una lista de recursos de RemoteApp desde el servidor y se presenta al usuario. Además, la conexión RDP se inicia cuando se selecciona un recurso. Las siguientes opciones adicionales están disponibles para RD Web Access: – **Mantener abierta la ventana de selección de recursos**: con esta opción seleccionada, los usuarios pueden abrir varios recursos simultáneamente en la ventana de selección de recursos. – **Iniciar automáticamente el único recurso**: con esta opción seleccionada, y si hay un único recurso publicado, ese recurso se iniciará automáticamente tras la conexión. – **Filtro de recursos** y **Navegador de alimentación de la web**: pueden usarse para limitar los recursos remotos que se pondrán a la disposición del usuario en la ventana de selección de recursos. – **Tiempo para desconexión automática**: con esta opción seleccionada, puede definir cuánto tiempo se puede mantener una conexión Web Access antes de que se cierre automáticamente como medida de seguridad. **NOTA:** Una ventaja de utilizar RD Web Access es que maneja automáticamente los detalles de las conexiones intermediadas y la URL de equilibrio de carga. Para obtener más información, consulte el informe técnico sobre HP ThinPro *«RD Web Access Deployment Example»* (disponible solo en inglés).

Ventana

La siguiente tabla describe los ajustes disponibles en la categoría Ventana al editar una conexión RDP.

Tabla 5-14 Ventana

Opción	Descripción
Ocultar la decoración de la ventana	Esta configuración garantiza que no se muestran los elementos de la pantalla como la barra de menú, las opciones minimizar y cerrar, y los bordes de la ventana.
Window Size (Tamaño de ventana)	Ajusta el tamaño de la ventana a **completo**, **fijo** o **porcentaje**.

Tabla 5-14 **Ventana (continúa)**

Opción	Descripción
Tamaño de porcentaje	Si **Tamaño de ventana** se establece como **porcentaje**, esta opción establece el porcentaje de la pantalla que ocupa una ventana del escritorio. **NOTA:** Los tamaños resultantes podrían redondearse. **NOTA:** RemoteFX admite solo una lista fija de resoluciones.
Tamaño Fijo	Si **Tamaño de ventana** se establece como **fijo**, esta opción establece la altura y el ancho que ocupa una ventana del escritorio en píxeles.

Opciones

La siguiente tabla describe los ajustes disponibles en la categoría Opciones al editar una conexión RDP.

Tabla 5-15 **Opciones**

Opción	Descripción
Permitir eventos de movimiento	Si está activado, los movimientos del mouse se transmiten continuamente al servidor RDP.
Permitir compresión de datos	Activa la compresión de datos a granel entre el servidor de RDP y el cliente de RDP.
Activar la encriptación RDP anterior	Permite la encriptación RDP de la última generación cuando NLA no está disponible.
Activar caché fuera de pantalla	Si está activado, se utiliza la memoria fuera de pantalla para guardar en caché los mapas de bits.
Conectar a la consola de administrador	Establece la conexión con el puerto de consola de administrador.
Copiar/pegar entre sesiones	Si está activado, las opciones copiar y pegar están activadas entre diferentes sesiones RDP.
Activar el almacenamiento en memoria intermedia de los primitivos de RDP6	Si está activado, el rendimiento de gráficos que no son RemoteFX aumenta al costo de actualizaciones de pantalla menos frecuentes.
Habilitar el códec Progressive RemoteFX	Habilita el códec Progressive RemoteFX, que transmite el escritorio en una serie de imágenes cada vez más nítidas. **NOTA:** Este códec podría causar elementos visuales en los escritorios con contenido altamente dinámico, de forma que este códec se puede deshabilitar si es necesario.
Habilitar redirección de contenido multimedia	Permite que se envíen archivos multimedia directamente al cliente para reproducción local.
Política de verificación de certificados	Seleccione una de las siguientes opciones: • **Aceptar todos los certificados de servidor RDP** • **Utilizar hosts recordados; advertir si se trata de un certificado desconocido o inválido** • **Omitir los hosts recordados; advertir si se trata de un certificado desconocido o inválido** • **Conectarse sólo a los servidores RDP previamente aprobados**

Tabla 5-15 **Opciones (continúa)**

Opción	Descripción
Versión de TLS	Establece la versión de Transport Layer Security que se va a usar durante las fases iniciales de negociación con el servidor RDP. Establézcala de forma que coincida con la versión de TLS utilizada por su servidor RDP, o trate de establecerla en **auto**. NOTA: Hay algunos defectos del lado del servidor en ciertos servidores RDP sin parches que pueden hacer que el ajuste automático falle, de forma que no sea el ajuste predeterminado.
Enviar nombre de host como	Con referencia al licenciamiento por dispositivo, esto selecciona la forma en que se envía el nombre de host del cliente al servidor de RDP. Seleccione **nombre de host** o **mac**.
Nombre de host que se va a enviar	Normalmente, el nombre de host del thin client se utiliza para las Licencias de acceso de cliente. Este campo permite enviar un valor distinto. SUGERENCIA: Seleccione el icono **(i)** al lado de esta opción para obtener más información.
Información de equilibrio de carga	Utilice esta opción con una conexión RDP intermediada. SUGERENCIA: Seleccione el icono **(i)** al lado de esta opción para obtener más información.

NOTA: Para obtener más información sobre las opciones **Habilitar el cifrado RDP obsoleto** y **Versión de TLS**, consulte el informe técnico sobre HP ThinPro *«Security Layers for RDP Connections»* (disponible solo en inglés).

Recursos Locales

La siguiente tabla describe los ajustes disponibles en la categoría Recursos Locales al editar una conexión RDP.

NOTA: HP recomienda la redirección de dispositivos de alto nivel a menos que haya una razón específica para usar la redirección de USB (USBR). Para obtener más información, consulte el informe técnico sobre HP ThinPro *«USB Manager»* (disponible solo en inglés).

Tabla 5-16 **Recursos Locales**

Opción	Descripción
Dispositivos de audio	Determina si los dispositivos de audio están redirigidos por redirección de audio RDP de nivel alto, redirección USB de nivel bajo, o si están desactivados para esta conexión.
Impresoras	Determina si las impresoras están redirigidas por la redirección de impresora de nivel alto (esta opción requiere que configure las impresoras a través de la herramienta Impresoras en el Panel de control), USB de nivel bajo, o si están desactivadas para esta conexión.
Puertos seriales/paralelos	Determina si los puertos seriales y paralelos están redirigidos o desactivados para esta conexión.
Almacenamiento USB	Determina si se redirigen los dispositivos de almacenamiento USB, como las unidades flash y ópticas, mediante una redirección de almacenamiento de alto nivel o una redirección de USB de bajo nivel, o si se deshabilitan para esta conexión.
Particiones locales	Determina si las particiones locales de la unidad flash del thin client se redirigen o deshabilitan para esta conexión.

Tabla 5-16 **Recursos Locales (continúa)**

Opción	Descripción
Smart cards	Determina si se redireccionan las smart cards mediante la redirección de smart card de alto nivel o se deshabilita para esta conexión. NOTA: Cuando está habilitada la configuración **Usar smart card predefinida**, se deshabilita este ajuste.
Otros dispositivos USB	Determina si otras clases de dispositivos USB (como cámaras web y tablets) están redirigidas por redirección USB de bajo nivel, o si se deshabilitan para esta conexión.

Experiencia

La siguiente tabla describe los ajustes disponibles en la categoría Experiencia al editar una conexión RDP.

Tabla 5-17 **Experiencia**

Opción	Descripción
Seleccione su velocidad de conexión para optimizar el rendimiento	Si selecciona una velocidad de conexión (**LAN**, **Banda ancha** o **Módem**) activará o desactivará las siguientes opciones para optimizar el rendimiento: • **Segundo plano de escritorio** • **Suavizado de fuentes** • **Composición del escritorio** • **Mostrar el contenido de la ventana mientras se arrastran elementos** • **Animación de menús y ventanas** • **Temas** La selección de **Configuraciones preferidas del cliente** permite que el cliente de RDP elija qué opciones utilizará para proporcionar la mejor experiencia de RDP. También puede seleccionar su propia combinación personalizada de opciones.
Supervisión del estado de la conexión de extremo a extremo	Seleccione esta alternativa para activar las opciones de intervalo de espera. NOTA: Para obtener más información, consulte el informe técnico sobre HP ThinPro *«RDP Connection Drop Detection»* (disponible solo en inglés).
Intervalo de Advertencia	Especifica la cantidad de tiempo en segundos después de recibir el último tráfico de red desde el servidor antes de que se advierta al usuario que se perdió la conexión. Puede desactivar esta función si no selecciona la opción o define la hora en cero. Con la opción **Mostrar el diálogo de advertencia** seleccionada, se mostrará un cuadro de diálogo de advertencia cuando se alcanza el intervalo de espera. De lo contrario, la advertencia solo se escribe en el registro de la conexión. SUGERENCIA: HP recomienda que aumente el valor del tiempo de espera para redes con períodos muy ocupados o interrupciones momentáneas frecuentes.
Tiempo de espera hasta recuperación	Especifica la cantidad de tiempo en segundos después de recibir el último tráfico de red del servidor que el cliente de RDP espera para que se recupere la conexión sin realizar ninguna acción especial. Al final de este período, el cliente de RDP intenta una reconexión rápida con la sesión.
Intervalo de Error	Especifica la cantidad de tiempo en segundos después de recibir el último tráfico de red del servidor que el cliente de RDP espera antes de dejar de intentar conectarse con ese servidor.

Diagnóstico

La siguiente tabla describe los ajustes disponibles en la categoría Diagnóstico al editar una conexión RDP.

Estos recursos diagnostican problemas específicos y están deshabilitados de forma predeterminada.

Tabla 5-18 Diagnóstico

Opción	Descripción
Mostrar el panel de control de RDP	Si se habilita, se muestra el panel de RDP durante la conexión. **SUGERENCIA:** Seleccione el icono **(i)** al lado de esta opción para obtener más información.
Mostrar gráfico de estado de conexión	Con esta opción activada, se mostrará una representación gráfica bidimensional del tiempo de respuesta del servidor de RDP cuando se inicia la conexión. **SUGERENCIA:** Seleccione el icono **(i)** al lado de esta opción para obtener más información.
Análisis de redirección USB	Este recurso determina y muestra el método actual de redirección de cada dispositivo USB redirigido. **SUGERENCIA:** Seleccione el icono **(i)** al lado de esta opción para obtener más información.
X11 sincrónico	Fuerza la descarga frecuente de búfers X11 al costo del rendimiento.
Inicio de sesión	Habilita el logfile X11. Seleccione la opción **Descarga automática** para aumentar la frecuencia de salida de registros al costo del rendimiento.
Capture	Permite la captura y reproducción de salida X11 desde una sesión.

Avanzado

Esta sección menciona dónde puede encontrar información sobre las configuraciones de conexión avanzada, en la categoría Avanzado, al editar una conexión.

NOTA: Consulte Ajustes de conexión avanzada en la página 13 para obtener información sobre los ajustes disponibles en la categoría Avanzado al editar una conexión.

RemoteFX

RemoteFX es un protocolo avanzado de pantalla gráfica que está diseñado para reemplazar el componente de gráficos del protocolo de RDP tradicional. Utiliza los recursos de aceleración de hardware de la GPU del servidor para codificar los contenidos de la pantalla a través del códec RemoteFX y para enviar las actualizaciones de pantalla al cliente de RDP. RemoteFX utiliza tecnologías avanzadas de canalización y gráficos adaptables para asegurarse de ofrecer la mejor experiencia posible según el tipo de contenido, la CPU y la disponibilidad de ancho de banda de red, así como la velocidad de la renderización.

RemoteFX está activado de forma predeterminada. El administrador o el usuario no deben cambiar ningún ajuste para activarlo. El cliente de RDP negocia con cualquier servidor de RDP con el que se comunique y, si RemoteFX está disponible, se utilizará.

NOTA: Para obtener más información, consulte el informe técnico sobre HP ThinPro *«Enabling RemoteFX for RDP»* (disponible solo en inglés).

Sesiones con varios monitores de RDP

No se requiere una configuración especial para compatibilidad real con varios monitores. El cliente RDP identifica automáticamente cuál es el monitor especificado como principal en los ajustes locales y coloca los iconos de la barra de tareas y el escritorio en ese monitor. Cuando una ventana se maximiza en la sesión remota, la ventana solo cubre al monitor en el que se maximizó.

Las preferencias de video y las resoluciones del monitor pueden verse pero no modificarse en la sesión remota. Para modificar la resolución de la sesión, cierre la sesión y cambie la resolución en el thin client local.

De forma predeterminada, todas las sesiones de RDP serán en pantalla completa y cubrirán todos los monitores para mejorar la experiencia de virtualización. Hay opciones de ventana adicionales disponibles en el Administrador de conexión RDP.

NOTA: Es posible que las sesiones del Host de virtualización de escritorio remoto (RDVH) con soporte para tarjeta de gráficos solo admitan ciertas resoluciones y cantidad de monitores. Los límites se especifican cuando se configura el dispositivo de gráficos virtual RemoteFX para la máquina virtual RDVH.

NOTA: Para obtener más información acerca de RDP, consulte el informe técnico sobre HP ThinPro *«True Multi-Monitor Mode for RDP»* (disponible solo en inglés).

Redirección de multimedia de RDP

La redirección de multimedia (MMR) es una tecnología que se integra con Windows Media Player en el host remoto y transmite el contenido multimedia codificado al cliente de RDP en lugar de reproducirlo en el host remoto y de volver a codificarlo a través de RDP. Esta tecnología reduce el tráfico de la red y la carga del servidor y mejora en gran medida la experiencia multimedia, permitiendo la reproducción a 24 fps de videos 1080p con sincronización de audio automática. MMR está activado de forma predeterminada. El cliente de RDP negociará con cualquier servidor de RDP con el que se comunique y, si MMR está disponible, se utilizará.

MMR también utiliza un esquema avanzado de detección de códecs que identifica si el thin client admite el códec solicitado por el host remoto antes de intentar redirigirlo. El resultado es que solo los códecs compatibles serán redirigidos y todos los códecs no compatibles pasan a la renderización del lado del servidor.

SUGERENCIA: Para permitir una administración simplificada, HP recomienda que MMR se active o desactive en el host remoto.

Redirección de dispositivo de RDP

La redirección de dispositivos garantiza que cuando un usuario conecta un dispositivo en el thin client, el dispositivo se detecta automáticamente y se puede acceder a él en la sesión remota. RDP admite la redirección de muchos tipos de dispositivos distintos.

Redirección de USB de RDP

La redirección USB funciona al transmitir mediante la red las llamadas del protocolo USB de bajo nivel al host remoto. Cualquier dispositivo USB conectado al host local aparece dentro del host remoto como un dispositivo USB nativo, como si estuviera conectado localmente. Los controladores estándar de Windows admiten el dispositivo en la sesión remota y todos los tipos de dispositivos son compatibles sin necesidad de controladores adicionales en el thin client.

No todos los dispositivos se establecen para redirigir USB de forma predeterminada. Por ejemplo, los teclados, el mouse y los otros dispositivos de entrada USB generalmente no están configurados para redirigirse, ya que la sesión remota espera que la entrada de información proceda del thin client. Es posible

que algunos dispositivos, por ejemplo los de almacenamiento masivo, las impresoras y los dispositivos de audio, utilicen opciones adicionales para la redirección.

Tenga en cuenta la siguiente información adicional acerca de la redirección USB con RDP:

- El servidor debe admitir la redirección USB para que esté disponible para el thin client. Los servidores RDVH con RemoteFX, Windows 8, Windows 10, Windows Server 2012 y Windows Server 2016 admiten la redirección USB para fines generales.
- El protocolo en el Administrador de USB en el Panel de control debe configurarse como RDP.
- Para las conexiones RDP, los controles en el Administrador de USB determinan si un dispositivo USB se puede redireccionar. Los ajustes para la conexión individual determinan cómo se redirecciona un dispositivo USB.

Redirección de almacenamiento masivo en RDP

De forma predeterminada, la sesión de RDP redirige todos los dispositivos de almacenamiento masivo al host remoto mediante la redirección de unidades de alto nivel. Cuando un dispositivo como una unidad flash USB, una unidad DVD-ROM USB o una unidad de disco duro externo USB está conectado al thin client, éste detecta y monta la unidad en el sistema de archivos local. Luego, RDP detecta una unidad montada y la redirige al host remoto. Dentro del host remoto aparecerá como una nueva unidad de disco en Windows Explorer, con el nombre `<etiqueta del dispositivo> en <nombre de host del cliente>`; por ejemplo, `Bill_USB on HP04ab598100ff`.

Hay tres restricciones a este tipo de redirección.

- El dispositivo no aparecerá en la barra de tareas en el host remoto con un icono para expulsar el dispositivo. Debido a esto, asegúrese de dar al dispositivo una cantidad de tiempo suficiente para sincronizar los datos después una copia antes de retirar el dispositivo para asegurarse de que el dispositivo no resulte dañado. Normalmente, menos de un segundo es necesario después de que finalice el diálogo de copia de archivos, pero hasta 10 segundos podrían ser necesarios en función de la velocidad de escritura del dispositivo y la latencia de la red.
- Se montarán solo los sistemas de archivos compatibles con el thin client. Los sistemas de archivos compatibles son FAT32, NTFS, ISO9660 (CD-ROM), UDF (DVD-ROM) y ext3.
- El dispositivo se tratará como un directorio; las tareas comunes de la unidad como el formateo y la modificación de la etiqueta de disco no estarán disponibles.

La redirección USB de dispositivos de almacenamiento puede desactivarse en los ajustes individuales de una conexión. Si lo desea, puede desactivar la redirección de almacenamiento masivo por completo. Para ello, apague la redirección USB y luego cambie las claves de registro como se describe en la siguiente tabla.

Tabla 5-19 Redirección de almacenamiento masivo en RDP

Entrada de registro	Valor por establecer	Descripción
root/USB/root/holdProtocolStatic	1	Asegúrese de que el tipo de USBR no se cambiará automáticamente cuando se activa o desactiva una conexión
root/USB/root/protocol	local	Asegúrese de que la conexión RDP no intenta redirigir ningún dispositivo a la sesión remota

Para desactivar por completo que se monten dispositivos de almacenamiento masivo USB o para desactivar la redirección de dispositivos de almacenamiento masivo USB pero permitir que se redireccionen otros

dispositivos, en el sistema de archivos del thin client, elimine la regla udev `/etc/udev/rules.d/010_usbdrive.rules`.

Redirección de impresora de RDP

De forma predeterminada, RDP dispone de dos métodos de redirección de impresora activados:

- **Redirección de USB**: cualquier impresora USB conectada al dispositivo se mostrará como impresora local en la sesión remota. El proceso de instalación estándar de la impresora debe realizarse en la sesión remota si la impresora no está instalada en ese host remoto. No hay ningún ajuste que administrar localmente.
- **Redirección de alto nivel**: si la redirección de USB no está disponible en el host remoto o la impresora es una impresora en serie o paralela, utilice la redirección de alto nivel. Configure la impresora para que use una cola de impresión de la impresora local y el cliente de RDP configurará automáticamente una impresora remota que envía comandos de cola de impresión a través de un canal virtual desde el host remoto hasta el thin client.

  Si no se ha especificado ningún controlador, se usa un controlador de postscript genérico, pero podría haber disponibles recursos de impresión adicionales si la impresora se configura localmente con un controlador específico de Windows. Este controlador de Windows debe coincidir con el controlador que la impresora utilizaría cuando se conecta localmente a un sistema operativo Windows. Esta información se suele encontrar en **Modelo**, en las propiedades de la impresora.

NOTA: Consulte Configuración de impresora en serie o paralela en la página 90 para obtener más información.

Redirección de audio de RDP

De forma predeterminada, la redirección de audio de alto nivel redirigirá el audio desde el host remoto hasta el thin client. Es posible que necesite configurar el control de voz básico. Además, RDP 7.1 contiene una serie de recursos avanzados de redirección de audio que podrían requerir una configuración adicional.

Consulte las siguientes notas sobre el uso de redirección de audio con RDP:

- RDP ofrece la máxima calidad de audio que permita el ancho de banda. RDP reduce la calidad audio para reproducir en conexiones con poco ancho de banda.
- No hay mecanismos de sincronización de audio o vídeo nativos disponibles en RDP. Es posible que los videos más largo no se sincronicen con el audio. MMR o Remotefx puede resolver este problema.
- HP recomienda la redirección de audio de alto nivel, pero la redirección USB de dispositivos audio es posible si hay funciones adicionales, como un control de volumen digital. La redirección de alto nivel solo está disponible para dispositivos analógicos.
- La redirección del micrófono está activada de forma predeterminada. Es posible que deba ajustar el volumen predeterminado del micrófono en el thin client. Se deben modificar los ajustes de los servidores Windows RDP más antiguos para permitir la entrada de audio.
- Tanto la configuración local como la remota afectarán al volumen final. HP recomienda configurar el volumen local al máximo y ajustar el volumen en el host remoto.

Redirección de smart card de RDP

Para activar el inicio de sesión de smartcard para una conexión RDP:

De forma predeterminada, las smartcards se redirigirán mediante redirección de alto nivel. Esto permite usarlas para ingresar a la sesión y a otras aplicaciones remotas.

▲ Seleccione **Usar smart card predefinida** en el Administrador de conexión RDP.

Esto permitirá que el usuario se conecte sin especificar antes las credenciales. El cliente RDP iniciará la sesión RDP y se le solicitará al usuario la autenticación con smartcard.

Esta tecnología requiere controladores para el lector de smart card que se va a instalar en el thin client. De forma predeterminada, los controladores CCID y Gemalto están instalados, lo que agrega compatibilidad con la mayoría de los lectores de smart card disponibles. Puede instalar controladores adicionales agregándolos a `a/usr/lib/pkcs11 /.`

NOTA: Cuando el inicio de sesión de smart card está activado, no se admite la autenticación a nivel de red y se desactiva automáticamente.

VMware Horizon View

Ajustes de VMware Horizon View por conexión

La siguiente sección describe las configuraciones disponibles en las diversas categorías al editar la conexión VMware Horizon View.

NOTA: Estos ajustes afectan solo la conexión que está configurando en ese momento.

Red

La siguiente tabla describe los ajustes disponibles en la categoría Red al editar una conexión VMware Horizon View.

Tabla 5-20 Red

Opción	Descripción
Nombre	Escriba un nombre para esta conexión.
Dirección	Escriba el nombre de host o dirección IP de un servidor de VMware Horizon View.
Credenciales	• **Iniciar sesión de forma anónima con acceso no autenticado** • **Usar credenciales de inicio de sesión único**: las credenciales usadas en el inicio de sesión también se usan para empezar la conexión. • **Pedir credenciales en el inicio de la conexión**: no hay componentes de credencial suministrados previamente. • **Usar usuario, contraseña y/o dominio predefinidos**: algunas o todas las credenciales se almacenan y suministran para la conexión. • **Usar smart card predefinida**: se espera que se use la conexión con una smart card para la autenticación.
Usuario	Escriba el nombre de usuario que utilizará para la conexión.
Contraseña	Escriba la contraseña que utilizará para la conexión.
Dominio	Escriba el dominio que utilizará para la conexión.

General

La siguiente tabla describe los ajustes disponibles en la categoría General al editar una conexión VMware Horizon View.

Tabla 5-21 General

Opción	Descripción
Habilitar MMR	Habilita la redirección de multimedia para las conexiones BLAST y PCoIP. **NOTA:** HP recomienda deshabilitar esta opción. En el caso de las conexiones hechas con el protocolo RDP, use la opción Habilitar redirección de multimedia. Consulte Opciones RDP en la página 34.
Habilitar la conexión automática de USB al insertarla	Habilita la redirección del dispositivo USB cuando se inserta un dispositivo USB.
Habilitar la conexión automática de USB al inicio	Habilita la redirección del dispositivo USB cuando se inicia una conexión VMware View.
Enviar Ctrl + Alt + Supr al escritorio virtual	Habilita el envío de Ctrl + Alt + Supr al escritorio virtual directamente.
Permitir que se compartan los datos del Horizon Client	Si su administrador de Horizon optó por participar en el programa de mejoría de la experiencia del cliente, VMware recopila y recibe datos anónimos en los sistemas clientes para priorizar la compatibilidad de hardware y software.
Habilitar la redirección de la unidad cliente	Habilita el recurso de carpeta compartida para las conexiones BLAST y PCoIP. Esta opción está habilitada de forma predeterminada.
No inicia la aplicación maximizada	Si está activada, las aplicaciones no se inician en ventanas maximizadas.
Inicio de sesión automático	Cuando está habilitado, el usuario inicia sesión automáticamente cuando se establece la conexión. **NOTA:** HP recomienda habilitar esta opción.
Paquete de virtualización para Skype Empresarial	Habilita la virtualización de Skype Empresarial. **NOTA:** Las llamadas de video podrían usar la mayoría de la potencia de procesamiento de un thin client. HP recomienda deshabilitar esta opción.
Escritorio predeterminado	Especifica que un escritorio se inicie automáticamente cuando se abre una conexión VMware Horizon View.
Protocolo preferido	Le permite seleccionar PCoIP, RDP o BLAST como protocolo preferido o elegir seleccionar el protocolo más tarde.
Tamaño de la aplicación	Ajusta el tamaño de ventana de la aplicación. Puede seleccionar **Todos los monitores**, **Pantalla completa**, **Ventana grande** o **Ventana pequeña**.
Tamaño del escritorio	Ajusta el tamaño de la ventana del escritorio. Puede seleccionar **Todos los monitores**, **Pantalla completa**, **Ventana grande** o **Ventana pequeña**.
Impresoras	Controla la forma en que se maneja la redirección de la impresora: • **ThinPrint**: comparte impresoras mediante la redirección de alto nivel. • **Redirección de USB** • **Deshabilitar** **NOTA:** En el caso de las conexiones realizadas con el protocolo RDP, consulte Redirección de impresora de RDP en la página 31.

Seguridad

La siguiente tabla describe los ajustes disponibles en la categoría Seguridad al editar una conexión VMware Horizon View.

Tabla 5-22 Seguridad

Opción	Descripción
Close After Disconnect (Cerrar tras desconectar)	Hace que el cliente de VMware Horizon View se cierre automáticamente después de que los usuarios terminan la sesión en sus escritorios o si la sesión se termina a causa de un error. Esta opción es un recurso de seguridad diseñada para que el usuario no tenga que dar un paso adicional para cerrar sesión totalmente después de que haya terminado con su sesión de escritorio. Esta opción está activada de forma predeterminada por razones de seguridad, pero puede desactivarse si los usuarios cambian a menudo a un nuevo grupo de escritorio después cerrar una sesión y no desean volver a pasar por el proceso de inicio sesión completo.
Ocultar barra de menú superior	La barra de menú superior se torna invisible para los usuarios. Esta opción esta activada de forma predeterminada. Puede desactivarla si los usuarios prefieren acceder a las opciones de tamaño de ventana o selección de grupo de escritorio en una sesión de VMware Horizon View.
Evitar que los usuarios cambien la dirección del servidor	Si está activado, los usuarios finales no pueden cambiar la dirección del servidor.
Habilitar el monitor de roaming de la sesión	Cierra la conexión si la sesión realiza roaming desde otro cliente. Esta opción solo se admite en las conexiones PCoIP.
Política de verificación de certificados	Seleccione una de las siguientes opciones: • **Permitir todas las conexiones** • **Advertencia** • **Rechazar las conexiones inseguras**

Opciones RDP

La siguiente tabla describe los ajustes disponibles en la categoría Opciones RDP al editar una conexión VMware Horizon View.

Tabla 5-23 Opciones RDP

Opción	Descripción
Permitir eventos de movimiento	Permite eventos de movimiento para esta conexión.
Permitir compresión de datos	Utiliza compresión de datos para esta conexión.
Activar la encriptación RDP anterior	Permite encriptación para esta conexión.
Activar caché fuera de pantalla	Si está activado, se utiliza la memoria fuera de pantalla para guardar en caché los mapas de bits.
Conectar a la consola de administrador	Establece la conexión con el puerto de consola de administrador.
Copiar/pegar entre sesiones	Si está activado, las opciones copiar y pegar están activadas entre diferentes sesiones RDP.

Tabla 5-23 **Opciones RDP (continúa)**

Opción	Descripción
Activar el almacenamiento en memoria intermedia de los primitivos de RDP6	Si está activado, el rendimiento de gráficos que no son RemoteFX aumenta al costo de actualizaciones de pantalla menos frecuentes.
Habilitar el códec Progressive RemoteFX	Habilita el códec Progressive RemoteFX, que transmite el escritorio en una serie de imágenes cada vez más nítidas.
Habilitar redirección de contenido multimedia	Permite que se envíen archivos multimedia directamente al cliente para reproducción local. Para obtener más información, consulte Redirección de multimedia de RDP en la página 29.
Versión de TLS	Establece la versión de Transport Layer Security que se va a usar durante las fases iniciales de negociación con el servidor RDP. Establézcala de forma que coincida con la versión de TLS utilizada por su servidor RDP, o trate de establecerla en **auto**. **NOTA:** Hay algunos defectos del lado del servidor en ciertos servidores RDP sin parches que pueden hacer que el ajuste automático falle, de forma que no sea el ajuste predeterminado.
Enviar nombre de host como	Con referencia al licenciamiento por dispositivo, esto selecciona la forma en que se envía el nombre de host del cliente al servidor de RDP. Seleccione **nombre de host** o **mac**.
Nombre de host que se va a enviar	Normalmente, el nombre de host del thin client se utiliza para las Licencias de acceso de cliente. Este campo permite enviar un valor distinto. **SUGERENCIA:** Seleccione el icono **(i)** al lado de esta opción para obtener más información.
Información de equilibrio de carga	Utilice esta opción con una conexión RDP intermediada. **SUGERENCIA:** Seleccione el icono **(i)** al lado de esta opción para obtener más información.
Sonido de equipo remoto	Especifica dónde debe reproducirse el sonido del equipo remoto (de forma local o remota) o si no se debe reproducir en absoluto.
Activa la asignación de puerto	Asigna los puertos en serie y paralelos del thin client a la sesión remota.
Activa la asignación de impresora	Asigna la cola de la impresora local a la sesión remota. Utilice esta opción si la redirección USB no está disponible en el host remoto o si la impresora es una impresora en serie o paralela. Configure la impresora para que use una cola de impresión de la impresora local y el cliente de VMware Horizon View configurará automáticamente una impresora remota que envía comandos de cola de impresión a través de un canal virtual desde el host remoto hasta el thin client. Este método requiere configurar la impresora en el thin client y especificar un controlador de Windows en el thin client debido a que el cliente de VMware Horizon View necesita especificar al host remoto cuál controlador va a utilizar para la impresora remota. Este controlador de Windows debe coincidir con el controlador que la impresora utilizaría cuando se conecta localmente a un sistema operativo Windows. Esta información se suele encontrar en **Modelo**, en las propiedades de la impresora.
Carpetas compartidas	**Agregar**, **Eliminar** o **Editar** carpetas compartidas.

Experiencia RDP

La siguiente tabla describe los ajustes disponibles en la categoría Experiencia RDP al editar una conexión VMware Horizon View.

Tabla 5-24 **Experiencia RDP**

Opción	Descripción
Seleccione su velocidad de conexión para optimizar el rendimiento	Si selecciona una velocidad de conexión (**LAN**, **Banda ancha** o **Módem**) activará o desactivará las siguientes opciones para optimizar el rendimiento: • **Segundo plano de escritorio** • **Suavizado de fuentes** • **Composición del escritorio** • **Mostrar el contenido de la ventana mientras se arrastran elementos** • **Animación de menús y ventanas** • **Temas** Al seleccionar **Ajustes preferidos del cliente**, el cliente de VMware Horizon View puede elegir qué opciones utilizar. También puede seleccionar su propia combinación personalizada de opciones.
Supervisión del estado de la conexión de extremo a extremo	Seleccione esta alternativa para activar las opciones de intervalo de espera.
Intervalo de Advertencia	Especifica la cantidad de tiempo en segundos después de recibir el último tráfico de red desde el servidor antes de que se advierta al usuario que se perdió la conexión. Puede desactivar esta función si no selecciona la opción o define la hora en cero. Con la opción **Mostrar el diálogo de advertencia** seleccionada, se mostrará un cuadro de diálogo de advertencia cuando se alcanza el intervalo de espera. De lo contrario, la advertencia solo se escribe en el registro de la conexión. **SUGERENCIA:** HP recomienda que aumente el valor del tiempo de espera para redes con períodos muy ocupados o interrupciones momentáneas frecuentes.
Tiempo de espera hasta recuperación	Especifica la cantidad de tiempo en segundos después de recibir el último tráfico de red del servidor que el cliente de RDP espera para que se recupere la conexión sin realizar ninguna acción especial. Al final de este período, el cliente de RDP intenta una reconexión rápida con la sesión.
Intervalo de Error	Especifica la cantidad de tiempo en segundos después de recibir el último tráfico de red del servidor que el cliente de RDP espera antes de dejar de intentar conectarse con ese servidor. **SUGERENCIA:** Seleccione el icono **?** al lado de este campo para obtener más información.

Avanzado

Esta sección menciona dónde puede encontrar información sobre las configuraciones de conexión avanzada, en la categoría Avanzado, al editar una conexión.

NOTA: Consulte Ajustes de conexión avanzada en la página 13 para obtener información sobre los ajustes disponibles en la categoría Avanzado al editar una conexión.

Sesiones con varios monitores de VMware Horizon View

VMware Horizon View admite sesiones con varios monitores. Para mejorar la experiencia de virtualización, las sesiones de VMware Horizon View predeterminadas usan pantalla completa y abarcan todos los monitores. Para elegir un tamaño de ventana diferente, seleccione **Pantalla completa: todos los monitores** en el tipo de protocolo del grupo de escritorio para la conexión y luego elija otra opción de la lista de tamaños de ventana. La siguiente vez que se conecte a una sesión se abre la ventana en el tamaño seleccionado.

Accesos directos del teclado de VMware Horizon View

Accesos directos de teclado de Windows

A fin de ayudar a administrar los sistemas Windows, VMware Horizon View admite accesos directos de teclado de Windows. Por ejemplo, cuando se utiliza Ctrl+Alt+Supr, VMware Horizon View muestra un mensaje que ofrece las siguientes opciones:

- Enviar un comando **Ctrl+Alt+Supr**.
- Desconectar la sesión: use esta opción cuando no tiene otra forma de poner fin a la sesión.

Los accesos directos de teclado de Windows se enviarán a la sesión de escritorio remota. De esta forma, los accesos directos del teclado local, como Ctrl+Alt+Tab y Ctrl+Alt+F4, no funcionarán dentro de la sesión remota.

SUGERENCIA: Para que pueda alternar las sesiones, desactive la opción **Ocultar barra de menú superior** en el Administrador de conexión VMware Horizon View o mediante la clave de registro `root/ConnectionType/view/connections/<UUID>/hideMenuBar`.

Teclas multimedia

VMware Horizon View utiliza las teclas multimedia para controlar opciones como el volumen, reproducir/pausa y silencio durante una sesión de escritorio remoto. Esto es compatible con programas multimedia como Windows Media Player.

Redirección de dispositivo de VMware Horizon View

Redirección de USB de VMware Horizon View

Para habilitar USBR para las conexiones de VMware Horizon View, seleccione **VMware Horizon View** como protocolo remoto en el Administrador de USB.

Para obtener más información sobre USBR, incluida la redirección de dispositivos y específica de clase, consulte Redirección de USB de RDP en la página 29.

Redirección de audio de VMware Horizon View

Si no necesita la capacidad de grabación de audio, utilice la redirección de audio de alto nivel. El audio se reproducirá a través del conector de 3,5 mm o, de forma predeterminada, un set de auriculares y micrófono USB si están conectados. Utilice el administrador de audio local para ajustar el nivel de entrada/salida, seleccione reproducir y capture los dispositivos.

El cliente VMware Horizon View solo admite la redirección de la grabación de audio de alto nivel mediante el tipo de conexión PCoIP en las unidades x86 cuando se conecta a un servidor que ejecuta VMware Horizon View 5.2 Feature Pack 2 o superior; o el tipo de conexión BLAST en las unidades x86 cuando se conecta a un servidor que ejecuta VMware Horizon View 7.x o superior. Si necesita grabación de audio y está utilizando una configuración diferente, use uno de los siguientes métodos:

- Si su sistema utiliza VMware Horizon View Client 1.7 o superior, utilice el protocolo RDP para permitir la redirección de audio de alto nivel mediante el conector de 3,5 mm o un set de auriculares y micrófono USB.

NOTA: Para utilizar la redirección de grabación de audio de alto nivel mediante el protocolo RDP, el servidor debe admitirlo y debe estar configurado para permitir grabación de audio a través de una sesión remota. El servidor debe ejecutar Windows 7 o superior. También debe asegurarse de que la

clave de registro `HKLM\SYSTEM\CurrentControlSet\control\Terminal Server\Winstation\RDP-TCP\fdisableaudiocapture` esté ajustada en `0`.

- Si tiene un set de auriculares con micrófono USB, puede utilizar USBR. Establezca que el set de auriculares y micrófono USB se redirija a la sesión. El set de auriculares y micrófono se mostrará como un dispositivo de audio. De forma predeterminada, los dispositivos de audio USB no se redirigen y el cliente de VMware Horizon View utiliza redirección de audio de alto nivel. Para redirigir el set de auriculares y micrófono USB, utilice el Administrador de USB del thin client y seleccione el set de auriculares y micrófono USB que desea redirigir. Asegúrese de que **VMware Horizon View** esté seleccionado como el protocolo USBR y de que el set de auriculares y micrófono esté marcado en los dispositivos que se van a redirigir.

NOTA: VMware y HP no recomiendan utilizar USBR para el set de auriculares. Se requiere un gran ancho de banda de red para transmitir datos de audio en el protocolo USBR. Además, es posible que experimente audio de mala calidad con este método.

Redirección de smart card de VMware Horizon View

Para utilizar una smart card para iniciar la sesión en el servidor de VMware Horizon View:

1. Asegúrese de que el inicio de sesión de smartcard está activado en el Administrador de conexión VMware Horizon View.

   Después de iniciar la conexión, el cliente de VMware Horizon View mostrará una lista de credenciales del servidor.

2. Para desbloquear las credenciales y acceder al servidor de VMware Horizon View Manager, escriba el PIN correspondiente para el servidor.

NOTA: Después de proporcionar el PIN correcto, las credenciales del usuario se utilizarán para iniciar la sesión en el servidor de VMware Horizon View Manager. Consulte la documentación de VMware Horizon View para obtener más información acerca de cómo configurar el servidor para admitir el inicio de sesión con smart card. Siempre que el servidor esté configurado para permitir inicio de sesión con smart card, las credenciales del usuario pasarán y se iniciará sesión en el escritorio sin tener que introducir el PIN de nuevo.

NOTA: Para iniciar sesión en el servidor de administrador de VMware Horizon View Manager con una smart card, el controlador de smart card local debe estar instalado en el thin client. Consulte Redirección de smart card de RDP en la página 31 para obtener más información sobre la instalación del controlador de la smart card. Una vez iniciada la sesión en el host remoto, la smart card pasará al host remoto mediante un canal virtual, no USBR. Esta redirección del canal virtual garantiza que la smart card pueda utilizarse para realizar tareas como la firma de correo electrónico, el bloqueo de pantalla y así sucesivamente. No obstante, podría causar que la smart card no se muestre como un dispositivo de smart card en el administrador de dispositivos de Windows.

NOTA: El host remoto debe tener los controladores de smart card adecuados instalados.

Redirección de cámara web de VMware Horizon View

El cliente de VMware Horizon View admite la redirección de cámara web de alto nivel solo a través de RTAV en unidades x86 conectadas a un servidor back-end que ejecuta VMware Horizon View 5.2 Pack 2 o superior.

Otros métodos de conexión no admiten la redirección de cámara web de alto nivel y pueden redireccionar cámaras web solo mediante USBR. De acuerdo con pruebas y validaciones internas, HP ha descubierto que el rendimiento de una cámara web conectada a través de USBR básica no funciona correctamente. HP no recomienda el uso de esta configuración y sugiere que los clientes que requieran esta función prueben usar las unidades x86 con tecnología RTAV para asegurar un buen nivel de rendimiento. Es posible que al utilizar

USBR, la cámara web funcione de manera deficiente o que directamente no funcione. Consulte Redirección de USB de RDP en la página 29 para obtener más información.

Redirección de puerto COM de VMware Horizon View

Para habilitar la redirección de puerto COM para la conexión VMware Horizon View:

▲ Establezca `root/ConnectionType/view/general/enableComPortRedirection` en 1 en regeditor.

NOTA: De forma predeterminada, esta configuración está habilitada.

Cambio del protocolo de VMware Horizon View

VMware Horizon View Client puede usar el protocolo PCoIP, RDP o BLAST.

Para cambiar el protocolo:

1. En VMware Horizon View Client, seleccione un grupo que admita uno de los protocolos admitidos.
2. En el menú **Conexión**, seleccione **Ajustes**.
3. Cambie el protocolo utilizando el cuadro desplegable al lado de **Conectarse mediante**.

NOTA: Use VMware Horizon View Manager para establecer cuál protocolo se debe usar para cada grupo de escritorio.

SUGERENCIA: HP recomienda utilizar el protocolo PCoIP para mejorar la experiencia de escritorio. Sin embargo, el protocolo RDP ofrece más opciones de personalización y puede funcionar mejor en conexiones más lentas.

Requisitos de HTTPS y gestión de certificados de VMware Horizon View

VMware Horizon View Client 1.5 and VMware Horizon View Server 5.0 y posteriores requieren HTTPS. De forma predeterminada, el cliente de horizonte de VMware Horizon View advierte sobre los certificados del servidor que no son de confianza, como los autofirmados (por ejemplo el certificado predeterminado de VMware Horizon View Manager) o los certificados caducados. Si un certificado está firmado por una autoridad certificadora (AC), y la AC es de confianza, la conexión indicará un error y al usuario no se le permitirá conectarse.

HP recomienda el uso de un certificado firmado verificado por una AC raíz de confianza estándar en el servidor de VMware Horizon View Manager. De este modo se garantiza que los usuarios puedan conectarse al servidor sin que tengan que realizar ninguna configuración. Si utiliza una AC interna, la conexión del cliente de VMware Horizon View indica un error hasta que se realice una de las tareas siguientes:

- Utilice el Administrador de certificados para importar el certificado desde un archivo o URL.
- Utilice una actualización de perfil remoto para importar un certificado.
- En el Administrador de conexión VMware Horizon View, establezca el **Nivel de seguridad de conexión** como **Permitir todas las conexiones**.

La siguiente tabla describe la confianza del certificado cuando el nivel de seguridad se establece como **Rechazar conexiones inseguras**.

Tabla 5-25 Rechazar las conexiones inseguras

Confianza del certificado	Resultado
De confianza	De confianza
Autofirmado	Error
Expirado	Error
No confiable	Error

La siguiente tabla describe la confianza del certificado cuando el nivel de seguridad se establece como **Advertir**.

Tabla 5-26 Advertencia

Confianza del certificado	Resultado
De confianza	De confianza
Autofirmado	Advertencia
Expirado	Advertencia
No confiable	Error

La siguiente tabla describe la confianza del certificado cuando el nivel de seguridad se establece como **Permitir todas las conexiones**.

Tabla 5-27 Permitir todas las conexiones

Confianza del certificado	Resultado
De confianza	De confianza
Autofirmado	No confiable
Expirado	No confiable
No confiable	No confiable

La siguiente tabla describe el comportamiento de la conexión asociado con cada resultado.

Tabla 5-28 Comportamiento de la conexión

Resultado	Descripción
De confianza	Se conecta sin un diálogo de advertencia de certificado y muestra un icono de bloqueo verde
No confiable	Se conecta sin un diálogo de advertencia de certificado y muestra un icono de desbloqueo rojo
Advertencia	Se conecta con un diálogo de advertencia de certificado y muestra un icono de desbloqueo rojo
Error	No permite la conexión

Navegador web

Configuraciones de Web Browser por conexión

La siguiente sección describe las configuraciones disponibles en las diversas categorías al editar la conexión de Web Browser.

NOTA: Estos ajustes afectan solo la conexión que está configurando en ese momento.

Configuración

La siguiente tabla describe las configuraciones disponibles en la categoría Configuración al editar los ajustes generales de Web Browser.

Tabla 5-29 Configuración

Opción	Descripción
Nombre	El nombre de la conexión.
URL	La URL para la conexión.
Uso previsto	Le permite especificar cómo se realiza la redirección de USB cuando se inicia la conexión Web Browser. Seleccione **Citrix**, **RDP** o **Internet**.
Permitir el inicio de sesión con una smart card	La permite usar la autenticación de smart card para una conexión si selecciona una URL o un icono que inicia una conexión remota.
Habilitar modo de quiosco	Activa el modo quiosco.
Habilitar pantalla completa	Utiliza el modo de pantalla completa para la conexión.
Habilitar cuadro de diálogo de impresión	Activa el cuadro de diálogo de impresión.

Preferencias

Use estas opciones para configurar Web Browser. Estas opciones pueden compartirlas varias conexiones Web Browser o pueden ser específicas para una sola conexión.

Avanzado

Esta sección menciona dónde puede encontrar información sobre las configuraciones de conexión avanzada, en la categoría Avanzado, al editar una conexión.

NOTA: Consulte Ajustes de conexión avanzada en la página 13 para obtener información sobre los ajustes disponibles en la categoría Avanzado al editar una conexión.

AVD (Azure Virtual Desktop)

Azure Virtual Desktop (Escritorio virtual Azure) forma parte del sistema Microsoft Azure® y brinda acceso a escritorios remotos y aplicaciones remotas basadas en la nube. El cliente de AVD para ThinPro es un complemento que puede obtener de ThinUpdate o Easy Update. Reinicie después de instalar AVD para crear

conexiones AVD. Además de AVD, el cliente AVD también admite Windows 365®. Para ver el complemento de optimización de Zoom UC para ThinPro, visite el sitio web de Zoom.

Ajustes por conexión AVD

Esta sección describe la configuración de AVD por conexión.

NOTA: Estos ajustes solo afectan la conexión que está configurando en un determinado momento.

Configuración

La siguiente tabla describe las configuraciones disponibles en la categoría **Configuración** cuando edita una conexión AVD.

Tabla 5-30

Opción	Descripción
Nombre	El nombre de la conexión.
URL de Workspace	La URL para la conexión. Por ejemplo, https://rdweb.wvd.microsoft.com/api/arm/feeddiscovery.
Credenciales	• Pedir credenciales en el inicio de la conexión. • Usar usuario, contraseña y dominio predefinidos.
Nombre de usuario	El nombre de usuario para esta conexión.
Contraseña	La contraseña de esta conexión.
Dominio	El dominio de esta conexión.

Ventana

La siguiente tabla describe los ajustes disponibles en la categoría **Ventana** al editar una conexión AVD.

Tabla 5-31

Opción	Descripción
Tamaño de Ventana	Establece el tamaño de la ventana en una de las siguientes opciones: **Escritorio completo**: La sesión remota se inicia en modo de pantalla completa y cubre todos los monitores que están conectados al cliente. **Pantalla completa**: La sesión remota se inicia en modo de pantalla completa solo en la pantalla primaria. **Maximizado**: La sesión remota se inicia en modo de pantalla completa solo en la pantalla primaria, dejando espacio para la barra de tareas. Si selecciona **Ocultar la decoración de la ventana**, se eliminarán todas las decoraciones de ventanas de tamaño fijo, lo que incluye la barra de título y los bordes de la ventana. **Fijo**: La sesión remota se inicia con una ventana de tamaño fijo.

Tabla 5-31

Opción	Descripción
	Ancho/fijo: Establece el tamaño fijo del ancho de la ventana de sesión. **Altura/fija:** Establece el tamaño fijo de la altura de la ventana de sesión.

NOTA: Abre aplicaciones remotas de AVD en una sola ventana de ThinPro. Puede minimizar o cambiar el tamaño de las aplicaciones dentro de esta ventana. Use Alt+Tab para pasar por las aplicaciones activas.

Opciones

La siguiente tabla describe los ajustes disponibles en la categoría Opciones cuando edita una conexión AVD.

Tabla 5-32 **Opciones de conexión AVD y sus descripciones**

Opción	Descripción
Autorrellenar credenciales	Rellena automáticamente las credenciales en la página de inicio de sesión.
Modo sin cabeza	Rellena automáticamente las credenciales en la página de inicio de sesión oculta.
Recordar	Crea una caché de token cifrada para que no se requiera un diálogo de autenticación web en cada inicio.
Olvidar	Borra la caché de token cifrada que se crea al seleccionar **Recordar**.
Espacio de trabajo para inicio automático	Especifica el espacio de trabajo desde el cual un recurso se inicia automáticamente (opcional).
Recurso de inicio automático	Especifica el nombre de un recurso que se iniciará automáticamente.
Cerrar la ventana de Feed AVD automáticamente	Cierra la venta de feed AVD de forma automática cuando se cierra la ventana de una sesión.
Establecer zona horaria local	Establece la zona horaria de sesión remota con la zona horaria del sistema.
Desactivar la barra de menús	Desactiva la barra de menús en la ventana de la sesión.
Desactivar la barra de menú desplegable	Desactiva la barra de menú desplegable que aparece cuando la ventana de la sesión está en pantalla completa.
Botón Cerrar	Active el botón **Cerrar** en la barra desplegable.
Botón Minimizar	Active el botón Minimizar en la lista desplegable.
Botón Maximizar	Active el botón Maximizar en la lista desplegable.
Ctrl+Alt+D	Agregue Ctrl+Alt+Supr a la lista de accesos directos de teclado en la lista desplegable.

Recursos Locales

La siguiente tabla describe los ajustes disponibles en la categoría Recursos Locales al editar una conexión AVD.

Tabla 5-33

Opción	Descripción
Salida de audio	Determina si la salida de audio se redirige o no.
Entrada de audio	Determina si la entrada de audio se redirige o no.
Sistema de archivos	Determina si se redirige el almacenamiento extraíble.
Smart cards	Determina si se redirigen las smart cards.
Portapapeles	Determina si se redirige el portapapeles.
Complementos de canal virtual	Determina si los complementos de canal virtual están activados o desactivados. Debe estar activado para el complemento de optimización de Zoom UC.
Cámara	Determina si se redirige la cámara.

TTerm

Como TTerm no se incluye con la imagen base, debe descargarlo e instalarlo por separado.

Para instalar el paquete TTerm:

1. Descargue thinpro-tterm-<version>.xar y cópielo en ThinClient.
2. Instale el paquete .xar.
3. Reinicie.

Para configurar y utilizar la conexión TTerm:

1. Haga clic con el botón derecho en el escritorio, seleccione **Crear**, seleccione **Otro** y seleccione **TTerm**; esto creará una conexión TTerm en el escritorio.
2. Haga clic con el botón derecho en la **conexión TTerm**, seleccione **Editar** y luego edite la conexión.

Configuración

La siguiente tabla describe las configuraciones disponibles en la categoría Configuración al editar una conexión TTERM.

Tabla 5-34

Opción	Descripción
Nombre	El nombre de la conexión.
Perfil	Haga clic en **Abrir directorio de perfiles**. Abrirá **TTermLinux**. Haga clic en **Create New profile**, edite el perfil en Profile Editor y haga clic en **Save** para guardar el perfil en la base de datos tterm;
Configuración del monitor	**Pantalla completa**: TTerm se abrirá en modo de pantalla completa;

Tabla 5-34 (continúa)

Opción	Descripción
	Maximizado: TTerm se abrirá en modo maximizado.
Ver la configuración	Mostrar panel de sesión: desactívelo para ocultar el panel de sesión; actívelo para mostrar el panel de sesión.
Servidor de fuente	El servidor de fuentes no se activa a menos que la opción **Usar servidor de fuente** esté marcada.
Configurar vídeo	Seleccione para definir la configuración de la pantalla para la conexión. Si no se define esta configuración, se utilizará la configuración predeterminada.

Tipos de conexión adicionales (solo en ThinPro)

Esta sección describe las configuraciones disponibles en varias categorías al editar tipos de conexión adicionales.

NOTA: De forma predeterminada, estos tipos de conexión no están disponibles en Smart Zero. Para obtener más información, consulte Elección de una configuración de SO en la página 1.

XDMCP

La siguiente sección describe las configuraciones disponibles en las diversas categorías al editar la conexión XDMCP.

NOTA: Estos ajustes afectan solo la conexión que está configurando en ese momento.

Configuración

La siguiente tabla describe las configuraciones disponibles en la categoría Configuración al editar una conexión XDMCP.

Tabla 5-35 **Configuración**

Opción	Descripción
Nombre	El nombre de la conexión.
Tipo	El tipo de conexión XDMCP Las opciones válidas son: **selector**, **consulta** y **difusión**.
Dirección	Este valor se requiere si el valor de **Tipo** está definido para **consulta**.
Utilizar servidor de fuente	Utiliza un servidor de fuentes X remoto en lugar de fuentes instaladas localmente.
Servidor de fuente	El servidor de fuentes no se activa a menos que la opción **Usar servidor de fuente** esté marcada.
Configurar vídeo	Seleccione para definir la configuración de la pantalla para la conexión. Si no se define esta configuración, se utilizará la configuración predeterminada.

Avanzado

Esta sección menciona dónde puede encontrar información sobre las configuraciones de conexión avanzada, en la categoría Avanzado, al editar una conexión.

NOTA: Consulte Ajustes de conexión avanzada en la página 13 para obtener información sobre los ajustes disponibles en la categoría Avanzado al editar una conexión.

Secure Shell

La siguiente sección describe las configuraciones disponibles en las diversas categorías al editar la conexión Secure Shell.

NOTA: Estos ajustes solo afectan la conexión que está configurando en ese momento.

Configuración

La siguiente tabla describe las configuraciones disponibles en la categoría Configuración al editar una conexión SSH.

Tabla 5-36 Configuración

Opción	Descripción
Nombre	El nombre de la conexión.
Dirección	La dirección IP del sistema remoto.
Puerto	El puerto remoto a utilizar para la conexión.
Nombre de usuario	El nombre de usuario a utilizar para la conexión.
Ejecutar aplicación	La aplicación a ejecutar para hacer la conexión.
Compresión	Seleccione esta opción si desea comprimir los datos enviados entre el servidor y la thin client.
Reenvío de conexión X11	Si el servidor posee un servidor X dentro de él, seleccione esta opción para permitir que el usuario abra interfaces de usuario desde la sesión SSH y las exhiba localmente en la thin client.
Obligue alocación TTY	Seleccione esta opción y especifique un comando para iniciar una sesión temporal para ejecutar el comando. Cuando se complete el comando, la sesión finalizará. Si no se especifica ningún comando, la sesión se ejecutará normalmente como si la opción no se hubiese seleccionado.
Color de primer plano	El color predeterminado del texto en la sesión SSH.
Color de segundo plano	El color predeterminado de segundo plano en la sesión SSH.
Font (Fuente)	Las opciones válidas son: **7X14**, **5X7**, **5X8**, **6X9**, **6X12**, **7X13**, **8X13**, **8X16**, **9X15**, **10X20** y **12X24**.

Avanzado

Esta sección menciona dónde puede encontrar información sobre las configuraciones de conexión avanzada, en la categoría Avanzado, al editar una conexión.

NOTA: Consulte Ajustes de conexión avanzada en la página 13 para obtener información sobre los ajustes disponibles en la categoría Avanzado al editar una conexión.

Telnet

La siguiente sección describe las configuraciones disponibles en las diversas categorías al editar la conexión Telnet.

NOTA: Estos ajustes afectan solo la conexión que está configurando en ese momento.

Configuración

La siguiente tabla describe las configuraciones disponibles en la categoría Configuración al editar una conexión Telnet.

Tabla 5-37 Configuración

Opción	Descripción
Nombre	El nombre de la conexión.
Dirección	La dirección IP del sistema remoto.
Puerto	El puerto a utilizar en el sistema remoto.
Color de primer plano	El color de primer plano.
Color de segundo plano	El color de segundo plano.
Font (Fuente)	Las opciones válidas son: **7X14**, **5X7**, **5X8**, **6X9**, **6X12**, **6X13**, **7X13**, **8X13**, **8X16**, **9X15**, **10X20** y **12X24**.

Avanzado

Esta sección menciona dónde puede encontrar información sobre las configuraciones de conexión avanzada, en la categoría Avanzado, al editar una conexión.

NOTA: Consulte Ajustes de conexión avanzada en la página 13 para obtener información sobre los ajustes disponibles en la categoría Avanzado al editar una conexión.

Personalizada

Si desea instalar una aplicación personalizada de Linux®, puede usar la conexión Custom para que le permita abrir esta aplicación a través del Administrador de conexión.

NOTA: Estos ajustes afectan solo la conexión que está configurando en ese momento.

Configuración

La siguiente tabla describe las configuraciones disponibles en la categoría Configuración al editar una conexión Custom.

Tabla 5-38 Configuración

Opción	Descripción
Nombre	El nombre de la conexión.
Ingrese el comando a ejecutar	El comando a ejecutar para hacer la conexión remota.

Avanzado

Esta sección menciona dónde puede encontrar información sobre las configuraciones de conexión avanzada, en la categoría Avanzado, al editar una conexión.

NOTA: Consulte Ajustes de conexión avanzada en la página 13 para obtener información sobre los ajustes disponibles en la categoría Avanzado al editar una conexión.

6 HP True Graphics

HP True Graphics descarga el contenido multimedia pesado a la GPU del thin client, lo que brinda imágenes con gran tasa de cuadros y acelera la eficiencia.

Requisitos con respecto al servidor

Consulte en la siguiente tabla la lista de productos de servidor compatibles de proveedores de software independientes (ISV) que está usando en su infraestructura de escritorio virtual (VDI).

Tabla 6-1 Requisitos con respecto al servidor

ISV	Productos compatibles
Citrix®	XenApp®/XenDesktop® 7.0 o posterior **IMPORTANTE:** El servidor Citrix debe admitir el envío de datos de la sesión en formato H.264 (una tecnología de Citrix conocida como SuperCodec). H.264 viene habilitado de forma predeterminada y se procesa con el codificador DeepCompressionV2, un algoritmo de compresión basado en la CPU.
VMware®	VMware Horizon™ 6.0 y posterior VMware Horizon View™ 5.2 y 5.3 VMware View® 5.1

Requisitos con respecto al cliente

Consulte en la siguiente tabla la lista de sistemas operativos del thin client y el software de thin client compatibles de ISV que está usando en su VDI.

NOTA: HP True Graphics no está disponible con una licencia de prueba de ThinPro.

Tabla 6-2 Requisitos con respecto al cliente

Sistemas operativos compatibles	Clientes de Citrix compatibles	Clientes de VMware compatibles
HP ThinPro 5.0 y posterior	Citrix Receiver 13.1.1 y posterior **NOTA:** Una versión de Citrix Receiver que admite HP True Graphics viene preinstalada en las versiones a partir de HP ThinPro 5.2 y está disponible como complemento para HP ThinPro 5.0 y 5.1.	VMware Horizon Client 4.0 y posterior (usando el protocolo Blast)

Configuración del lado del cliente

Esta sección describe la configuración del lado del cliente.

NOTA: La información de esta sección solo corresponde a Citrix. En el caso de VMware, basta usar el protoloco Blast para habilitar HP True Graphics.

Ajustes de compresión

Para habilitar HP True Graphics en HP ThinPro:

▲ Seleccione la configuración general **Habilitar compresión H264** para las conexiones de Citrix.

NOTA: Algunos datos de la pantalla, como el texto, podrían enviarse utilizando métodos distintos a H.264. En general, es mejor mantener esta función activada, pero para la solución de problemas o casos de uso específicos, las siguientes claves de registro pueden configurarse en **0** con el fin de desactivar este recurso:

- **root/ConnectionType/xen/general/enableTextTracking**
- **root/ConnectionType/xen/general/enableSmallFrames**

Ajustes de la ventana

Para forzar a que las aplicaciones remotas se ejecuten en modo de ventanas:

▲ Establezca la configuración general **Modo TWI** para las conexiones de Citrix en **Forzar la desactivación de la continuidad**.

Limitaciones de hardware y disposición del monitor

Tenga en cuenta las siguientes limitaciones en la disposición del monitor:

- Se admite la mayoría de las configuraciones con un máximo de dos monitores que tengan una resolución de 1920 ×1200.
- HP t420 Thin Client: debido a su configuración de BIOS predeterminada, este modelo utiliza HP True Graphics solo en un monitor. Consulte Activación de HP True Graphics para varios monitores en el HP t420 en la página 50 para obtener más información.
- HP t630 Thin Client: este modelo admite un máximo de dos monitores a 1920 × 1200 o un monitor a 3840 × 2160.
- HP t730 Thin Client: este modelo admite un máximo de tres monitores a 1920 × 1200.
- Es posible que los monitores girados no se vean correctamente.
- Si está usando HP True Graphics con dos monitores e intenta reproducir un video mediante HDX MediaStream, el video va a fallar porque H.264 solo admite dos sesiones de decodificación de hardware, consumidas por los monitores.

NOTA: HDX MediaStream también trata de aprovechar la decodificación de hardware local de H.264, lo que causa el problema.

Activación de HP True Graphics para varios monitores en el HP t420

Para activar HP True Graphics en varios monitores en el HP t420:

1. Reinicie el thin client y presione F10 para acceder al BIOS.
2. Seleccione **Advanced (Avanzado)** > **Integrated Graphics (Gráficos integrados)**.

3. Establezca **Gráficos integrados** como **Forzar**.

4. Establezca **UMA Frame Buffer Size** (Tamaño de memoria de cuadro UMA) en **512 MB**

Después de que se realizan estos pasos, se expande la cantidad de memoria disponible para gráficos y se puede usar HP True Graphics en dos monitores.

SUGERENCIA: Estos ajustes también se pueden configurar mediante HPDM o a través de las herramientas del BIOS que se incluyen con HP ThinPro.

Consejos y mejores prácticas

Tome en cuenta lo siguiente al usar HP True Graphics:

- Después de conectarse a un escritorio remoto, puede usar Citrix HDX Monitor para determinar cuál codificador está utilizando la sesión. Para ello, examine el valor de **Component_Encoder** en la sección **Graphics - Thinwire Advanced**. Si el valor lee **DeepCompressionV2Encoder** o **DeepCompressionEncoder**, el servidor está enviando correctamente los datos en un formato acelerado por HP True Graphics.

NOTA: Si se fuerzan gráficos heredados mediante una política de servidor, como CompatibilityEncoder o LegacyEncoder, el servidor comprime los gráficos en un método compatible con versiones anteriores de clientes Citrix y HP True Graphics no mejorará el rendimiento.

- HP True Graphics podría proporcionar algunos beneficios a versiones anteriores de XenDesktop si usa HDX 3D Pro. No se brinda ninguna ventaja si se usa HDX 3D Pro con la calidad visual establecida en **Sin pérdidas siempre**, debido a que la información gráfica no se envía al thin client en el formato H.264.

7 Integración de Active Directory

Al usar la integración de Active Directory, puede obligar a los usuarios a iniciar sesión en el thin client mediante las credenciales del dominio. Como opción, esas credenciales se pueden encriptar y almacenar para suministrarlas después a las conexiones remotas a medida que se inician. Este proceso se conoce como inicio de sesión único.

NOTA: La habilitación de la autenticación no requiere permisos de dominio especiales.

La integración de Active Directory puede operar en dos modos. Con solo habilitar la autenticación contra el dominio, se pueden usar las credenciales del dominio para las siguientes operaciones:

- Iniciar sesión en el thin client
- Iniciar una conexión mediante el inicio de sesión único
- Alternar al modo de administrador mediante credenciales administrativas
- Desbloquear una pantalla bloqueada mediante las credenciales de inicio de sesión
- Anular una pantalla bloqueada mediante las credenciales administrativas

El thin client también se puede integrar formalmente al dominio. Esto agrega el thin client a la base de datos del dominio y podría habilitar el DNS dinámico, de modo que el thin client informe al servidor DNS sobre los cambios en su dirección de IP o la asociación del nombre de host. A diferencia de la autenticación de dominio, una integración formal requiere credenciales de un usuario del dominio autorizado para agregar clientes al dominio. La integración al dominio es opcional. Todas las funciones del dominio excepto DNS dinámico están disponibles sin la integración.

Pantalla de inicio de sesión

Cuando se habilita la autenticación de dominio, ThinPro muestra una pantalla de inicio de sesión en el dominio al iniciarse. La pantalla de inicio de sesión también incluye opciones que podría ser necesario configurar antes de iniciar sesión.

La presentación de fondo del escritorio, el estilo del diálogo de inicio de sesión, el texto del diálogo de inicio de sesión y los botones que están disponibles se pueden ajustar mediante las configuraciones de registro y/o los ajustes del archivo de configuración. Para obtener más información, consulte el informe técnico sobre HP ThinPro *"Login Screen Customization"* (disponible solo en inglés).

Si el sistema detecta que el usuario trató de iniciar sesión con credenciales vencidas, se le pide que actualice sus credenciales.

Inicio de sesión único

Después de que un usuario del dominio inicia sesión, las credenciales que usó también se pueden presentar en el inicio de cualquier conexión configurada para usarlas. Esto permite que un usuario inicie sesión en el thin client y empiece las sesiones de Citrix, VMware Horizon View y RDP sin tener que introducir de nuevo sus credenciales, durante el tiempo en que esté en la sesión del thin client.

Escritorio

Una vez que el usuario ha iniciado sesión correctamente mediante las credenciales de dominio, aparece un icono de Active Directory disponible en la barra de tareas. El usuario puede seleccionar el icono para que realice las siguientes funciones:

- Mostrar quién está en la sesión del sistema
- Bloquear la pantalla
- Cambiar la contraseña del dominio

NOTA: Los cambios de contraseña de dominio de ThinPro pueden fallar por varios motivos. Estos son algunos de los modos de falla conocidos:

Los cambios en la contraseña pueden fallar si tiene las siguientes opciones activadas en las directivas de seguridad de AD:

```
Configuración del equipo\Configuración de Windows\Configuración
de seguridad\Directivas locales\Opciones de seguridad\Seguridad de
red\Seguridad de sesión mínima para clientes basados en SSP NTLM
(incluido RPC seguro)
```

Requiere seguridad de la sesión NTLMv2

Requiere encriptación de 128 bits

```
Configuración del equipo\Configuración de Windows\Configuración
de seguridad\Directivas locales\Opciones de seguridad\Seguridad de
red\Seguridad de sesión mínima para servidor basado en SSP NTLM
(incluido RPC seguro)
```

Requiere seguridad de la sesión NTLMv2

Requiere encriptación de 128 bits

La Política de edad mínima de la contraseña no está configurada en 0:

```
GPO Default Domain Policy Comp Config\Policies\Windows Setting\Security
Settings\Account Policies\Password Policy\Minimum password age:
```

Establecer este valor en 0 podría ayudar a solucionar el límite, pero es probable que no sea aceptable con el cliente.

El cliente debe usar prácticas alternativas de AD para ayudar a los usuarios finales a cambiar una contraseña caducada en esas situaciones.

Bloquear la pantalla

La pantalla se puede bloquear debido al tiempo de inactividad o mediante el bloqueo manual. Si un usuario de dominio bloqueó la pantalla, el cuadro de diálogo de desbloqueo espera que el usuario brinde la misma contraseña de dominio con la que inició sesión. Así como sucede con el diálogo de inicio de sesión, se brindan opciones, además de una función adicional: desbloquear pantalla Si se selecciona el botón de desbloqueo de la pantalla, la pantalla de desbloqueo requiere la contraseña raíz (administrador) o cualquier conjunto de credenciales de dominio en el grupo de administradores de dominio, designado durante la configuración de autenticación del dominio. Cuando el usuario brinda credenciales de anulación, la pantalla no regresa al escritorio; vuelve a la pantalla de inicio de sesión.

Modo de administrador

Además del método tradicional de usar la contraseña raíz para entrar en el modo de administrador, se pueden usar las credenciales de dominio de un usuario en el grupo de administradores del dominio designado para pasar al modo de administrador.

Configuraciones y usuario del dominio

Cuando un usuario del dominio inicia sesión, cualquier cambio en las configuraciones se guarda en una capa de registro que se aplica solo a ese usuario. Esto incluye las conexiones que se acaban de crear.

Si el usuario no ha hecho cambios a las conexiones o las configuraciones del sistema, se aplicarán los valores predeterminados del sistema.

Cuando el sistema pasa al modo de administrador, los cambios en las conexiones y las configuraciones se dejan de aplicar a la capa específica del usuario en el registro. En vez de ello, mientras esté en el modo de administrador, todos los cambios se aplican al registro del nivel base. De esta forma, mientras esté en el modo de administrador, un cambio en una configuración se aplica a todos los usuarios, a menos que ya se haya especificado una configuración personalizada y específica del usuario.

8 Menú de Inicio

Para abrir el menú de Inicio, seleccione **Inicio**.

Administración de conexiones

El menú enumera todas las conexiones disponibles. Haga clic derecho en el nombre de la conexión para administrar esa conexión o selecciónela para iniciar la conexión. Si la conexión se está ejecutando y la selecciona, se detiene.

Para obtener más información acerca de la administración de conexiones, consulte Administración de conexiones del escritorio en la página 11.

Cambiar a Administrador/Cambiar a usuario

Esta opción le permite alternar entre el modo de administrador y el de usuario.

Información del sistema

Esta opción inicia la aplicación Información del sistema.

Para obtener más información, consulte .

Panel de control

Esta opción inicia el Panel de control.

Para obtener más información, consulte .

Herramientas

Se brindan muchas herramientas del sistema, incluida una para iniciar los programas, como una terminal de texto, o para ejecutar por segunda vez el Asistente de configuración inicial. Si ha iniciado sesión como usuario, solo se muestran las herramientas autorizadas. Si esta lista está vacía, la entrada al menú de Herramientas está oculta.

Tabla 8-1 Herramientas

Opción de menú	Descripción
Terminal de X	Le permite ejecutar comandos de Linux.
Estadísticas de conexión inalámbrica	Le permiten ver información sobre los puntos de acceso inalámbrico.
Buscar actualizaciones	Busca actualizaciones del servidor.
Editor de textos	Abre un editor de texto básico para ver y editar archivos de texto.

Tabla 8-1 **Herramientas (continúa)**

Opción de menú	Descripción
Administrador de tareas	Le permite supervisar el uso de la CPU y el historial de uso de la CPU en el thin client.
Recortes	Le permite tomar una instantánea de una selección rectangular de la pantalla, una ventana específica o la pantalla completa.
Editor de registro	Abre el Editor de registro de ThinPro.
Asistente de configuración inicial	Inicia el Asistente de configuración inicial.
Verificación de compatibilidad	Ejecuta la herramienta Verificación de compatibilidad de ThinPro, que evalúa la idoneidad del sistema para ejecutar ThinPro.

Alimentación

Estas opciones le permiten cerrar sesión, apagar el equipo, reiniciarlo o habilitar el estado de Suspensión.

Un administrador puede restringir las opciones visibles para un usuario mediante la herramienta Administrador de energía. Consulte Sistema en la página 57.

Buscar

Cuando escribe en la casilla de búsqueda, aparece una lista de posibles coincidencias para su búsqueda, de la más probable a la menos probable. La búsqueda incluye los nombres visibles de los controles, las herramientas y las conexiones y alias y sinónimos asociados. Por ejemplo, si está en el modo de administrador y escribe `encriptación` aparece el control de Seguridad porque ese control ofrece parámetros de encriptación.

Para ver todas las opciones disponibles, escriba un espacio en el cuadro de búsqueda o seleccione el icono de la lupa.

La búsqueda también informa las opciones para crear nuevas conexiones de todos los tipos disponibles. Esto puede utilizarse para administrar las conexiones.

9 Panel de control

El Panel de control le permite modificar la configuración del sistema.

Abrir el Panel de control

Para abrir el panel de control:

▲ Seleccione **Inicio** y luego seleccione **Panel de control**.

NOTA: También puede buscar una función específica del Panel de control mediante el cuadro de búsqueda del menú de Inicio.

NOTA: Se puede acceder a todos los elementos del Panel de control en el modo de administrador. Cuando se encuentra en el modo de usuario, solo se puede acceder a los elementos del Panel de control que el administrador haya habilitado para el uso de los usuarios.

SUGERENCIA: Para especificar a cuáles elementos del Panel de control tienen acceso los usuarios finales, abra el Panel de control, seleccione **Apariencia**, seleccione **Centro de personalización** y luego seleccione o desmarque elementos de la lista de **Aplicaciones**.

Sistema

Esta sección describe la configuración del sistema.

Tabla 9-1

Opción de menú	Descripción
Fecha y Hora	Le permite configurar la zona horaria y las opciones de fecha y hora.
Red	Le permite configurar los ajustes de la red. Para obtener más información, consulte Ajustes de la red en la página 58.
Opciones DHCP	Le permite configurar las opciones de DHCP. Para obtener más información, consulte Opciones DHCP en la página 62.
Administrador de energía	Le permite configurar los ajustes de administración de energía como el protector y el bloqueo de pantalla, las configuraciones de la CPU, el momento de apagar la pantalla y el de entrar en el modo de suspensión. En el modo de administrador, puede restringir el acceso a las opciones relacionadas con la energía (como el reinicio) para todo el sistema.
Configuración de Imprivata	Le permite habilitar el modo Imprivata Appliance y especificar el servidor Imprivata; consulte Configuración de Imprivata en la página 63.

Tabla 9-1 (continúa)

Opción de menú	Descripción
Administrador de componentes	Le permite eliminar componentes del sistema. Para obtener más información, consulte Administrador de componentes en la página 64.
Restablecimiento de valores de fábrica	Le permite restaurar el thin client a su configuración predeterminada de fábrica.
Instantáneas	Le permite restaurar el thin client a un estado anterior o a su configuración predeterminada de fábrica.

Ajustes de la red

Los ajustes de red se pueden configurar utilizando el Administrador de red.

Abrir el Administrador de red

Para abrir el Administrador de red:

▲ Seleccione **Sistema** y luego **Red** en el Panel de control.

Consulte las siguientes secciones para obtener más información sobre las distintas fichas en el Administrador de red:

Ajustes para la red cableada

La siguiente tabla describe las opciones disponibles en la ficha **Cableada** del Administrador de red.

Tabla 9-2 **Ajustes para la red cableada**

Opción	Descripción
Activar IPv6	Activa IPv6. IPv4 se utiliza de forma predeterminada, y no pueden utilizarse al mismo tiempo.
Velocidad de Ethernet	Le permite definir la velocidad de Ethernet. Si su interruptor o concentrador no tiene un requisito especial, opte por la configuración predeterminada **Automática**.
Método de conexión	Le permite elegir entre **Automática** y **Estática**. Si su entorno de red usa DHCP, la opción **Automática** debe funcionar sin que sea necesario establecer otro tipo de configuraciones. Si se selecciona **Estática**, aparece el ajuste **Configuración de dirección estática**. Asegúrese de ingresar estos valores de acuerdo con la opción que está utilizando, IPv4 o IPv6.
MTU	Le permite ingresar la unidad de transmisión máxima (en bytes).
Ajustes de seguridad	Le permite definir uno de los siguientes ajustes de autenticación: • Ninguna • 802.1X-TTLS • 802.1X-PEAP • 802.1X-TLS Tenga en cuenta lo siguiente sobre TTLS y PEAP: • La opción de **Autenticación interna** debe configurarse de acuerdo con lo que admite el servidor.

Tabla 9-2 **Ajustes para la red cableada (continúa)**

Opción	Descripción
	• El ajuste **Certificado CA** debe hacer referencia al certificado del servidor en el thin client local. • El **Nombre de usuario** y la **Contraseña** son las credenciales del usuario. Tenga en cuenta lo siguiente sobre TLS: • El ajuste **Certificado CA** debe hacer referencia al certificado del servidor en el thin client local. • Si su archivo de **Clave privada** es .p12 o .pfx, entonces, el ajuste **Certificado de usuario** puede dejarse en blanco. • El ajuste **Identidad** debe ser el nombre de usuario que corresponde al certificado de usuario. • El ajuste de la **Contraseña de clave privada** es la contraseña del archivo de clave privada del usuario.

Ajustes para la red inalámbrica

Use esta ficha para agregar, editar y eliminar los perfiles inalámbricos que corresponden a redes inalámbricas.

Las siguientes tablas describen las opciones disponibles cuando agrega o edita un perfil inalámbrico.

NOTA: Esta ficha está disponible solo si el thin client tiene un adaptador para conexiones inalámbricas.

SUGERENCIA: También puede acceder a estas configuraciones seleccionando el icono de estado de la red en la barra de tareas.

Use la ficha **Conexiones inalámbricas** para configurar los valores generales.

Tabla 9-3 **Ajustes para la red inalámbrica**

Opción	Descripción
Búsqueda de AP	Busca las redes inalámbricas disponibles.
SSID	Utilice esta casilla para introducir el SSID de la red inalámbrica en forma manual si no se encontró en la búsqueda.
Banda inalámbrica	Seleccione **Automática**, **2,4 GHz** o **5 GHz**.
SSID oculto	Active esta opción si el SSID de la red inalámbrica está configurado como oculto (no está transmitiendo).
Activar IPv6	Activa IPv6. IPv4 se utiliza de forma predeterminada, y no pueden utilizarse al mismo tiempo.
Activar la administración de energía	Activa el recurso de administración de energía del adaptador de conexiones inalámbricas.
Método de conexión	Permite seleccionar entre **Automática** y **Estática**. Si su entorno de red usa DHCP, la opción **Automática** debe funcionar sin otro tipo de configuraciones. Si se selecciona **Estática**, aparece el ajuste **Configuración de dirección estática**. Asegúrese de ingresar estos valores de acuerdo con la opción que está utilizando, IPv4 o IPv6.
Ajustes de seguridad	Le permite definir uno de los siguientes ajustes de autenticación: • Ninguna • WEP • WPA/WPA2-PSK

Tabla 9-3 Ajustes para la red inalámbrica (continúa)

Opción	Descripción
	• 802.1X-TTLS • 802.1X-PEAP • 802.1X-TLS • EAP-FAST En el caso de WEP y WPA2/WPA-PSK, solo tiene que introducir la clave de red y seleccionar **Aceptar**. Para EAP-FAST, configure **Identidad anónima**, **Nombre de usuario**, **Contraseña** y **Método de aprovisionamiento**. No necesita cambiar los ajustes del archivo PAC. Consulte Ajustes para la red cableada en la página 58 para obtener más información sobre TTLS, PEAP y TLS.
Conexión automática	Esta opción está reservada para el futuro.
Activar conexiones inalámbricas	Activa el adaptador de conexiones inalámbricas.

Use la ficha **IPv4** para configurar los ajustes de la conexión IPv4.

Tabla 9-4 Ajustes de conexión IPv4

Opción	Descripción
IPv4 activada	Activa IPv4.
Método IPv4	Permite seleccionar entre **Automática** y **Estática**. Si su entorno de red usa DHCP, la opción **Automática** debe funcionar sin otro tipo de configuraciones. Si se selecciona **Estática**, aparecen los valores de la **Configuración de dirección estática** y debe introducir las configuraciones de IPv4.

Use la ficha **IPv6** para configurar los ajustes de la conexión IPv6.

Tabla 9-5 Ajustes de conexión IPv6

Opción	Descripción
IPv6 activada	Activa el uso de una dirección global de IPv6. **NOTA:** HP ThinPro trata de obtener una dirección global de IPv6 mediante la publicidad de la ruta o de DHCPv6.
Método IPv6	Permite seleccionar entre **Automática** y **Estática**. Si su entorno de red usa DHCP, la opción **Automática** debe funcionar sin otro tipo de configuraciones. Si se selecciona **Estática**, aparecen los valores de la **Configuración de dirección estática** y debe introducir las configuraciones de IPv6.

Use la ficha **Seguridad** para configurar los valores de seguridad de la conexión.

Tabla 9-6 Ajustes de seguridad de la conexión

Opción	Descripción
Autenticación	Le permite definir uno de los siguientes ajustes de autenticación: • Ninguna • WEP • WPA/WPA2-PSK • WPA/WPA2 Enterprise-TTLS • WPA/WPA2 Enterprise-PEAP • WPA/WPA2 Enterprise-TLS • EAP-FAST En el caso de WEP y WPA2/WPA-PSK, solo tiene que introducir la clave de red y seleccionar **Aceptar**. Para EAP-FAST, configure **Identidad anónima**, **Nombre de usuario**, **Contraseña** y **Método de aprovisionamiento**. No necesita cambiar los ajustes del archivo PAC. Consulte Ajustes para la red cableada en la página 58 para obtener más información sobre TTLS, PEAP y TLS.

configuración DNS

La siguiente tabla describe las opciones disponibles en la ficha **DNS** del Administrador de red.

Tabla 9-7 configuración DNS

Opción	Descripción
Nombre de host	Este se genera automáticamente según la dirección MAC del thin client. También puede configurar un nombre de host personalizado.
Servidores DNS	Utilice esta casilla para definir la información del servidor DNS personalizado.
Búsqueda de dominios	Utilice esta casilla para restringir los dominios que se buscan.
Proxy HTTP Proxy FTP Proxy HTTPs	Utilice estas casillas para definir la información del servidor proxy usando el formato siguiente: `http://<dirección>:<puerto>` HP recomienda utilizar el prefijo `http://` para los tres ajustes de proxy. De esta forma, logrará una mejor compatibilidad. **NOTA:** Los ajustes de proxy se predeterminan en las variables medioambientales **http_proxy**, **ftp_proxy** y **https_proxy** para el sistema.

Reglas de IPSec

Utilice esta ficha para agregar, editar y eliminar reglas IPSec. Una regla IPSec debe ser la misma para cada sistema que utiliza IPSec al comunicarse.

Al configurar una regla IPSec, utilice la ficha **General** para establecer la información de la regla, las direcciones y el método de autenticación. La **Dirección de origen** es la dirección IP del thin client y la Dirección de destino es la dirección IP del sistema con el cual el thin client va a comunicarse.

NOTA: Solo se admiten los tipos de autenticación **PSK** y **Certificado**. No se admite la autenticación Kerberos.

Use la ficha **Túnel** para establecer los ajustes del modo túnel.

Utilice las fichas **Etapa I** y **Etapa II** para configurar los ajustes avanzados de seguridad. Los ajustes deben ser iguales para todos los sistemas pares que se comuniquen entre sí.

NOTA: También puede usar una regla IPSec para comunicarse con un equipo con Windows.

Configuración de los ajustes de VPN

HP ThinPro admite dos tipos de VPN:

- Cisco
- PPTP

Active la opción de **Inicio automático** para iniciar la VPN automáticamente.

Tenga en cuenta lo siguiente respecto de la creación de una VPN con Cisco:

- El **Gateway** es la dirección IP del gateway o el nombre de host.
- El **Nombre del grupo** y la **Contraseña del grupo** son el ID IPSec y la contraseña IPSec.
- La configuración de **Dominio** es opcional.
- El **Nombre de usuario** y la **Contraseña de usuario** son las credenciales del usuario que tenga derechos para crear una conexión VPN en el lado del servidor.
- El **Tipo de seguridad** debe configurarse de la misma manera que del lado del servidor.
- La opción **NAT Traversal** debe establecerse según su entorno de VPN.
- La opción **Grupo de DH IKE** establece el grupo Diffie-Hellman que se va a usar en la VPN.
- La opción **Tipo de PFS** establece el grupo Diffie-Hellman que se va a usar en Perfect Forward Secrecy.

Tenga en cuenta lo siguiente respecto de la creación de una VPN con PPTP:

- El **Gateway** es la dirección IP del gateway o el nombre de host.
- La configuración de **Dominio NT** es opcional.
- El **Nombre de usuario** y la **Contraseña de usuario** son las credenciales del usuario que tenga derechos para crear una conexión VPN en el lado del servidor.

Opciones DHCP

Cómo configurar y administrar las opciones de DHCP.

Abrir el Administrador de opciones DHCP

Para abrir el Administrador de opción DHCP:

▲ Seleccione **Sistema** y luego **Opciones de DHCP** en el Panel de control.

Solicitar o ignorar las opciones de DHCP

Para que el thin client solicite o ignore opciones específicas de DHCP:

El Administrador de opción DHCP muestra detalles de las opciones DHCP solicitadas por el thin client.

SUGERENCIA: La lista desplegable le permite filtrar cuáles etiquetas de DHCP aparecen.

▲ Marque o desmarque las casillas de verificación en la columna **Solicitada**.

Cambiar un código DHCP

Para cambiar un código DHCP:

Si se muestra un lápiz en la columna de **Código DHCP**, puede cambiar el número de código en caso de que haya un conflicto en su servidor DHCP respecto de un número de código específico.

▲ Haga doble clic en el código DHCP y escriba un número de nuevo.

NOTA: Los códigos DHCP modificables solo pueden modificarse si esa opción DHCP está activada en la columna **Solicitada**.

Información sobre las opciones DHCP

Para obtener más información sobre cómo se usa una opción DHCP en el thin client y en el servidor DHCP:

▲ Seleccione el icono en la columna **Información** de dicha opción.

Configuración de Imprivata

Estos dos paquetes están instalados en ThinPro:

- Cargador Imprivata OneSign Bootstrap: onesign-bootstrap-loader
- Scripts de ayuda de HP Imprivata (scripts de inicio del proveedor): hptc-imprivata-helper

Cuando el Modo de dispositivo Imprivata está activado, el cargador OneSign Bootstrap se conecta en el servidor Imprivata OneSign especificado e instala o actualiza el agente incorporado Imprivata ProveID (agente PIE).

El agente PIE se encuentra instalado en el directorio /usr/lib/imprivata/runtime/.

A partir de ThinPro 7.2, necesitará un servidor Imprivata OneSign 6.3 o posterior. Los scripts de ayuda de HP Imprivata inician el cliente VDI. El cliente VDI es un cliente De Citrix, VMware o RDP.

Los scripts de ayuda de HP están instalados en el directorio /usr/lib/Imprivata-helper/.

Los agentes de Imprivata usan dos archivos de registro:

- /usr/lib/imprivata/runtime/log/OneSign.log
- /usr/lib/imprivata/runtime/log/OneSignAgent.log

NOTA: Puede encontrar más información en http://documentation.imprivata.com.

NOTA: Verifique que el certificado del servidor Imprivata OneSign sea válido en ThinPro. Es posible que deba instalarlo o su certificado raíz de CA. Consulte Administrador de certificados en la página 67.

Para abrir la configuración de Imprivata:

▲ Seleccione **Sistema** y luego **Configuración de Imprivata** en el Panel de control.

Administrador de componentes

El Administrador de componentes le permite eliminar los componentes del sistema que no se utilizan en su entorno, lo que puede ser deseable para reducir el tamaño de la imagen o aumentar la seguridad. Por ejemplo, si las conexiones Citrix nunca se utilizan en su entorno, es posible que quiera eliminar el componente de Citrix.

A medida que se eliminan los componentes, la nueva configuración puede probarse antes de aplicar los cambios de forma permanente. También puede deshacer los cambios que se hicieron, si estos aún no se han aplicado permanentemente.

IMPORTANTE: Después de que se aplica la nueva configuración de forma permanente, todas las instantáneas se eliminan y se crea una nueva instantánea de fábrica. Los componentes eliminados no se pueden restaurar después de este punto.

NOTA: La eliminación de componentes podría no reducir el uso de espacio de disco local, pero debe reducir el tamaño de cualquier imagen de disco creada desde el sistema local.

Para abrir el Administrador de componentes:

Abrir el Administrador de componentes

Para abrir el Administrador de componentes:

▲ Seleccione **Sistema** y luego **Administrador de componentes** en el Panel de control.

Eliminación de componentes

Para eliminar componentes:

1. En el Administrador de componentes, seleccione los componentes deseados.

   SUGERENCIA: Para seleccionar varios componentes, use Ctrl o Mayús.

2. Seleccione **Eliminar componente(s)**.
3. Si aparece el cuadro de diálogo de confirmación, seleccione **Aceptar**.
4. Después de eliminar los componentes, pruebe la nueva configuración.

Deshacer un cambio

Puede deshacer cada cambio, uno por uno, si los cambios aún no se han aplicado permanentemente. Se necesita reiniciar el thin client después de cada cambio deshecho.

Para deshacer un cambio realizado con el Administrador de componentes:

1. En el Administrador de componentes, seleccione **Revertir el último cambio**.
2. Seleccione **Sí** para reiniciar el thin client.

Repita este proceso con todos los cambios que desee deshacer.

IMPORTANTE: Si usted toma una instantánea de la imagen mientras prueba una nueva configuración, no puede deshacer los cambios a través del Administrador de componentes. Solo puede deshacer estos

cambios mediante la restauración de una instantánea anterior a través de la herramientas Instantáneas. Sin embargo, esto no funciona si los cambios ya se han aplicado de forma permanente, debido a que esa función elimina todas las instantáneas existentes. Si ya se han aplicado los cambios permanentemente, deberá reinstalar el sistema operativo para restaurar la mayoría de los componentes eliminados. Algunos componentes (como Citrix, RDP y VMware Horizon View) podrían estar disponibles como complementos en la web y se pueden restaurar al reinstalarlos.

Aplicar los cambios de forma permanente

Para aplicar permanentemente los cambios realizados con el Administrador de componentes:

IMPORTANTE: Después de que se aplica la nueva configuración de forma permanente, todas las instantáneas se eliminan y se crea una nueva instantánea de fábrica. Los componentes eliminados no se pueden restaurar después de este punto.

1. En el Administrador de componentes, seleccione **Aplicar configuración del componente**.
2. Seleccione **Yes** (Sí).

Seguridad

Esta sección describe la configuración de Seguridad.

Tabla 9-8

Opción de menú	Descripción
Seguridad	Para obtener más información, consulte Configuraciones de seguridad en la página 65.
Cambiar contraseña del dominio	Si se usa un dominio, le permite cambiar la contraseña del dominio.
Certificados	Abre el Administrador de certificados, que le permite importar, ver o eliminar certificados fácilmente. Para obtener más información, consulte Administrador de certificados en la página 67.
Administrador de firewall	Le permite configurar los ajustes de firewall.
Administrador de SCEP	Permite la administración de certificados basados en red.

Configuraciones de seguridad

Los ajustes de seguridad se pueden configurar utilizando el Administrador de seguridad. Para abrir el Administrador de seguridad, seleccione **Seguridad** y luego seleccione **Seguridad** en el Panel de control.

Consulte las siguientes secciones para obtener más información sobre las distintas fichas del Administrador de seguridad.

- Cuentas locales en la página 66
- Encriptación en la página 66
- Opciones en la página 66

Cuentas locales

La ficha Cuentas locales se puede usar para cambiar las contraseñas de la cuenta de usuario y de raíz local o para deshabilitar la autenticación mediante esas cuentas.

⚠ **PRECAUCIÓN:** La deshabilitación de las cuentas de usuario y/o raíz podrían dejar su sistema inutilizable a menos que esté habilitada la autenticación de Active Directory. Por ejemplo, si se deshabilita la cuenta raíz, solo podrá cambiar el modo de administrador mediante las credenciales de dominio de un administrador. No obstante, si se deshabilitan las cuentas locales, podría mejorar la seguridad cuando está habilitada la autenticación de Active Directory porque ya no tiene que mantener y actualizar un secreto compartido como la contraseña raíz del thin client.

Si se utilizó la autenticación de Active Directory y hay datos almacenados en la caché para los usuarios del dominio en el thin client, desde esta ficha también puede eliminar los datos en caché del usuario.

NOTA: Si el usuario inició sesión mediante una cuenta de dominio, no puede eliminar los datos de su propia cuenta porque esto dejaría el sistema en un estado indeterminado.

Encriptación

Las credenciales de Active Directory y otros secretos se pueden ocultar con hash para funciones como el desbloqueo de la pantalla y/o encriptar y almacenar en el sistema para el inicio de sesión único.

El algoritmo hash para crear una hash de la contraseña se puede seleccionar en este menú. El valor predeterminado, scrypt, es una función de derivación de clave bien aceptada. También hay disponible otra función de derivación de clave, así como los hashes convencionales SHA-256 y SHA-512. La ventaja de una función de derivación de clave es que es computacionalmente costoso calcular una tabla arco iris que haga coincidir contraseñas en texto sin formato con valores hash calculados previamente, considerando que los hashes convencionales se deben ejecutar lo más rápido posible. Todos los hashes se almacenan con 128 o más bits de semilla aleatoria que cambia cada vez que la hash de la contraseña se computa y almacena.

Las contraseñas encriptadas se usan en las situaciones en las que se pueden revertir y suministrar a las conexiones cuando se inician (inicio de sesión único). El algoritmo de encriptación se puede seleccionar aquí desde una amplia variedad admitida por OpenSSL. A menos que haya una buena razón para seleccionar un valor diferente, HP recomienda que use el algoritmo de encriptación predeterminado, que la comunidad relacionada con la seguridad suele considerar un algoritmo moderno y seguro. La cantidad de bits de sal y de bits de clave van a variar de un algoritmo a otro y puede obtener detalles al presionar el botón de información que está al lado del selector de algoritmo. Las claves de encriptación son únicas por thin client y se almacenan en un lugar que solo los administradores pueden leer. Además, solo ciertas aplicaciones autorizadas en el sistema pueden hacer desencriptación.

Tanto los hashes como los secretos encriptados se pueden configurar con un tiempo de vida. Si el tiempo entre el momento en que el secreto se ocultó con hash o se encriptó y el momento en que se usó o desencriptó supera el tiempo de vida, la coincidencia de hash o la desencriptación fallarán.

De forma predeterminada, la contraseña de inicio de sesión único se puede usar solo durante un día, pero las contraseñas guardadas con los ajustes de la conexión o la red se pueden usar de forma indefinida.

Opciones

El usuario local debe iniciar sesión: si se selecciona esta opción cuando la autenticación de Active Directory está desactivada, la pantalla de inicio de sesión sigue apareciendo en el inicio y al cerrar la sesión. En esta situación, deben usarse las credenciales de raíz o usuario local para obtener acceso al sistema.

Activar pico secreto: si está activada, la mayoría de los campos de entrada secretos y de contraseña del sistema muestran un pequeño icono en forma de ojo al lado derecho. Si selecciona el icono del ojo al presionar

y mantener el botón izquierdo del mouse, aparece el secreto en texto sin formato mientras sostenga el botón del mouse. En el momento en que suelte el botón, se vuelve a oscurecer el secreto.

Usar la entrada de texto del dominio: si se habilita, se brinda un campo de entrada de Dominio separado para introducir el nombre del dominio cuando corresponda. Si se deshabilita, el dominio lo determina el valor introducido en el campo Usuario. Por ejemplo, si el campo de usuario contiene “mike@mycorp”, se asume que el dominio es “mycorp”. Si el campo de usuario es “graycorp\mary”, se asume que el dominio es “graycorp”.

Permitir que los administradores anulen el bloqueo de pantalla: si se habilita, puede anular una pantalla bloqueada y devolverla a la pantalla de inicio o al escritorio de ThinPro, como si el usuario hubiera cerrado sesión manualmente en el thin client.

Certificados

Esta sección describe información sobre el uso de certificados.

NOTA: Para obtener más información sobre el uso de los certificados en Linux, consulte https://www.openssl.org/docs/.

Administrador de certificados

Para abrir el Administrador de certificados:

▲ Seleccione **Seguridad** y luego **Certificados** en el Panel de control.

Utilice el Administrador de certificados para instalar manualmente un certificado de una autoridad de certificación (CA). Esta acción copia el certificado en el almacén de certificados local del usuario (/usr/local/share/ca-certificates) y configura OpenSSL para utilizar el certificado para verificar la conexión.

Si lo desea, utilice Profile Editor (Editor de perfiles) para adjuntar el certificado a un perfil, tal como se describe en Agregar certificados a un perfil de cliente en la página 89.

NOTA: Por lo general, un certificado autofirmado funcionará siempre que sea válido de acuerdo con la especificación y pueda ser verificado por OpenSSL.

Administrador de SCEP

Para abrir el Administrador de SCEP:

▲ Seleccione **Seguridad** y luego **Administrador de SCEP** en el Panel de control.

Utilice el Administrador de SCEP cuando necesita registrar o renovar los certificados del lado del cliente desde una CA.

Durante un registro o renovación, el Administrador de SCEP genera la clave privada y la solicitud de certificado del thin client. Luego envía la solicitud a la CA en el servidor SCEP. Cuando la CA emite el certificado, el certificado se devuelve y se coloca en el almacén de certificados del thin client. OpenSSL utiliza el certificado para verificar la conexión.

NOTA: Antes del registro, asegúrese de que el servidor SCEP está configurado correctamente.

Use la pestaña **Identificar** del Administrador de SCEP para ingresar información sobre el usuario, si lo desea.

NOTA: El **Nombre común** es obligatorio. De forma predeterminada, este es el nombre de dominio completamente calificado (FQDN) del thin client. El resto de la información es opcional. El **País o la Región** se escriben con dos letras, como US para los Estados Unidos y CN para China.

Use la ficha **Servidores** del Administrador de SCEP para agregar servidores SCEP y registrar o renovar certificados.

SUGERENCIA: Al introducir un nuevo servidor SCEP, primero, guarde la información del servidor, luego use el botón **Configuración** para regresar y realizar el registro.

Capacidad de administración

Esta sección describe la configuración de la Capacidad de administración.

Tabla 9-9

Opción de menú	Descripción
Active Directory	Para obtener más información, consulte Configuración de Active Directory en la página 68.
Actualización automática	Le permite configurar el servidor de Automatic Update manualmente. Para obtener más información, consulte HP Smart Client Services en la página 82.
Easy Update	Abre HP Easy Tools. Para obtener más información, consulte la guía de usuario de HP Easy Tools.
HPDM Agent	Le permite configurar al agente de HP Device Manager (HPDM). Para obtener más información, consulte la *Guía del administrador* de HPDM.
Administrador SSHD	Permite acceso a través de un shell seguro.
ThinState	HP ThinState le permite hacer una copia o restaurar la imagen del sistema operativo completa o sus ajustes de configuración. Para obtener más información, consulte HP ThinState en la página 70.
Vigilancia de VNC	Le permite configurar las opciones de duplicación VNC. Para obtener más información, consulte Duplicación VNC en la página 73.

Configuración de Active Directory

Ficha de Estado

Este control le permite activar o desactivar la autenticación contra un dominio, la integración al dominio y diversas opciones relacionadas con el dominio.

Después de que cambia los parámetros del dominio en la ficha de Estado, la página muestra una acción pendiente y debe seleccionar **Aplicar** para que la acción suceda. Integrarse o salirse de un dominio requiere credenciales con permisos para realizar esa operación. Después de habilitar la autenticación o de integrarse al dominio, algunos de los subparámetros podrían marcarse como solo de lectura porque no es posible cambiarlos en ese momento. En vez de eso, debe salirse o deshabilitar la autenticación y luego aplicar los cambios. Luego puede volver a habilitar la autenticación o integrarse con los subparámetros alterados.

Tabla 9-10 Ficha de Estado

Opción	Descripción
Nombre de dominio	Si el thin client puede determinar el nombre del dominio usando opciones de DHCP, se mostrará aquí. De lo contrario, tendrá que introducir de forma manual el nombre del dominio completamente calificado.
Autenticar contra el dominio	Si está activado, se pueden usar las credenciales del dominio, como se explica en la sección Integración de Active Directory de esta guía.
Requerir el inicio de sesión del thin client	Esto se activa de forma predeterminada y hace que el sistema se inicie en la pantalla de inicio de sesión del dominio. Si está desactivado, las credenciales del dominio se pueden usar para pasar al modo de administrador o para anular una plantalla bloqueada, pero no estará disponible el inicio de sesión único.
Grupo de trabajo	Por lo general, esto se detecta de forma automática a partir de la información proporcionada por los servidores de la red, pero puede usarlo como una anulación manual si tiene una topología de la red inusual.
Controladoras del dominio	Por lo general, esto se detecta mediante búsquedas de DNS, pero puede especificarlas manualmente si su red no brinda esa información.
Integrar el thin client al dominio	Como se explicó en el capítulo sobre Integración de Active Directory, esta opción le permite agregar el thin client formalmente a las bases de datos de Active Directory.
Unidad organizacional (OU)	El thin client suele agregarse a la OU “Equipos" de la base de datos, pero puede introducir manualmente un valor diferente aquí si su esquema de base de datos lo exige.
DNS dinámico	Si se habilita, el thin client intentará actualizar al servidor de DNS siempre que cambia la asociación de su dirección de IP/nombre de host.

Ficha Opciones

Esta sección describe las opciones dentro de la ficha Opciones.

Tabla 9-11

Opción	Descripción
Habilitar el inicio de sesión único	Si está activado, se encripta y se guarda en el sistema una contraseña suministrada en el inicio de sesión. Cuando se inicia una conexión con las credenciales de SSO configuradas, puede desencriptar la contraseña y pasarla a la conexión de forma que se pueda usar para el inicio de sesión remoto.
Grupo de inicio de sesión del dominio	Si está activado, el inicio de sesión se restringe a los usuarios en el grupo de dominio enumerado.
Grupo de administradores del dominio	Si está activado, el escalonamiento al modo de administrador y la anulación del bloqueo de pantalla se limita a los miembros del grupo de dominio enumerado.
Habilitar el inicio de sesión del dominio en caché	Si está activado, se guarda un hash de la contraseña del usuario en el sistema y se puede usar para el inicio de sesión incluso cuando no se pueda acceder al servidor de Active Directory.
Conservar las preferencias del usuario al cerrar la sesión	Si opción está activada, cualquier cambio en las configuraciones que haya sido realizado por un usuario del dominio se guarda en un lugar donde esas configuraciones se apliquen solo a ese usuario. Si esta opción está desactivada, cualquier cambio de ese tipo específico del usuario se desecha cuando el usuario cierra la sesión.
Permitir los cambios en la contraseña del dominio	Si está activado, las contraseñas vencidas generan un mensaje que le permite al usuario actualizar su contraseña y puede actualizar su contraseña manualmente mediante el icono del usuario en la barra de tareas.

HP ThinState

HP ThinState le permite capturar e implementar una imagen o configuración (perfil) de HP ThinPro en otro thin client de modelo y hardware compatibles.

Administración de una imagen HP ThinPro

Capturar una imagen HP ThinPro en un servidor FTP

Para capturar una imagen HP ThinPro en un servidor FTP:

IMPORTANTE: El directorio en el servidor FTP donde desea guardar la imagen capturada ya debe existir antes de iniciar la captura.

1. Seleccione **Administración > ThinState** en el Panel de control.
2. Seleccione **la imagen de HP ThinPro** y luego seleccione **Siguiente**.
3. Seleccione **hacer una copia de la imagen de HP ThinPro** y luego seleccione **Siguiente**.
4. Seleccione **en un servidor FTP** y luego seleccione **Siguiente**.
5. Ingrese la información del servidor FTP en los campos.

   NOTA: El nombre del archivo de imagen está configurado de forma predeterminada para que sea el nombre de host del thin client.

   Seleccione **Comprimir la imagen** si desea comprimir la imagen capturada.

   NOTA: El archivo de imagen de HP ThinPro es un simple disco de depósito. El tamaño sin comprimir es de aproximadamente 1 GB, y una imagen comprimida sin complementos es de aproximadamente 500 MB.

6. Seleccione **Finalizar**.

   Cuando comienza la captura de la imagen, todas las aplicaciones se detienen y aparece una nueva ventana que muestra el progreso. Si surge un problema, seleccione **Detalles** para obtener más información. El escritorio vuelve a aparecer al finalizar la captura.

Implementación de una imagen HP ThinPro usando FTP o HTTP

Para implementar una imagen HP ThinPro por medio de FTP o HTTP:

IMPORTANTE: Si detiene una implementación antes de terminar, no se restaurará la imagen anterior y el contenido de la unidad flash del thin client se dañará.

1. Seleccione **Administración > ThinState** en el Panel de control.
2. Seleccione **la imagen de HP ThinPro** y luego seleccione **Siguiente**.
3. Seleccione **restaurar una imagen de HP ThinPro** y luego seleccione **Siguiente**.
4. Seleccione el protocolo FTP o HTTP y luego ingrese la información del servidor en los campos.

   NOTA: Los campos **Nombre de usuario** y **Contraseña** no son obligatorios si usa el protocolo HTTP.

5. Seleccione **Retener la configuración de HP ThinPro** si desea conservar todas las configuraciones previas.

6. Seleccione **Finalizar**.

   Cuando comienza la implementación de la imagen, todas las aplicaciones se detienen y aparece una nueva ventana que muestra el progreso. Si surge un problema, seleccione **Detalles** para obtener más información. El escritorio vuelve a aparecer al finalizar la implementación.

NOTA: Se realiza una verificación MD5sum solo si el archivo MD5 existe en el servidor.

Capturar una imagen HP ThinPro en una unidad flash USB

Para capturar una imagen HP ThinPro en una unidad flash USB:

IMPORTANTE: Haga una copia de seguridad de los datos de la unidad flash USB antes de comenzar. HP ThinState formatea automáticamente la unidad flash USB para crear una unidad flash USB de inicio. Este proceso borra todos los datos que se encuentren en la unidad flash USB.

1. Seleccione **Administración > ThinState** en el Panel de control.
2. Seleccione **la imagen de HP ThinPro** y luego seleccione **Siguiente**.
3. Seleccione **hacer una copia de la imagen de HP ThinPro** y luego seleccione **Siguiente**.
4. Seleccione **crear una unidad flash USB de arranque** y luego seleccione **Siguiente**.

   El thin client se reinicia y luego se le pedirá que introduzca una unidad flash USB.
5. Inserte una unidad flash USB en un puerto USB del thin client.
6. Seleccione la unidad flash USB y luego seleccione **Finalizar**.

   Una nueva ventana muestra el progreso. Si surge un problema, seleccione **Detalles** para obtener más información. El escritorio vuelve a aparecer al finalizar la captura.

Implementación de una imagen HP ThinPro con una unidad flash USB

Para implementar una imagen HP ThinPro con una unidad flash USB:

IMPORTANTE: Si detiene una implementación antes de terminar, no se restaurará la imagen anterior y el contenido de la unidad flash del thin client se dañará. En este estado, debe reinstalarse la imagen del thin client mediante una unidad flash USB.

1. Apague la thin client de destino.
2. Inserte la unidad flash USB.
3. Encienda el thin client.

NOTA: La pantalla permanece en negro de 10 a15 segundos mientras el thin client detecta la unidad flash USB y se inicia desde allí. Si la thin client falla en inicializar desde la unidad flash USB, intente desconectar todos los otros dispositivos USB y repita el procedimiento.

Administración de un perfil de cliente

Un perfil de cliente contiene las conexiones, los ajustes y las personalizaciones que configuró mediante el Administrador de conexión y el Panel de control. Un perfil se guarda en un archivo de configuración específico para la versión de HP ThinPro en que se creó.

NOTA: Un perfil también puede configurarse previamente e implementarse usando Profile Editor (Editor de perfiles) y Actualización automática (consulte Profile Editor (Editor de perfiles) en la página 87 y HP Smart Client Services en la página 82 para obtener más información).

Guardar un perfil de cliente en un servidor FTP

Para guardar un perfil de cliente en un servidor FTP:

IMPORTANTE: El directorio del servidor FTP donde desea guardar el perfil ya debe existir antes de comenzar a guardarlo.

1. Seleccione **Administración > ThinState** en el Panel de control.
2. Seleccione **la configuración de HP ThinPro** y luego seleccione **Siguiente**.
3. Seleccione **guardar la configuración** y luego seleccione **Siguiente**.
4. Seleccione **en un servidor FTP** y luego seleccione **Siguiente**.
5. Ingrese la información del servidor FTP en los campos.
6. Seleccione **Finalizar**.

Restauración de un perfil de cliente usando FTP o HTTP

Para restaurar un perfil de cliente usando FTP o HTTP:

1. Seleccione **Administración > ThinState** en el Panel de control.
2. Seleccione **la configuración de HP ThinPro** y luego seleccione **Siguiente**.
3. Seleccione **restaurar una configuración** y luego seleccione **Siguiente**.
4. Seleccione **en un servidor remoto** y luego seleccione **Siguiente**.
5. Seleccione el protocolo FTP o HTTP y luego escriba la información del servidor en los campos.

   NOTA: No son obligatorios los campos **Nombre de usuario** y **Contraseña** si usa el protocolo HTTP.

6. Seleccione **Finalizar**.

Guardar un perfil de cliente en una unidad flash USB

Para guardar un perfil de cliente en una unidad flash USB:

1. Inserte una unidad flash USB en un puerto USB del thin client.
2. Seleccione **Administración > ThinState** en el Panel de control.
3. Seleccione **la configuración de HP ThinPro** y luego seleccione **Siguiente**.
4. Seleccione **guardar la configuración** y luego seleccione **Siguiente**.
5. Seleccione **en una llave USB** y seleccione **Siguiente**.
6. Seleccione la unidad flash USB.
7. Seleccione **Examinar**.
8. Vaya a la ubicación deseada en la unidad flash USB y asigne un nombre de archivo al perfil.

9. Seleccione **Guardar**.
10. Seleccione **Finalizar**.

Restaurar un perfil de cliente desde una unidad flash USB

Para restaurar un perfil de cliente desde una unidad flash USB:

1. Inserte la unidad flash USB que contiene el perfil en un puerto USB del thin client de destino.
2. Seleccione **Administración > ThinState** en el Panel de control.
3. Seleccione **la configuración de HP ThinPro** y luego seleccione **Siguiente**.
4. Seleccione **restaurar una configuración** y luego seleccione **Siguiente**.
5. Seleccione **en una llave USB** y seleccione **Siguiente**.
6. Seleccione la llave USB.
7. Seleccione **Examinar**.
8. Haga doble clic en el archivo de configuración deseado en la llave USB.
9. Seleccione **Finalizar**.

Duplicación VNC

Para acceder a la herramienta Sombreamiento VNC:

Virtual Network Computing (VNC) es un protocolo de escritorio remoto que le permite ver el escritorio de un equipo remoto y controlarlo con su teclado y su mouse locales.

Para aumentar la seguridad, HP recomienda que deje VNC deshabilitado a menos que se necesite para el diagnóstico remoto. Luego, deshabilite VNC cuando ya no sea necesario el acceso remoto al thin client.

▲ Seleccione **Capacidad de administración** y luego **Duplicación VNC** en el Panel de control.

NOTA: Debe reiniciar el thin client antes de que los cambios a las opciones de Duplicación VNC surtan efecto.

La siguiente tabla describe las opciones disponibles en la herramienta Sombreamiento VNC.

Tabla 9-12 Duplicación VNC

Opción	Descripción
Activar Duplicación VNC	Activa la duplicación VNC.
VNC de solo lectura	Hace que la sesión de VNC sea solo de lectura.
Contraseña de usuario VNC	Es obligatorio escribir una contraseña cuando se accede al thin client mediante VNC. Seleccione **Defina Contraseña** para configurar la contraseña.
Mostrar el botón "Detener duplicación"	Si está habilitado, aparece un botón **Detener duplicación** en la esquina superior izquierda del sistema remoto. Detiene la duplicación VNC cuando se presiona.
Permitir solo bucle invertido para VNC	Si está habilitado, solo puede conectarse al servidor de VNC desde este thin client identificado por la dirección de bucle invertido.

Tabla 9-12 **Duplicación VNC (continúa)**

Opción	Descripción
Notificación de VNC al usuario para permitir el rechazo	Activa un cuadro de diálogo de notificación en el sistema remoto que le informa al usuario remoto cuando alguien intenta conectarse utilizando VNC. El usuario puede permitir o rechazar el acceso.
Cerrar automáticamente la notificación tras (segundos)	Cierra el Mensaje de notificación del usuario después de x segundos.
Mensaje de notificación al usuario	Le permite mostrar un mensaje en el cuadro de diálogo notificación al usuario remoto.
Rechazar las conexiones de forma predeterminada	Si está activado, la conexión VNC será rechazada de forma predeterminada cuando se termine el tiempo.
Volver a configurar el servidor VNC ahora	Restablece el servidor VNC después de aplicar los nuevos ajustes.

SNMP

SNMP es un protocolo de red para recopilar y organizar información sobre dispositivos administrados en redes y para modificar esa información para cambiar el comportamiento de los dispositivos.

Se han creado tres versiones de SNMP. SNMPv1 es la versión original, pero SNMPv2c y SNMPv3 son más utilizadas. El daemon HP admite todas las versiones de los protocolos SNMP.

El comportamiento del daemon de SNMP se define por /etc/snmp/snmpd.conf. snmpd.conf, que admite muchas opciones. La interfaz gráfica de usuario (GUI) de ThinPro ofrece soporte limitado para estas opciones, lo que podría ser útil en casos básicos. Debe proporcionar su propio archivo de configuración snmpd si ThinPro GUI no satisface sus necesidades. Debe editar manualmente el archivo /etc/snmp/snmpd.conf. También debe habilitar root/snmp/agentBehaviour/usePrivateConfFile, o la próxima aplicación sobrescribirá sus cambios de configuración.

NOTA: SNMP es un protocolo altamente extensible y personalizable. ThinPro proporciona una herramienta de interfaz gráfica de usuario simple para configurar el agente SNMP en ThinPro. Los usuarios pueden configurar el agente SNMP que permite las consultas básicas de SNMP sobre el dispositivo. Se recomienda a los usuarios que configuren características de SNMP avanzadas, por ejemplo, extender OID privado y usar SNMPv3.

El archivo de configuración del agente SNMP es /etc/snmp/snmpd.conf en ThinPro. Consulte la página de snmpd.conf(5) para obtener detalles sobre la configuración del agente SNMP.

Activación de SNMP con archivo de configuración privada

Puede habilitar SNMP con un archivo de configuración privada.

1. Seleccione **Manageability** > **SNMP** en el panel de control.
2. Seleccione **Habilitar SNMP** para habilitar el agente SNMP en ThinPro.
3. Seleccione **Use el archivo de configuración privada**.
4. Copie el archivo de configuración privada en /etc/snmp/snmpd.conf.
5. Seleccione **Aplicar** para iniciar el agente SNMP.

Activación de SNMP con lista de comunidades

Puede activar SNMP con la Lista de comunidades.

1. Seleccione **Manageability** > **SNMP** en el panel de control.
2. Seleccione **Habilitar SNMP** para habilitar el agente SNMP en ThinPro.
3. Desmarque **Use el archivo de configuración privada**, si está seleccionado.
4. Seleccione Add/Edit/Delete community para cambiar las comunidades SNMP v1/v2c en la **Community List**; puede configurar tres atributos de una comunidad.
   - Escriba el `nombre` de la lista de la comunidad en el campo.
   - Seleccione **Permiso** de solo lectura o lectura-escritura.
   - Escriba `Accessible OID` en la lista de la comunidad en el campo.
5. Seleccione **Aplicar** para iniciar el agente SNMP.

Desactivar SNMP

Siga las instrucciones para desactivar SNMP.

1. Seleccione **Manageability** > **SNMP** en el panel de control.
2. Desmarque **Habilitar SNMP** para desactivar el agente SNMP en ThinPro.
3. Seleccione **Aplicar** para detener el agente SNMP.

Actualización de BIOS Capsule

ThinPro admite la actualización de BIOS Capsule. Debe obtener el paquete del BIOS en formato de cápsula (que generalmente termina con .cap) y luego seguir este procedimiento.

1. Transfiera el paquete del BIOS a ThinClient.
2. Cambie al modo de administrador e inicie un xterm.
3. Ejecute:
   a. `/usr/sbin/hptc-bios-capsule-update <bios file name>`
   b. `reboot -f`
4. Tras el reinicio, el sistema actualiza el BIOS.
4. Verifique la versión del BIOS en sysinfo o mediante el comando dmidecode para comprobar el resultado.

NOTA: No todos los modelos ThinClient y BIOS admiten actualización con cápsula. Cambie al método de actualización del BIOS estándar si falla la actualización del BIOS con cápsula.

Dispositivos de entrada

Esta sección describe los dispositivo de entrada.

Tabla 9-13

Opción de menú	Descripción
Teclado	Le permite cambiar la disposición del teclado para que se adapte al idioma utilizado por los teclados principal y secundario.
Accesos Directos de Teclado	Le permite crear, modificar y eliminar accesos directos del teclado.
Mouse	Le permite configurar la velocidad del mouse y si su funcionamiento será para la mano izquierda o la derecha. En los thin clients con un TouchPad, esta opción de menú también le permite activar y desactivar el TouchPad.
Pantalla táctil	Le permite configurar las opciones de la pantalla táctil.
Ibus	Le permite configurar Ibus (Intelligent Input Bus) para entradas multilingües. Ibus no viene habilitado de manera predeterminada. Para habilitar Ibus: **Panel de control > Dispositivos de entrada > Método de entrada Ibus > Inicial IBUS en el arranque** El archivo de configuración predeterminado de Ibus también se puede modificar o restaurar a las configuraciones de fábrica desde el Panel de control. Después del reinicio, aparece el icono de la bandeja de Ibus. Seleccione el icono para elegir el idioma. Haga clic con el botón derecho en el icono para ver más opciones de configuración. **NOTA:** Ibus en ThinPro viene precargado con los idiomas chino, japonés y coreano. Para agregar idiomas adicionales: 1. Haga clic con el botón derecho en el icono de la bandeja del sistema Ibus. 2. Seleccione la ficha **Método de entrada**. 3. Seleccione **Agregar**.

Hardware

Esta sección describe la configuración del hardware.

Tabla 9-14

Opción de menú	Descripción
Pantalla	Le permite configurar y probar las opciones de pantalla. Para obtener más información, consulte Administración de la pantalla en la página 77.
Sonido	Le permite controlar los niveles de audio de entrada, reproducción y dispositivos de entrada.
Administrador de USB	Le permite configurar las opciones de redirección para los dispositivos USB.

Tabla 9-14 (continúa)

Opción de menú	Descripción
	Para obtener más información, consulte Redirección de dispositivos USB en la página 77.
Administrador serial	Le permite configurar dispositivos serial.
Impresoras	Le permite configurar impresoras de red y locales. Las impresoras locales pueden compartirse en la red. Para obtener más información, consulte Configuración de impresoras en la página 77.
Bluetooth	Permite configurar servicios Bluetooth y conectar dispositivos. Para obtener más información, consulte Bluetooth en la página 78.

Administración de la pantalla

La administración de la pantalla le permite configurar la pantalla y aplicar estos cambios en la sesión. Para abrir la administración de la pantalla:

Panel de Control > Hardware > Administración de la pantalla.

Redirección de dispositivos USB

Para redirigir los dispositivos USB:

1. En el Panel de control, seleccione **Hardware** y luego **Administrador de USB**.
2. En la página **Protocolo**, seleccione un protocolo remoto.

   Si la configuración es **Local**, también puede especificar las opciones **permitir que se monten dispositivos** y **montar dispositivos de solo lectura**.
3. En la página **Dispositivos**, puede activar o desactivar la redirección de dispositivos individuales si es necesario.
4. En la página **Clases**, puede seleccionar clases de dispositivos específicos para que se redirijan a sesiones remotas.
5. Cuando haya terminado, seleccione **Aplicar**.

Configuración de impresoras

Para configurar una impresora:

1. Seleccione **Hardware** y luego **Impresoras** en el Panel de control.
2. En el cuadro de diálogo de **Impresión**, seleccione **Agregar** .
3. En el cuadro de diálogo **Nueva impresora**, seleccione la impresora a configurar y luego seleccione **Avanzar**.

NOTA: Si selecciona una impresora serial, asegúrese de ingresar los ajustes correctos en el lado derecho del cuadro de diálogo, o es posible que la impresora no funcione correctamente.

4. Seleccione el fabricante de la impresora. Si no está seguro, seleccione la opción **Genérico (recomendado)** y luego seleccione **Avanzar**.

5. Seleccione el modelo y el controlador de la impresora y luego, seleccione **Avanzar**.

NOTA: Si no está seguro del modelo de la impresora o qué controlador utilizar, o si el modelo de su impresora no aparece, seleccione **Atrás** y trate de usar la opción **Genérico (recomendado)** para la opción de fabricante de la impresora.

Si utiliza la opción de fabricante **Genérico (recomendado)**, asegúrese de seleccionar **solo texto (recomendado)** para el modelo e **Impresora genérica solo texto [ingl.] (recomendado)** para el controlador.

6. Complete la información opcional acerca de la impresora, como su nombre y ubicación.

NOTA: HP le recomienda escribir el nombre del controlador correcto en el cuadro **Controlador de Windows**. El controlador también debe estar instalado en el servidor de Windows para que la impresora funcione correctamente. Si no se especifica un controlador, se usa un controlador de postscript genérico. El uso de un controlador específico de Windows podría habilitar más funciones en la impresora.

7. Seleccione **Aplicar** y luego imprima una página de prueba, si lo desea.

De ser necesario, repita este proceso para configurar impresoras adicionales.

SUGERENCIA: El problema más común es utilizar el controlador incorrecto para la impresora. Para cambiar el controlador, haga clic con el botón derecho en la impresora y seleccione **Propiedades**, luego cambie el fabricante y el modelo.

Bluetooth

El servicio Bluetooth está desactivado de forma predeterminada. Activar Bluetooth permite que el servicio systemd (Bluez) se inicie desde el inicio. Consulte /etc/system/bluetooth.service.d/10-bluetooth-enabled.conf.

Después de activar el servicio, puede acceder a Bluetooth desde el icono visible en la bandeja del sistema de la barra de tareas.

Decida si los usuarios pueden:

- Ver el icono de Bluetooth en la bandeja del sistema.
- Activar o desactivar la interfaz de Bluetooth.
- Consultar la lista de dispositivos conectados.
- Mostrar el escáner de dispositivos. Puede utilizar el escáner para agregar o eliminar un dispositivo. Los usuarios también pueden eliminar dispositivos con el escáner.

Puede desactivar los mensajes de notificación desde el icono de la bandeja del sistema estableciendo el tiempo de espera en cero.

ThinPro funciona bien con la mayoría de los auriculares, mouse y teclados. Necesita un PIN para emparejarse con un teclado. Es posible que deba ponerse en contacto con el soporte técnico de HP para emparejarse con otros dispositivos.

NOTA: Los dispositivos encontrados por el escáner de dispositivos se filtran de acuerdo con la configuración del registro root/Bluetooth/SystrayApp/DeviceFilter/majorClass y root/Bluetooth/SystrayApp/DeviceFilter/services.

Apariencia

Esta sección describe la configuración de Apariencia.

Tabla 9-15

Opción de menú	Descripción
Administrador de imagen de fondo	Le permite configurar el tema de fondo y mostrar de forma dinámica la información del sistema (como el nombre de host, la dirección de IP, el modelo de hardware y la dirección MAC del thin client) en segundo plano. Para obtener más información, consulte el informe técnico sobre HP ThinPro *"Login Screen Customization"* (disponible solo en inglés).
Centro de personalización	Le permite realizar una de las siguientes acciones: • Alternar entre las configuraciones de ThinPro y Smart Zero • Configurar las opciones del escritorio y la barra de tareas • Seleccionar a qué tipos de conexión y elementos del Panel de control tienen acceso los usuarios finales Para obtener más información, consulte Centro de personalización en la página 79.
Idioma	Le permite mostrar la interfaz de HP ThinPro en un idioma distinto.

Centro de personalización

Siga estas instrucciones para abrir el Centro de personalización.

▲ Seleccione **Apariencia** y luego **Centro de personalización** en el Panel de control.

El botón en la parte superior de la página **Escritorio** puede utilizarse para alternar entre las configuraciones de ThinPro y Smart Zero. Consulte Elección de una configuración de SO en la página 1 para obtener más información sobre las diferencias entre estas dos configuraciones.

NOTA: Cuando cambia de ThinPro a Smart Zero, si configuró una única conexión, esa conexión se utiliza automáticamente como la conexión de Smart Zero. Si configuró varias conexiones, se le solicita que seleccione la conexión que desea utilizar.

Antes de pasar al modo de Smart Zero, se debe deshabilitar la función de autenticación del dominio en el thin client. La autenticación de dominio y el modo de Smart Zero son incompatibles.

La siguiente tabla describe el resto de las opciones disponibles en la página **Escritorio**.

Tabla 9-16 **Opciones de personalización**

Opción	Descripción
Abrir el Administrador de conexión en el inicio	Cuando está activado, el Administrador de conexión se abre automáticamente al iniciar el sistema.
Activar el menú del clic con el botón derecho.	Desactive esta opción si no desea que el menú de contexto aparezca al hacer clic derecho en el escritorio
Activar la seguridad de control de acceso Xhost	Cuando está activada, solo los sistemas enumerados en el área de la **Lista de Control de acceso XHost** pueden controlar el thin client de forma remota.
Activar actualización de USB	Permite instalar actualizaciones desde una unidad flash USB. Consulte actualizaciones de USB en la página 96 para obtener más información.
Autenticar actualización de USB	Desactive esta opción para permitir que los usuarios finales puedan instalar actualizaciones mediante USB.
Permitir al usuario pasar al modo de administrador	Desactive esta opción para eliminar la opción de **Cambio de modo Administrador/Usuario** desde el Panel de control en el modo de usuario.
Tiempo antes de cancelar el modo de administrador	Especifica el tiempo de inactividad (en minutos) después del cual se cancela el modo de administrador. Si se establece en 0 o en número negativo, el modo de administrador nunca se cancelará de forma automática.

Utilice las páginas de **Conexiones** y **Aplicaciones** para seleccionar qué tipos de conexión y aplicaciones del Panel de control están disponibles en el modo de usuario.

Utilice la página **Barra de tareas** para configurar la barra de tareas.

10 Información del sistema

En el menú de Inicio, seleccione **Información del sistema** para ver la información del sistema, la red y el software. La siguiente tabla describe la información que aparece en cada panel.

Tabla 10-1 Información del sistema

Panel	Descripción
General	Muestra información sobre el BIOS, el sistema operativo, la CPU y la memoria.
Red	Muestra información sobre la interfaz de red, el gateway y la configuración de DNS.
Herramientas de red	Ofrece las siguientes herramientas para supervisión y solución de problemas: • **Ping**: especifica una dirección IP de otro dispositivo en la red para intentar establecer contacto. • **Búsqueda de DNS**: use esta herramienta para resolver un nombre de dominio en una dirección IP. • **Rastrear ruta**: use esta herramienta para hacer un rastreo de la ruta de un paquete de red de un dispositivo a otro.
Software Information (Información de software)	Muestra una lista de complementos instalados en la ficha **Paquetes de servicio** e información de la versión de software en la ficha **Software instalado**. **SUGERENCIA:** También puede acceder a la Guía del administrador (este documento) desde esta pantalla.
Licencia de software	Muestra el CLUF del sistema operativo HP ThinPro y, si no tiene licencia automática, información sobre las licencias de ThinPro en el sistema.
Registros del sistema	Muestra los siguientes registros: • Autorización y seguridad • Administrador de conexiones • Arrendamientos de DHCP • Registro general del sistema • Kernel • Administrador de red • Smart Client Services • Servidor X • OneSign En el modo de administrador, el nivel de depuración se puede cambiar para mostrar información adicional que el soporte de HP podría solicitar para solucionar problemas. Seleccione **Diagnóstico** para guardar un archivo de diagnóstico. Para obtener más información, consulte Uso de los diagnósticos del sistema para solucionar problemas en la página 94.

NOTA: Consulte SystemInfo en la página 189 para obtener información acerca de las claves de registro que pueden utilizarse para ocultar las pantallas de información del sistema.

11 HP Smart Client Services

HP Smart Client Services es un conjunto de herramientas del lado del servidor que le permiten configurar perfiles de cliente que pueden distribuirse a una gran cantidad de thin clients. Esta función se llama Actualización automática.

HP ThinPro detecta un servidor de actualización automática en el inicio y configura los valores según corresponda. Esto simplifica la instalación y el mantenimiento del dispositivo

Para obtener HP Smart Client Services, vaya a ftp://ftp.hp.com/pub/tcdebian/SmartClientServices/

Sistemas operativos compatibles

HP Smart Client Services admite los siguientes sistemas operativos:

- Windows Server® 2019
- Windows Server 2016
- Windows 10
- Windows Server 2012 R2
- Windows Server 2012

NOTA: El instalador es solo de 32 bits, pero es compatible con versiones de 32 bits y 64 bits del sistema operativo Windows.

Requisitos previos para HP Smart Client Services

Antes de instalar HP Smart Client Services, compruebe el estado de la instalación y la configuración de los siguientes componentes:

- **Internet Information Services (IIS)**
- **.NET Framework 3.5**

Para obtener información sobre la instalación o activación de estos componentes en el sistema operativo que se está utilizando para el servidor, vaya a http://www.microsoft.com.

Visualización de sitio web de Automatic Update

Instrucciones para visualizar el sitio web de Automatic Update.

1. En el escritorio del servidor, seleccione **Inicio > Panel de control** y luego seleccione **Herramientas administrativas**.
2. Haga doble clic en **Administrador de Internet Information Services (IIS)**.
3. En el panel izquierdo del Administrador de IIS, expanda los siguientes elementos:

   “Nombre de servidor” > Sitios > HP Automatic Update > auto-update

NOTA: La ubicación física donde se almacenan los archivos de Automatic Update es la siguiente:

```
C:\Program Files (x86)\HP\HP Smart Client Service\auto-update
```

Creación de un perfil de Automatic Update

Actualización automática usa perfiles para implementar una configuración en thin clients.

De forma predeterminada, cuando crea un perfil mediante Profile Editor (Editor de perfiles), la herramienta le permite guardarlo en la siguiente carpeta:

```
C:\Program Files (x86)\HP\HP Smart Client Service\auto-
update\PersistentProfile\
```

También puede exportar un perfil existente de un thin client mediante HP ThinState y copiar el perfil en esta ubicación.

Cuando busca actualizaciones, HP ThinPro busca esta carpeta y aplica el perfil guardado en ella. Esto garantiza que todos los thin clients usen la misma configuración.

Para obtener más información sobre el Profile Editor, consulte Profile Editor (Editor de perfiles) en la página 87.

Perfiles específicos de la dirección MAC

Se pueden crear perfiles de Actualización automática para una única dirección MAC. Esto puede resultar útil cuando algunos thin clients necesitan una configuración diferente.

Los perfiles de una sola dirección MAC se deben guardar en el servidor de Actualización automática, en la siguiente carpeta:

```
C:\Program Files (x86)\HP\HP Smart Client Service\auto-
update\PersistentProfile\MAC\
```

Al buscar actualizaciones, HP ThinPro busca primero el perfil genérico y luego un perfil basado en la dirección MAC. Estos perfiles se funden e instalan juntos en el thin client. El perfil basado en la dirección MAC tiene prioridad; es decir, si la misma clave de registro cuenta con un valor diferente en ambos archivos, se usa el valor del perfil basado en la dirección MAC.

Esto garantiza que una configuración compartida se puede brindar a todos los thin clients, pero se puede agregar una personalización específica, si es necesario.

Esta sección describe cómo crear un perfil de Automatic Update` para una sola dirección MAC.

1. Obtenga la dirección MAC del thin client mediante la información del sistema. Por ejemplo, los siguientes pasos utilizan la dirección MAC `00fcab8522ac`.
2. Utilice Profile Editor (Editor de perfiles) para crear o modificar un perfil de cliente (consulte Profile Editor (Editor de perfiles) en la página 87) hasta que esté listo para guardar el perfil del cliente.
3. En **Profile Editor (Editor de perfiles)**, seleccione el enlace **Finish** (Terminar) en el panel izquierdo para acceder al panel **Current profile** (Perfil actual).
4. Seleccione **Save profile as** (Guardar perfil como) para guardar el perfil de cliente de la siguiente forma:

   ```
   C:\Program Files (x86)\HP\HP Smart Client Service\auto-
   update\PersistentProfile\MAC\00fcab8522ac.xml
   ```

5. Seleccione el botón **Finish** (Terminar) en el panel **Current profile** (Perfil actual) para salir de Profile Editor (Editor de perfiles).

6. Reinicie el thin client que utiliza la dirección MAC especificada para iniciar el proceso de actualización automática.

Actualizar thin clients

Uso del método de actualización por transmisión

Para hacer una actualización por transmisión, conecte el thin client a la misma red que el servidor de actualización. Una actualización por transmisión se basa en HP Smart Client Services, que funciona con IIS para forzar automáticamente actualizaciones en el thin client.

NOTA: Las actualizaciones por transmisión solo funcionan si el thin client está en la misma subred que el servidor.

SUGERENCIA: Para verificar que las actualizaciones por transmisión están funcionando, ejecute Profile Editor (Editor de perfiles) y realice algunos cambios. Conecte el thin client y cerciórese de haber descargado el nuevo perfil. Si no lo ha hecho, consulte Solución de problemas en la página 93.

Uso del método de actualización de la etiqueta DHCP

En los sistemas Windows Server, el etiquetado de DHCP permite actualizar un thin client. Utilice este método para actualizar thin clients específicos. Sin embargo, si solo tiene uno o dos thin clients que actualizar, considere el uso del método de actualización manual. De lo contrario, HP recomienda el método de actualización por transmisión.

Ejemplo de realización de etiquetado DHCP

El ejemplo de esta sección muestra cómo realizar el etiquetado DHCP en un servidor Windows 2008 R2.

NOTA: Para utilizar el etiquetado DHCP, consulte la documentación de su servidor DHCP.

1. En el escritorio del servidor, seleccione **Inicio > Herramientas administrativas > DHCP**.

2. En el panel izquierdo de la pantalla de **DHCP**, seleccione el dominio donde están conectados los thin clients.

3. En el panel derecho de la pantalla **DHCP**, expanda y haga clic con el botón derecho del mouse en **IPv4** y luego seleccione **Establecer opciones predefinidas**.

4. En el cuadro de diálogo **Opciones y valores predefinido**, seleccione **Agregar**.

5. En el cuadro **Tipo de opción**, configure las opciones tal como se describe en la siguiente tabla.

Tabla 11-1

Campo	Entrada
Nombre	Introduzca `auto-update`.
Tipo de datos	Seleccione **Cadena**.
Código	Introduzca `137`.

Tabla 11-1 (continúa)

Campo	Entrada
Descripción	Introduzca `HP Automatic Update`.

6. Seleccione **OK**.
7. En el cuadro de diálogo **Opciones y valores predefinidos**, en **Valor > String**, introduzca la dirección del servidor actualizada en el formato del siguiente ejemplo:

   ```
   http://auto-update.dominio.com:18287/auto-update
   ```

8. Para completar la configuración, seleccione **Aceptar**. El etiquetado de DHCP ya está listo para actualizar thin clients específicos.

Uso del método de actualización mediante alias de DNS

Durante el inicio del sistema, la actualización automática intenta resolver **auto-update** del alias de DNS. Si se resuelve ese nombre de host, intentará buscar actualizaciones en **http://auto-update:18287**. Este método de actualización permite que los thin clients accedan a un único servidor de actualización para todo el dominio, lo que simplifica la administración de implementaciones con varias subredes y servidores de DHCP.

Para configurar el método de actualización por alias DNS:

- Cambie el nombre de host del servidor que aloja el HP Smart Client Services a **Actualización automática** o cree un alias DNS de **Actualización automática** para ese servidor.

Uso del método de actualización manual

Utilice el método de actualización manual para conectar un thin client a un servidor específico para una actualización. Use también este método si desea probar una actualización en un único thin client antes de forzar la actualización en muchos thin clients, o si tiene actualizaciones específicas que quiere instalar en solo uno o dos thin clients.

NOTA: Asegúrese de especificar el nombre del host del servidor manual en el perfil que está actualizando. De lo contrario, las configuraciones se restauran al modo automático cuando se descarga el perfil. Use **Profile Editor (Editor de perfiles)** para modificar estas configuraciones en la raíz/actualización automática.

NOTA: Si varios thin clients requieren actualizaciones específicas, utilice el método por etiquetado de DHCP.

Si no necesita dividir las actualizaciones, la actualización por difusión es el método recomendado.

Realización de una actualización manual

Para realizar una actualización manual:

1. Seleccione **Administración > Actualización automática** en el Panel de control.
2. Seleccione **Activar configuración manual**.
3. Defina el **Protocolo** como **http**.

4. En el campo **Servidor**, introduzca el nombre de host y el puerto del servidor de actualización en el siguiente formato:

   ```
   <nombre de host>:18287
   ```

5. En el campo **Ruta**, introduzca lo siguiente:

   ```
   auto-update
   ```

6. Seleccione **Conservar la configuración del thin client** si desea conservar todas las configuraciones previas.

7. Seleccione **Aceptar** y luego el thin client realizará las actualizaciones.

12 Profile Editor (Editor de perfiles)

HP Smart Client Services contiene Profile Editor (Editor de perfiles), que permite a los administradores crear perfiles de cliente y cargarlos en el servidor de Actualización automática.

SUGERENCIA: Además de crear un nuevo perfil de cliente, puede editar un perfil existente que se haya exportado usando HP ThinState.

Un perfil de cliente contiene las conexiones, los ajustes y las personalizaciones que se configuraron mediante el Administrador de conexión y los distintos elementos del Panel de control. Un perfil de cliente se guarda en un archivo de configuración específico para la versión de HP ThinPro en que se haya creado.

Abrir Profile Editor (Editor de perfiles)

Para abrir el Editor de perfiles:

▲ Seleccione **Inicio**, seleccione **Todos los programas**, seleccione **HP**, seleccione **HP Automatic Update Server** y luego **Profile Editor**.

Carga de un perfil de cliente

El nombre del perfil de cliente que se ha cargado actualmente se indica en la pantalla inicial de Profile Editor (Editor de perfiles).

Para cargar un perfil de cliente:

1. En la pantalla inicial de Profile Editor (Editor de perfiles), seleccione el enlace que muestra el nombre del perfil de cliente cargado actualmente.
2. Navegue al perfil de cliente y luego seleccione **Open** (Abrir).

Personalización del perfil de cliente

Selección de la plataforma para un perfil de cliente

Use la pantalla **Platform** (Plataforma) de Profile Editor (Editor de perfiles) para hacer lo siguiente:

- Seleccionar la versión de imagen de HP ThinPro deseada que sea compatible con su hardware
- Elegir entre ThinPro y Smart Zero
- Ver kits de cliente instalados que ofrezcan configuraciones adicionales de registro

NOTA: Los kits de cliente deben colocarse en el siguiente directorio:

```
C:\Program Files (x86)\HP\HP Smart Client Service\auto-update\Packages
```

Para configurar la plataforma del perfil de cliente:

1. En la pantalla **Platform** (Plataforma) de Profile Editor (Editor de perfiles), seleccione una **OS Build ID** (ID de compilación de SO) que corresponda a la versión de imagen deseada.

IMPORTANTE: Asegúrese de crear un perfil de cliente diferente para cada tipo de hardware.

NOTA: Si se instala un kit de cliente, se muestra automáticamente en el cuadro de Kits de cliente y habrá configuraciones adicionales de registro disponibles en la pantalla de registro.

2. Establezca la configuración en **standard** (ThinPro) o **zero** (Smart Zero).

NOTA: En el caso de versiones anteriores de la imagen, esta configuración aparece en gris y se establece en cero de forma automática.

Configuración de una conexión predeterminada para un perfil de cliente

Para configurar una conexión predeterminada para un perfil de cliente:

1. En la pantalla **Connection** (Conexión) de Profile Editor (Editor de perfiles), seleccione el tipo de conexión deseado en la lista desplegable **Type** (Tipo).

NOTA: Los tipos de conexión disponibles varían dependiendo de que haya elegido ThinPro o Smart Zero en la pantalla Platform (Plataforma).

2. En el campo **Server** (Servidor), introduzca el nombre o la dirección IP del servidor.

Modificación de las configuraciones de registro de un perfil de cliente

Para cambiar la configuración predeterminada de registro para un perfil de cliente:

1. En la pantalla **Registry** (Registro) de Profile Editor (Editor de perfiles), amplíe las carpetas en el árbol de **Registry settings** (Configuraciones de registro) para ubicar la configuración de registro que desea cambiar.

2. Seleccione la clave de registro y luego introduzca el valor deseado en el campo **Value** (Valor).

NOTA: Consulte Claves de registro en la página 102 para ver una lista completa y la descripción de las claves de registro.

Agregar archivos a un perfil de cliente

Utilice la pantalla **Files** (Archivos) de Profile Editor (Editor de perfiles) para agregar los archivos de configuración que se instalarán automáticamente en el thin client cuando se haya instalado el perfil de cliente. Esto se suele utilizar por los siguientes motivos:

- Para agregar certificados
- Para modificar la configuración del dispositivo cuando un valor de registro para el cambio no está disponible
- Para modificar el comportamiento del sistema introduciendo scripts personalizados o modificando los scripts existentes

También puede especificar un enlace simbólico que apunta a un archivo ya instalado en el thin client. Utilice esta opción cuando deba acceder al archivo desde más de un directorio.

Agregar un archivo de configuración y certificados a un perfil de cliente

Instrucciones para agregar archivos de configuración y certificados a un perfil de cliente.

Agregar un archivo de configuración a un perfil de cliente

Puede agregar archivos de configuración a un perfil de cliente y especificar la ruta de la carpeta en la que están instalados los archivos.

1. En la pantalla **Files** (Archivos) de Profile Editor (Editor de perfiles), seleccione **Add a file** (Agregar un archivo).
2. Seleccione **Import File** (Importar archivo), ubique el archivo que se va a importar y luego seleccione **Open** (Abrir).

   NOTA: También se pueden exportar archivos mediante el botón **Exportar archivo**, si son necesarios más detalles sobre el archivo.

3. En el campo **Path** (Ruta), introduzca la ruta donde se instalará el archivo en el thin client.
4. En la sección **File details** (Detalles del archivo), establezca los campos **Owner** (Propietario), **Group** (Grupo) y **Permissions** (Permisos) según los valores adecuados.

   NOTA: Por lo general, configurar el propietario y grupo como **raíz** y los permisos como **644** es satisfactorio. Si se requiere un propietario, grupo o permisos adicionales especiales, consulte los permisos de archivo estándar de Unix® para obtener las orientaciones sobre el cambio de los detalles del archivo.

5. Seleccione **Save** (Guardar) para terminar de agregar el archivo de configuración al perfil de cliente.

NOTA: Un archivo instalado como parte de un perfil sobrescribirá automáticamente cualquier archivo existente en el sistema de archivos en la ruta de destino. Además, un segundo perfil sin el archivo adjunto no regresará a los archivos adjuntados previamente. Todos los archivos que se han instalado a través del adjunto del perfil son permanentes y deben revertirse manualmente o mediante el restablecimiento de los valores de fábrica.

Agregar certificados a un perfil de cliente

Los perfiles del cliente incluyen automáticamente certificados que se importan a un almacén de certificados de cliente estándar.

Se admiten los siguientes formatos:

- VMware Horizon View, Citrix, RDP
- Actualización automática
- HP Smart Client Services
- Almacenes de Web browser

Para importar otros certificados a un perfil de cliente:

1. En la pantalla **Files** (Archivos) de Profile Editor (Editor de perfiles), seleccione **Add a file** (Agregar un archivo).

2. Seleccione **Import File** (Importar archivo), ubique el certificado y luego seleccione **Open** (Abrir).

   NOTA: El certificado debe formatearse como un archivo `.pem` o `.crt`.

3. En el campo **Ruta**, defina la ruta de la siguiente manera:

   `/usr/local/share/ca-certificates`

4. Seleccione **Save** (Guardar) para terminar de agregar el certificado al perfil de cliente.

5. Después de instalar el perfil de cliente, utilice el **Administrador de certificados** para confirmar que el certificado se importó correctamente.

Agregar un enlace simbólico a un perfil de cliente

Instrucciones para agregar un enlace simbólico a un perfil de cliente.

1. En la pantalla **Files** (Archivos) de Profile Editor (Editor de perfiles), seleccione **Add a file** (Agregar un archivo).

2. En la lista desplegable **Tipo**, seleccione **Vínculo**.

3. En la sección **Symbolic link details** (Detalles de enlace simbólico), establezca el campo **Link** (Enlace) en la ruta del archivo deseado ya instalado en el thin client.

4. Seleccione **Save** (Guardar) para terminar de agregar el enlace simbólico.

Guardar el perfil de cliente

Instrucciones para guardar el perfil de cliente.

1. En **Profile Editor (Editor de perfiles)**, seleccione **Finish** (Terminar) en el panel izquierdo para acceder a la pantalla **Current profile** (Perfil actual).

2. Seleccione **Save Profile** (Guardar perfil) para guardar el perfil actual de cliente, o seleccione **Save Profile As** (Guardar perfil como) para guardarlo como un nuevo perfil de cliente.

   NOTA: Si se desactiva **Save Profile** (Guardar perfil), su perfil de cliente no ha cambiado desde la última vez que se guardó.

3. Seleccione el botón **Finish** (Terminar) en el panel **Current profile** (Perfil actual) para salir de Profile Editor (Editor de perfiles).

Configuración de impresora en serie o paralela

Puede usar Profile Editor (Editor de perfiles) para establecer los puertos de impresión en serie o paralela. Una impresora USB realiza la asignación automática cuando se conecta.

Cómo obtener los ajustes de la impresora

Antes de configurar los puertos de la impresora, debe obtener los ajustes de esta. Si está disponible, consulte la documentación de la impresora antes de seguir adelante. Si no está disponible, siga estos pasos.

1. En la mayoría de impresoras, mantenga presionado el botón **Alimentación** mientras enciende el dispositivo.

2. Después de unos segundos, suelte el botón **Alimentación**. Esto permite que la impresora entre en un modo de prueba e imprima la información necesaria.

> **SUGERENCIA:** Es posible que necesite apagar la impresora para cancelar el modo de prueba o presionar **Alimentación** nuevamente para imprimir la página de diagnóstico.

Configuración de los puertos de la impresora

Instrucciones para configurar los puertos de la impresora.

1. En **Profile Editor** (Editor de perfiles), seleccione **Registry** (Registro) y marque la casilla de verificación **Show all settings** (Mostrar todas las configuraciones).
2. Active la asignación de puerto de impresora para su tipo de conexión:
   - Citrix: no se requiere ninguna acción.
   - RDP: navegue a **root > ConnectionType > freerdp**. Haga clic derecho en la carpeta **conexiones**, seleccione **Nueva conexión** y luego seleccione **Aceptar**. Establezca la clave de registro **portMapping** en `1` para habilitar la asignación de puerto de la impresora.
   - VMware Horizon View: navegue a **root > ConnectionType > view**. Haga clic derecho en la carpeta **conexiones**, seleccione **Nueva conexión** y luego seleccione **Aceptar**. En la carpeta **xfreerdpOptions**, establezca la clave de registro **portMapping** en `1` para habilitar la asignación de puerto de la impresora.
3. Navegue a **root > Serial**. Haga clic derecho en la carpeta **Serial**, seleccione **New UUID** (Nueva UUID) y luego seleccione **OK** (Aceptar).
4. En el directorio nuevo, ajuste los valores de **baudios**, **dataBits**, **flujo** y **paridad** según los obtenidos en Cómo obtener los ajustes de la impresora en la página 90.

   Establezca el valor de **dispositivo** según el puerto al que se conectará la impresora. Por ejemplo, el primer puerto serial sería `/dev/ttyS0`, el segundo puerto serial sería `/dev/ttyS1`, y así sucesivamente. Para las impresoras seriales USB, utilice el formato `/dev/ttyUSB#`, en que `#` es el número del puerto, comenzando con 0.

Instalación de impresoras en el servidor

Instrucciones para instalar impresoras en el servidor.

1. En el escritorio de Windows, seleccione **Inicio > Impresoras y faxes**.
2. Seleccione **Agregar impresora** y luego seleccione **Siguiente**.
3. Seleccione **Impresora local conectada a este equipo** y, si es necesario, anule **Detectar e instalar mi impresora Plug and Play automáticamente**.
4. Cuando haya terminado, seleccione **Siguiente**.
5. En el menú, seleccione un puerto.

> **NOTA:** El puerto que necesita está en la sección de puertos con la etiqueta **TS###**, donde ### es un número entre 000–009, 033–044. El puerto adecuado depende de su nombre de host y de la impresora que desea instalar. Por ejemplo, con un nombre de host como hptc001 y una impresora de serie, seleccione el puerto con **(hptc001:COM1)**. Para una impresora paralela, seleccione **(hptc001:LPT1)**. El **TS###** es asignado por el Servidor, por lo que no será siempre el mismo.

6. Seleccione el fabricante y el controlador correspondientes a su impresora.

SUGERENCIA: Si lo desea, utilice el disco de controladores **Windows Update** para instalar el controlador.

NOTA: Para impresión básica o de prueba, el **Fabricante genérico** o **Genérico/solo texto** suele funcionar.

7. Si se le pide que mantenga el controlador existente y se sabe que está funcionando, manténgalo y luego seleccione **Siguiente**.

8. Asignar un nombre a la impresora. Para usarla como impresora predeterminada, seleccione **Sí** y luego seleccione **Siguiente**.

9. Para compartir la impresora, seleccione **Compartir nombre** y asignarla a un nombre compartido. De lo contrario, seleccione **Siguiente**.

10. En la siguiente página, puede solicitar una impresión de prueba. HP recomienda hacerlo, ya que así verificará que la configuración de la impresora es correcta. Si la impresora no ha sido configurada adecuadamente, revise las opciones de configuración e inténtelo nuevamente.

NOTA: Si el thin client se desconecta del servidor, la impresora deberá volver a configurarse la próxima vez que se conecta el thin client.

13 Solución de problemas

Solución de problemas de conectividad de red

Instrucciones para solucionar problemas de conectividad de red.

1. Haga ping en un servidor siguiendo estos pasos:

   a. Seleccione el botón de información del sistema en la barra de tareas y luego seleccione la ficha **Herramientas de Red**.

   b. En **Seleccionar herramienta**, seleccione **Ping**.

   c. En la casilla **Host de destino**, introduzca la dirección del servidor y luego seleccione **Empezar el proceso**.

   Si el ping se realiza correctamente, el sistema muestra la siguiente información:

   ```
   Haciendo ping a 10.30.8.52 (10.30.8.52) con 56(84) bytes de datos.

   64 bytes from 10.30.8.52:icmp_seq-1 ttl=64 time=0.81 5 ms 64 bytes
   from 10.30.8.52:icmp_seq=2 ttl=64 time=0.735 ms
   ```

   Si el ping no tiene éxito, el thin client puede estar desconectado de la red y experimentar una demora prolongada sin salida del sistema.

2. Si el thin client no responde al ping, haga lo siguiente:

   a. Compruebe el cable de red y los ajustes de la red en el Panel de control.

   b. Pruebe enviar un ping a otros servidores o thin clients.

   c. Si puede llegar a otros thin clients, compruebe que ha escrito la dirección del servidor correcto.

   d. Envíe el ping al servidor mediante la dirección IP en lugar del nombre de dominio o al revés.

3. Compruebe los registros del sistema haciendo lo siguiente:

   a. Seleccione el botón de información del sistema en la barra de tareas y luego seleccione la ficha **Registros del sistema**.

   b. Compruebe si hay errores en los registros.

   c. Si hay un error, aparecerá la notificación **El servidor no está configurado**. Verifique que el servidor está configurado correctamente y que HP Smart Client Services se está ejecutando.

Solución de problemas para expiración de contraseñas de Citrix

Si no se solicita a los usuarios que cambien las contraseñas vencidas de Citrix, asegúrese de que el sitio de servicios XenApp (sitio PNAgent) tenga el método de autenticación **Solicitar** configurado para permitir que los usuarios cambien las contraseñas vencidas. Si permite que los usuarios cambien sus

contraseñas al conectarse directamente a la controladora de dominio, asegúrese de que la hora del thin client esté sincronizada con la controladora de dominio y use el nombre de dominio completo (por ejemplo, `nombre_dominio.com`) al introducir las credenciales de inicio de sesión de Citrix. Para obtener más información, consulte la documentación de Citrix.

Uso de los diagnósticos del sistema para solucionar problemas

Los diagnósticos del sistema toman una instantánea del thin client que puede utilizarse para ayudar a solucionar los problemas sin acceso físico al thin client. Esta instantánea contiene archivos de registro de la información del BIOS y los procesos activos en el momento en que se ejecutó el diagnóstico del sistema.

SUGERENCIA: Puede cambiar la configuración de **Depuración de nivel** en la ficha **Registros del sistema** de la ventana **Información del sistema** para especificar la cantidad de información que se incluirá en el informe de diagnóstico. HP podría solicitar esta información para solucionar problemas. Debido a que el sistema restablece los archivos de registro cuando se reinicia, asegúrese de capturar los registros antes de un reinicio.

Para obtener los registros más útiles, establezca el nivel para capturar un alto nivel de detalle antes de reproducir el problema y de crear un informe de diagnóstico.

Guardar los datos de diagnóstico del sistema

Instrucciones para guardar los datos de diagnóstico del sistema.

1. Inserte una unidad flash USB en el thin client.
2. Seleccione el botón de información del sistema en la barra de tareas y luego seleccione la ficha **Registros del sistema**.
3. Seleccione **Diagnóstico** y luego guarde el archivo de diagnóstico comprimido **Diagnostic.tgz** en la unidad flash USB.

Descompresión de los archivos de diagnóstico del sistema

El archivo de diagnóstico del sistema **Diagnostic.tgz** está comprimido y deberá descomprimirse antes de poder ver los archivos de diagnóstico.

Descompresión de los archivos de diagnóstico del sistema en sistemas basados en Windows

DESCRIPCIÓN BREVE

1. Descargue e instale una copia de la versión para Windows de **7-Zip**.

   NOTA: Puede obtener una copia gratuita de 7–Zip para Windows en http://www.7-zip.org/download.html.

2. Inserte la unidad flash USB que contiene el archivo de diagnóstico del sistema guardado y luego copie **Diagnostic.tgz** en el escritorio.
3. Haga clic con el botón secundario en **Diagnostic.tgz** y seleccione **7-Zip>Extraer archivos**.
4. Abra la carpeta recién creada con el nombre **Diagnóstico** y repita el paso 3 con **Diagnostic.tar**.

Descompresión de los archivos de diagnóstico del sistema en sistemas basados en Linux o Unix

Instrucciones para descomprimir los archivos de diagnóstico del sistema en sistemas basados en Linux o Unix.

1. Inserte la unidad flash USB que contiene el archivo de diagnóstico del sistema guardado y luego copie **Diagnostic.tgz** para el directorio inicial.
2. Abra una terminal y explore hasta el directorio inicial.
3. En la línea de comandos, ingrese `tar xvfz Diagnostic.tgz`.

Visualización de los archivos de diagnóstico del sistema

Los archivos de diagnóstico del sistema archivos se dividen entre las carpetas **Comandos**, **/var/log** y **/etc**.

Visualización de archivos en la carpeta Comandos

Esta tabla describe los archivos que se deben buscar en la carpeta **Comandos**.

Tabla 13-1 Archivos en la carpeta Comandos

Archivo	Descripción
demidecode.txt	Este archivo contiene información sobre el BIOS del sistema y gráficos.
dpkg_--list.txt	Este archivo indica los paquetes instalados en el momento en que se ejecutó el diagnóstico del sistema.
ps_-ef.txt	Este archivo indica los procesos activos en el momento en que se ejecutó el diagnóstico del sistema.

Visualización de archivos en la carpeta var/log

El archivo útil de la carpeta **/var/log** es **Xorg.0.log**.

Visualización de archivos en la carpeta /etc

La carpeta **/etc** contiene el sistema de archivos en el momento en que se ejecutó el diagnóstico del sistema.

A actualizaciones de USB

Cuando las actualizaciones de USB están activadas, puede usar una unidad flash USB para instalar simultáneamente múltiples complementos y certificados, así como para implementar un perfil.

Para obtener más información sobre cómo activar las actualizaciones USB, consulte Centro de personalización en la página 79.

actualizaciones de USB

Siga estas instrucciones para activar las actualizaciones USB.

Cuando las actualizaciones de USB están activadas (consulte Centro de personalización en la página 61), puede usar una unidad flash USB para instalar simultáneamente múltiples complementos y certificados, así como para implementar un perfil.

1. Coloque los archivos deseados en una unidad flash USB.

   NOTA: Los archivos se pueden colocar en el directorio raíz o en las subcarpetas.

2. Conecte la unidad flash USB al thin client.

   Las actualizaciones se detectan automáticamente y se muestran en el cuadro de diálogo de **Actualización USB**, donde puede buscar y ver detalles sobre las actualizaciones detectadas.

3. Seleccione las casillas de verificación junto a las actualizaciones que desea instalar y luego seleccione **Instalar**.

4. Después de la instalación, reinicie al thin client si se le solicita.

HP ThinUpdate

HP ThinUpdate le permite descargar imágenes y complementos de HP y crear unidades flash USB de inicio para la implementación de la imagen. Para obtener más información, consulte la *Guía del administrador* de HP ThinUpdate.

B Herramientas del BIOS (solo thin clients de escritorio)

Existen dos tipos de herramientas del BIOS para HP ThinPro:

- Herramienta de ajustes del BIOS: se usa para recuperar o modificar los ajustes del BIOS
- Herramienta de actualización del BIOS: se usa para actualizar el BIOS

Estas herramientas se pueden ejecutar mediante una terminal X.

Herramienta de ajustes del BIOS

La siguiente tabla describe la sintaxis para la herramienta de configuraciones del BIOS.

NOTA: Los cambios no entran en efecto hasta el siguiente reinicio.

Tabla B-1

Sintaxis	Descripción
`hptc-bios-cfg -G <nombre del archivo>`	Recupera los ajustes actuales del BIOS y los guarda en un archivo especificado para que se puedan visualizar o modificar (CPQSETUP.TXT de forma predeterminada).
`hptc-bios-cfg -S <nombre del archivo>`	Escribe los ajustes del BIOS desde el archivo especificado (CPQSETUP.TXT de forma predeterminada) al BIOS.
`hptc-bios-cfg -h`	Muestra una lista de opciones.

Herramienta de copia del BIOS

La siguiente tabla describe la sintaxis para la herramienta de copia del BIOS.

NOTA: Los cambios no entran en efecto hasta el siguiente reinicio.

Tabla B-2 Sintaxis para la herramienta de actualización del BIOS

Sintaxis	Descripción
`hptc-bios-flash <nombre de la imagen>`	Prepara el sistema para actualizar el BIOS durante el siguiente reinicio. Este comando copia de forma automática los archivos en el lugar correcto y le pide que reinicie el thin client. **NOTA:** Este comando requiere que la opción **Tool-less update** (Actualización sin herramientas) en las configuraciones del BIOS esté establecida en **Auto**.
`hptc-bios-flash -h`	Muestra una lista de opciones.

C Cambiar el tamaño de la partición de la unidad flash

Para usar el espacio completo de la unidad flash, tiene que modificar el tamaño de la partición y ampliar el sistema de archivos para que ocupe ese espacio adicional. Esto se logra con el script `resize-image` a través de una terminal X.

IMPORTANTE: Los thin clients HP que se envían de fábrica con HP ThinPro utilizan toda la unidad flash. Los métodos de captura de imagen capturan la imagen más reducida posible, lo que permite implementar las imágenes de unidades flash más grandes en unidades flash menores con suficiente espacio para la imagen capturada. Ya no será necesario cambiar el tamaño de la partición de la unidad flash para los thin clients HP que se envían de fábrica con HP ThinPro. En el caso de los thin clients con HP ThinPro que no estén utilizando toda la unidad flash por cualquier motivo, consulte la siguiente información.

NOTA: Cuando se implementa una imagen a través de HPDM, HP ThinState o Actualización automática, el sistema de archivos se redimensiona de forma automática para utilizar todo el espacio disponible en la unidad flash.

La siguiente tabla describe la sintaxis para el comando `resize-image`

Tabla C-1 Sintaxis para el script de cambio de tamaño de la imagen

Sintaxis	Descripción
`resize-image`	Cuando se llama con ningún parámetro, la secuencia de comandos muestra el tamaño actual de la partición y la cantidad de espacio disponible en la unidad flash. La línea de comandos le pedirá que introduzca el tamaño de la partición objetivo y que luego confirme el cambio. El cambio surte efecto después del próximo reinicio de thin client. **NOTA:** No es posible disminuir el tamaño de la partición. El valor ingresado debe ser mayor que el tamaño actual de la partición.
Ejemplo: `resize-image --size 1024`	Con esta sintaxis, puede especificar el tamaño de la partición de destino en megabytes (MB) como un parámetro y luego confirmar el cambio.

`resize-image --no-prompt`
 	
O bien:
 	
`resize-image --no-prompt --size <size in MB>`
 	
Ejemplo: `resize-image --no-prompt --size 1024`
	Con esta sintaxis, la secuencia de comandos se ejecuta automáticamente sin necesidad de la interacción del usuario.
	
	Si no se proporciona un tamaño específico como parámetro simultáneamente, el tamaño de la partición se aumenta al tamaño máximo.
	
	SUGERENCIA: Este modo no interactivo es útil para secuencias de comandos y para realizar esta operación desde una herramienta de administración remota como HP Device Manager.

D comando mclient

El comando cliente para manticore daemon es mclient, que mantiene el registro de configuración y aplica nuevas configuraciones. Necesita ser root para utilizar el comando mclient en la mayoría de los casos. Puede obtener ayuda sobre mclient si ejecuta mclient sin ningún tipo de argumento.

ThinPro 7.2 admite actualmente los siguientes comandos:

```
# mclient
MANTICORE Registry command line frontend

mclient [--quiet] <command>

comandos mclient:
  wait-daemon [timeout seconds]
  set <regkey> <regvalue> [regparam]
  get <regkey> [regparam] | [regparam lang]
  gettree <regkey> [regparam] | [regparam lang]
  contains <regkey>
  commit [regkey]
  [--sync] apply [regkey]
  rollback [regkey]
  watch <regkeylist> [timeout]
  changes
  create <regkey> [keytype]
  delete <regkey>
  import <file>
  export <rootDir> <file>

args mclient:
  regkey : string
  regkeylist : string space separated
  regvalue : string
  regparam : string (value|type|regexp|description)
  timeout : int
  keytype : string (string|rc4|uuid|char|ipv4|ipv6|ipaddr|number|float|
date|bool|crypt|encrypted)
```

Además, puede obtener la capacidad de autocompletar de bash después de ejecutar el siguiente comando en ThinPro:

```
# . /etc/bash_completion.d/mclient
```

Las modificaciones en el registro de configuración se realizan en tres pasos:

1. Agregar, modificar o eliminar el valor.
2. Publique el comando `mclient commit` para confirmar el cambio y guardar los cambios en el disco.

3. Publique el comando `mclient apply` para aplicar los cambios.

NOTA: HP recomienda realizar un reinicio completo para confirmar las nuevas configuraciones.

Otros usos útiles de mclient son:

Puede utilizar la exportación de mclient y la importación de mclient para exportar o importar una rama del registro. Estos comandos son útiles si necesita exportar una conexión o una configuración Wi-Fi, pero no toda la configuración.

Por ejemplo, si ha configurado una conexión Wi-Fi en ThinPro, puede averiguar la rama del registro donde se guarda esta configuración:

```
# mclient -q get root/Network/Wireless/Profiles
root/Network/Wireless/Profiles/{de0ff9cb-7f9d-48ba-9ac3-89d28cfad469}#
mclient -q get root/Network/Wireless/Profiles/
{de0ff9cb-7f9d-48ba-9ac3-89d28cfad469}/SSID
NETGEAR89-5G
```

NOTA: `{de0ff9cb-7f9d-48ba-9ac3-89d28cfad469}` es la muestra de UUID que se encuentra en el sistema de prueba. Es posible que tenga un UUID diferente para su configuración de conexión.

Luego, puede exportar a configuración usando este comando:

```
# mclient export root/Network/Wireless/Profiles/
{de0ff9cb-7f9d-48ba-9ac3-89d28cfad469} wifi.xml
```

El resultado wifi.xml se puede importar a otras máquinas más adelante.

La herramienta `/usr/bin/mencrypt` puede ser conveniente para establecer el valor de las claves de registro con un tipo cifrado, por ejemplo:

```
# mclient set root/Network/
Wireless/Profiles/{ de0ff9cb-7f9d-48ba-9ac3-89d28cfad469}/Security/PSK/
PreSharedKey "$(echo -n 'my shared key' | mencrypt)"
# mclient commit root/Network
# mclient apply root/Network
```

E Claves de registro

Las claves de registro de HP ThinPro se agrupan en carpetas y se pueden modificar de varias formas diferentes:

- Use una tarea **_File and Registry** en HPDM.
- Use el componente Editor de registro en Profile Editor y luego implemente el nuevo perfil.
- Use el Editor de registro en la interfaz de usuario de HP ThinPro, disponible en el menú de Herramientas en el modo de administrador.

Cada sección del nivel superior en este apéndice corresponde a una de las carpetas de registro de nivel superior.

NOTA: Es posible que algunas claves de registro se apliquen solo a ThinPro o Smart Zero.

Audio

Claves de registro de audio.

Tabla E-1 Claves de registro de audio

Clave de registro	Descripción
`root/Audio/AdjustSoundPath`	Establece la ruta completa al sonido reproducido cuando el volumen de reproducción cambia a través de los controles de volumen.
`root/Audio/JackRetask`	Esta clave de registro se aplica solo a los thin clients que cuentan con conectores que se pueden adaptar de acuerdo con el objetivo. Para el puerto frontal inferior del t730: • 0/1: No hay cambios / auriculares • 2: Micrófono Para el puerto posterior del t630: • 0: No hay cambios / entrada de línea • 1: Auriculares / salida de línea Debe reiniciar el thin client después de cambiar estas configuraciones.
`root/Audio/OutputMute`	Si se configura en 1, se desactivan el conector de auriculares y el altavoz interno.
`root/Audio/OutputScale`	Establece la escala de volumen del conector de auriculares y el altavoz interno, de 1 a 400.
`root/Audio/OutputScaleAuto`	Si se establece en 1, el valor de `OutputScale` se configurará automáticamente según en el modelo de thin client.
`root/Audio/OutputVolume`	Establece el volumen del conector de auriculares y el altavoz interno, de 1 a 100.

Tabla E-1 Claves de registro de audio (continúa)

Clave de registro	Descripción
`root/Audio/PlaybackDevice`	Establece el dispositivo que se utiliza para la reproducción.
`root/Audio/PulseBuffer`	El rango recomendado para este valor es entre 1024 y 8192. Un valor demasiado alto podría producir inestabilidad en la reproducción, y un valor demasiado bajo podría hacer que el thin client falle.
`root/Audio/RecordDevice`	Establece el dispositivo que se utiliza para la captura.
`root/Audio/RecordMute`	Si se establece en 1, el conector de micrófono está en silencio.
`root/Audio/RecordScale`	Establece la escala de volumen del conector de micrófono, de 1 a 400.
`root/Audio/RecordScaleAuto`	Si se establece en 1, el valor de `RecordScale` se configurará automáticamente según en el modelo de thin client.
`root/Audio/RecordVolume`	Establece el volumen del conector de micrófono, de 1 a 100.
`root/Audio/VisibleInSystray`	Si se establece en 1, aparece un icono del altavoz visible en la bandeja del sistema.
`root/Audio/shortcutPassThrough`	Define las aplicaciones que permiten que pasen los atajos del audio mediante una lista separada por espacios. Las opciones disponibles son `freerdp`, `view` y `xen`.

Bluetooth

Claves de registro de Bluetooth.

Tabla E-2 Claves de registro de Bluetooth

Clave de registro	Descripción
`root/Bluetooth/enableBluetotoh`	Si se establece en 1, se inicia el servicio Bluetooth.
`root/Bluetooth/visibleInSystemTray`	Si está configurado en 1 y también en `enableBluetooth`, aparece el icono de Bluetooth en la bandeja del sistema.
`root/Bluetooth/SystrayApp/DeviceFilter/majorClass`	Filtro de clase de dispositivo principal. Lista separada por punto y coma de los números decimales de las clases de dispositivo. Se ignora la cadena después de dos puntos. Las clases conocidas son 0:Miscellaneous; 1:Computer; 2:Phone; 3:LAN/Network Access Point; 4:Audio/Video; 5:Peripheral; 6:Imaging; 7:Wereable; 8:Toy; 9:Health; 31:Uncategorized. Los dispositivos que anuncian una de las clases especificadas se muestran en el escáner de dispositivos. Filtrado más relevante con dispositivos Bluetooth clásicos. Una cadena vacía desactiva el filtro.
`root/Bluetooth/SystrayApp/DeviceFilter/services`	Filtro de servicios. Lista separada por punto y coma de UUID de 16 bits o UUID de 128 bits completos. Se ignora la cadena después de dos puntos. Los UUID de 16 bits se completan con el sufijo 0000-1000-8000-00805f9b34fb para obtener un UUID de 128 bits con servicio Bluetooth completo. Los Servicios pertinentes de GATT se definen aquí: https://www.bluetooth.com/specifications/gatt/services/. Los dispositivos que anuncian uno de los UUID especificados se muestran en el escáner. Filtrado más relevante

Tabla E-2 Claves de registro de Bluetooth (continúa)

Clave de registro	Descripción
	con dispositivos Bluetooth Smart. Una cadena vacía desactiva el filtro. NOTA: El filtro de servicios se pasa por alto cuando la clase de dispositivo principal de un dispositivo determinado coincide con el filtro de clase de dispositivo principal.
root/Bluetooth/SystrayApp/devices	Si se establece en 1, se mostrarán los dispositivos remotos Bluetooth emparejados y conectados.
root/Bluetooth/SystrayApp/messageTimeout	Tiempo en segundos para mostrar las notificaciones de mensajes en la parte superior del icono de la bandeja del sistema. Si se establece en 0, se desactivan las notificaciones. Puede abrirse una notificación cuando se acaba de conectar un dispositivo, por ejemplo.
root/Bluetooth/SystrayApp/scanner	Si se establece en 1, aparecerá el escáner de Bluetooth. También es posible agregar o eliminar dispositivos remotos Bluetooth emparejados con esta configuración.
root/Bluetooth/SystrayApp/switch	Si se establece en 1, aparecerá el interruptor de Bluetooth para activar o desactivar el adaptador Bluetooth.

CertMgr

Esta categoría del registro se utiliza internamente y no tiene entradas definidas por el usuario.

ComponentMgr

Clave de registro de ComponentMgr.

Tabla E-3 Clave de registro de ComponentMgr

Clave de registro	Descripción
root/ComponentMgr/ NotShowDeleteSnapshotWarning	Si se establece en 1, no se mostrará la información de advertencia mientras se elimina una instantánea.

ConnectionManager

Claves de registro de ConnectionManager.

Tabla E-4 Claves de registro de ConnectionManager

Clave de registro	Descripción
root/ConnectionManager/ createSampleConnections	Si se establece en 1, en el primer inicio, se crean en el escritorio ejemplos de iconos de conexión que el usuario puede modificar.
root/ConnectionManager/customLogoPath	

Tabla E-4 Claves de registro de ConnectionManager (continúa)

Clave de registro	Descripción
root/ConnectionManager/defaultConnection	Para iniciar adecuadamente una conexión al inicio, esta opción debe establecerse en una conexión válida mediante el formato <tipo>:<etiqueta>, como en el ejemplo siguiente: xen:Default Connection.
root/ConnectionManager/minHeight	
root/ConnectionManager/minWidth	
root/ConnectionManager/splashLogoPath	Establece la ruta completa a la imagen que aparece mientras se está cargando una conexión.
root/ConnectionManager/useKioskMode	
root/ConnectionManager/ useSplashOnConnectionStartup	Si se establece en 1, se activa la imagen definida por splashLogoPath. De forma predeterminada, esta opción está activada para ThinPro y desactivada para Smart Zero.

ConnectionType

custom

Claves de registro de ConnectionType/custom.

Tabla E-5 Claves de registro de ConnectionType/custom

Clave de registro	Descripción
root/ConnectionType/custom/authorizations/ user/add	Si se establece en 1, un usuario final tiene permiso para agregar una nueva conexión de este tipo utilizando el Administrador de conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/custom/authorizations/ user/general	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones generales para este tipo de conexión utilizando el Administrador de conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/custom/connections/ <UUID>/afterStartedCommand	Establece el comando que se debe ejecutar después de que se ha iniciado la conexión.
root/ConnectionType/custom/connections/ <UUID>/afterStoppedCommand	Establece el comando que se debe ejecutar después de que se ha detenido la conexión.
root/ConnectionType/custom/connections/ <UUID>/authorizations/user/edit	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones para esta conexión.
root/ConnectionType/custom/connections/ <UUID>/authorizations/user/execution	Si se establece en 1, un usuario final tiene permiso para ejecutar esta conexión.
root/ConnectionType/custom/connections/ <UUID>/autoReconnect	Si se establece en 1, la conexión se reiniciará cuando se cierre o desconecte.

Tabla E-5 Claves de registro de ConnectionType/custom (continúa)

Clave de registro	Descripción
root/ConnectionType/custom/connections/<UUID>/autoReconnectDelay	Establece la cantidad de tiempo en segundos que se deben esperar antes de volver a conectar la sesión. El valor predeterminado 0 hará que la conexión se reactive inmediatamente. Esta configuración solo surte efecto cuando autoReconnect se establece en 1.
root/ConnectionType/custom/connections/<UUID>/autostart	Si se establece en un valor de 1 a 5, la conexión se iniciará automáticamente después de que arranque el sistema, con el valor de 1 con la prioridad más alta.
root/ConnectionType/custom/connections/<UUID>/beforeStartingCommand	Establece que se ejecute el comando antes de que empiece la conexión.
root/ConnectionType/custom/connections/<UUID>/command	Establece que se ejecute el comando principal de la conexión personalizada.
root/ConnectionType/custom/connections/<UUID>/connectionEndAction	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/custom/connections/<UUID>/coord	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/custom/connections/<UUID>/dependConnectionId	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/custom/connections/<UUID>/extraEnvValues/<UUID>/key	Establece el nombre de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/custom/connections/<UUID>/extraEnvValues/<UUID>/value	Establece el valor de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/custom/connections/<UUID>/fallBackConnection	Establece la conexión alternativa a través de su UUID.
root/ConnectionType/custom/connections/<UUID>/hasDesktopIcon	Si se establece en 1, se activa el icono del escritorio para esta conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/custom/connections/<UUID>/iconPosition	Establece las coordinadas x,y de un icono de escritorio fijo. Si no se especifica, el icono queda flotante.
root/ConnectionType/custom/connections/<UUID>/label	Establece el nombre de conexión que se muestra en la interfaz de usuario. En Smart Zero, por lo general esta opción se establece en Default Connection y no aparece en la interfaz de usuario.
root/ConnectionType/custom/connections/<UUID>/startMode	Si se ajusta en el valor predeterminado focus (concentrar) y la conexión se ha iniciado, la conexión se concentrará. De lo contrario, aparecerá un error que indica que la conexión ya se ha iniciado.
root/ConnectionType/custom/connections/<UUID>/waitForNetwork	Si se establece en 1, la conexión no se iniciará hasta que la red esté disponible. Esto garantiza que, en una red lenta, la conexión no se inicie antes de que la red esté disponible, lo que podría provocar una falla.
root/ConnectionType/custom/coreSettings/USBrelevant	Especifica si este tipo de conexión es relevante para el USB. Si es así, puede tener un complemento USB para redirigir dispositivos USB.

Tabla E-5 Claves de registro de ConnectionType/custom (continúa)

Clave de registro	Descripción
root/ConnectionType/custom/coreSettings/appName	Establece el nombre de la aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/custom/coreSettings/className	Establece el nombre de la clase de aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/custom/coreSettings/editor	Establece el nombre de la aplicación interna que se utiliza cuando se inicia el Administrador de conexión para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/custom/coreSettings/generalSettingsEditor	Establece el nombre de la aplicación interna que se utiliza cuando se inicia el Administrador de ajustes generales para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/custom/coreSettings/icon	Especifica el icono del conjunto de temas de iconos que se pueden usar con esta conexión.
root/ConnectionType/custom/coreSettings/icon16Path	Establece la ruta al icono de 16 x 16 píxeles para esta aplicación.
root/ConnectionType/custom/coreSettings/icon32Path	Establece la ruta al icono de 32 x 32 píxeles para esta aplicación.
root/ConnectionType/custom/coreSettings/icon48Path	Establece la ruta al icono de 48 x 48 píxeles para esta aplicación.
root/ConnectionType/custom/coreSettings/iconActive	Reservado para uso futuro.
root/ConnectionType/custom/coreSettings/label	Establece el nombre que se va a mostrar para este tipo de conexión en la interfaz de usuario.
root/ConnectionType/custom/coreSettings/priorityInConnectionLists	Establece la prioridad de este tipo de conexión cuando se muestra en el Administrador de conexiones y en el asistente de configuración que aparece durante la configuración inicial. Un valor más alto mueve el tipo de conexión hacia la parte superior de la lista. Si se establece en 0, el tipo de conexión se oculta del asistente de configuración y aparece de último en el Administrador de conexiones. Los tipos de conexión con la misma prioridad se enumeran en orden alfabético.
root/ConnectionType/custom/coreSettings/serverRequired	Establece si un nombre o dirección de servidor es `unused`, `optional` o `required` para este tipo de conexión.
root/ConnectionType/custom/coreSettings/stopProcess	Establece el comportamiento que debería ocurrir cuando se llama `connection-mgr stop` en esta conexión. De forma predeterminada, está opción es `close`, lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como `kill`, el proceso especificado por `appName` se interrumpirá de forma forzada. Cuando se establece como `custom` se ejecutará una línea de comandos de ejecución personalizada especificada por `wrapperScript` con el argumento `stop` para finalizar el proceso correctamente.
root/ConnectionType/custom/coreSettings/tier	Especifica la importancia relativa de este tipo de conexión y el orden en el que se enumera en el menú Crear.

Tabla E-5 Claves de registro de ConnectionType/custom (continúa)

Clave de registro	Descripción
root/ConnectionType/custom/coreSettings/watchPid	Si se establece en 1, la conexión se supervisa bajo el nombre especificado por appName. No debería ser necesario modificar esta clave.
root/ConnectionType/custom/coreSettings/wrapperScript	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Este es el script principal que administra todos los ajustes de conexión y argumentos de línea de comandos para la conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/custom/gui/CustomManager/name	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/custom/gui/CustomManager/status	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/custom/gui/CustomManager/title	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/custom/gui/CustomManager/widgets/autoReconnect	Controla el estado del widget **Reconexión automática** en el Administrador de conexión Custom. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/custom/gui/CustomManager/widgets/autostart	Controla el estado del widget **Prioridad de inicio automático** en el Administrador de conexión Custom. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/custom/gui/CustomManager/widgets/command	Controla el estado del widget **Ingrese el comando a ejecutar** en el Administrador de conexión Custom. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/custom/gui/CustomManager/widgets/fallBackConnection	Controla el estado del widget **Conexión de Seguridad** en el Administrador de conexión Custom. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/custom/gui/CustomManager/widgets/hasDesktopIcon	Controla el estado del widget **Mostrar icono en escritorio** en el Administrador de conexión Custom. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/custom/gui/CustomManager/widgets/label	Controla el estado del widget **Nombre** en el Administrador de conexión Custom. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.

Tabla E-5 Claves de registro de ConnectionType/custom (continúa)

Clave de registro	Descripción
root/ConnectionType/custom/gui/CustomManager/widgets/waitForNetwork	Controla el estado del widget **Esperando por red antes de conectar** en el Administrador de conexión Custom. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.

firefox

Claves de registro de ConnectionType/firefox.

Tabla E-6 Claves de registro de ConnectionType/firefox

Clave de registro	Descripción
root/ConnectionType/firefox/authorizations/user/add	Si se establece en 1, un usuario final tiene permiso para agregar una nueva conexión de este tipo utilizando el Administrador de conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/firefox/connections/<UUID>/address	Establece la dirección URL o IP a la cual conectarse.
root/ConnectionType/firefox/connections/<UUID>/afterStartedCommand	Establece el comando que se debe ejecutar después de que se ha iniciado la conexión.
root/ConnectionType/firefox/connections/<UUID>/afterStoppedCommand	Establece el comando que se debe ejecutar después de que se ha detenido la conexión.
root/ConnectionType/firefox/connections/<UUID>/authorizations/user/edit	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones para esta conexión.
root/ConnectionType/firefox/connections/<UUID>/authorizations/user/execution	Si se establece en 1, un usuario final tiene permiso para ejecutar esta conexión.
root/ConnectionType/firefox/connections/<UUID>/autoReconnect	Si se establece en 1, la conexión se reiniciará cuando se cierre o desconecte.
root/ConnectionType/firefox/connections/<UUID>/autoReconnectDelay	Establece la cantidad de tiempo en segundos que se deben esperar antes de volver a conectar la sesión. El valor predeterminado 0 hará que la conexión se reactive inmediatamente. Esta configuración solo surte efecto cuando autoReconnect se establece en 1.
root/ConnectionType/firefox/connections/<UUID>/autostart	Si se establece en un valor de 1 a 5, la conexión se iniciará automáticamente después de que arranque el sistema, con el valor de 1 con la prioridad más alta.
root/ConnectionType/firefox/connections/<UUID>/autostartDelay	Reservado para uso futuro.
root/ConnectionType/firefox/connections/<UUID>/beforeStartingCommand	Establece que se ejecute el comando antes de que empiece la conexión.
root/ConnectionType/firefox/connections/<UUID>/connectionEndAction	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.

Tabla E-6 Claves de registro de ConnectionType/firefox (continúa)

Clave de registro	Descripción
root/ConnectionType/firefox/connections/<UUID>/coord	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/firefox/connections/<UUID>/dependConnectionId	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/firefox/connections/<UUID>/enablePrintDialog	Si se establece en 1, puede usarse el cuadro de diálogo de impresión en el explorador web.
root/ConnectionType/firefox/connections/<UUID>/enableSmartCard	Si se establece en 1, se habilita el inicio de sesión con smart card en las conexiones Citrix creadas mediante el navegador web.
root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/key	Establece el nombre de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/value	Establece el valor de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/firefox/connections/<UUID>/fallBackConnection	Establece la conexión alternativa a través de su UUID.
root/ConnectionType/firefox/connections/<UUID>/forbiddenFiles	Esta clave de registro solo funciona cuando está seleccionado **Permitir que las conexiones administren sus propias configuraciones** en el Administrador de configuraciones generales de la conexión Web Browser. Los archivos enumerados en el valor de esta clave de registro se eliminarán cuando finalice una conexión Web Browser. Los nombres de archivo deben separarse por comas y se admite un comodín. Por ejemplo: `*.rdf,cookies.sqlite`
root/ConnectionType/firefox/connections/<UUID>/fullscreen	Si se establece en 1, el explorador web se iniciará en modo de pantalla completa. Si `kioskMode` está desactivado, se puede acceder a la UI del navegador en modo de pantalla completa.
root/ConnectionType/firefox/connections/<UUID>/hasDesktopIcon	Si se establece en 1, se activa el icono del escritorio para esta conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/firefox/connections/<UUID>/iconPosition	Establece las coordinadas x,y de un icono de escritorio fijo. Si no se especifica, el icono queda flotante.
root/ConnectionType/firefox/connections/<UUID>/intendedUse	Establece el uso previsto de esta conexión Web Browser en `Citrix`, `RDP` o `Internet`.
root/ConnectionType/firefox/connections/<UUID>/kioskMode	Si se establece en 1, el explorador web se iniciará en el modo quiosco, lo que significa que el explorador web se iniciará en pantalla completa (incluso si `fullscreen` está establecido en 0) y no se puede acceder a la UI del navegador.
root/ConnectionType/firefox/connections/<UUID>/label	Establece el nombre de conexión que se muestra en la interfaz de usuario. En Smart Zero, por lo general esta opción se establece en `Default Connection` y no aparece en la interfaz de usuario.
root/ConnectionType/firefox/connections/<UUID>/manageOwnPrefs	Si se establece en 1, la conexión administra sus propias preferencias y las almacena en la siguiente ubicación: `/etc/firefox/<UUID>`. Si se establece en 0, la conexión usa las preferencias compartidas.
root/ConnectionType/firefox/connections/<UUID>/showBackForwardButton	Si se establece en 1, los botones Atrás y Adelante del navegador web se muestran cuando está habilitado el modo quiosco.

Tabla E-6 Claves de registro de ConnectionType/firefox (continúa)

Clave de registro	Descripción
root/ConnectionType/firefox/connections/<UUID>/showHomeButton	Si se establece en 1, el botón Inicio del navegador web se muestran cuando está habilitado el modo quiosco.
root/ConnectionType/firefox/connections/<UUID>/showSearchBar	Si se establece en 1, la barra de búsqueda del navegador web se muestran cuando está habilitado el modo quiosco.
root/ConnectionType/firefox/connections/<UUID>/showTabsBar	Si se establece en 1, las fichas del navegador web se muestran cuando está habilitado el modo quiosco.
root/ConnectionType/firefox/connections/<UUID>/showTaskBar	Si se establece en 1, la barra de tareas del navegador web se muestran cuando está habilitado el modo quiosco.
root/ConnectionType/firefox/connections/<UUID>/showUrlBarRefreshButton	Si se establece en 1, el botón Actualizar y la barra de URL del navegador web se muestran cuando está habilitado el modo quiosco.
root/ConnectionType/firefox/connections/<UUID>/startMode	Si se ajusta en el valor predeterminado `focus` (concentrar) y la conexión se ha iniciado, la conexión se concentrará. De lo contrario, aparecerá un error que indica que la conexión ya se ha iniciado.
root/ConnectionType/firefox/connections/<UUID>/waitForNetwork	Si se establece en 1, la conexión no se iniciará hasta que la red esté disponible. Esto garantiza que, en una red lenta, la conexión no se inicie antes de que la red esté disponible, lo que podría provocar una falla.
root/ConnectionType/firefox/coreSettings/USBrelevant	Especifica si este tipo de conexión es relevante para el USB. Si es así, puede tener un complemento USB para redirigir dispositivos USB.
root/ConnectionType/firefox/coreSettings/appName	Establece el nombre de la aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/firefox/coreSettings/className	Establece el nombre de la clase de aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/firefox/coreSettings/editor	Establece el nombre de la aplicación interna que se utiliza cuando se inicia el Administrador de conexión para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/firefox/coreSettings/icon	Especifica el icono del conjunto de temas de iconos que se pueden usar con esta conexión.
root/ConnectionType/firefox/coreSettings/icon16Path	Establece la ruta al icono de 16 x 16 píxeles para esta aplicación.
root/ConnectionType/firefox/coreSettings/icon32Path	Establece la ruta al icono de 32 x 32 píxeles para esta aplicación.
root/ConnectionType/firefox/coreSettings/icon48Path	Establece la ruta al icono de 48 x 48 píxeles para esta aplicación.
root/ConnectionType/firefox/coreSettings/iconActive	Reservado para uso futuro.
root/ConnectionType/firefox/coreSettings/label	Establece el nombre que se va a mostrar para este tipo de conexión en la interfaz de usuario.

Tabla E-6 Claves de registro de ConnectionType/firefox (continúa)

Clave de registro	Descripción
root/ConnectionType/firefox/coreSettings/priorityInConnectionLists	Establece la prioridad de este tipo de conexión cuando se muestra en el Administrador de conexión y en el Asistente de configuración que aparece durante la configuración inicial. Un valor superior moverá el tipo de conexión hacia la parte superior de la lista. Si se establece en 0, el tipo de conexión está oculto desde el Asistente de configuración y aparece de último en el Administrador de conexión. Los tipos de conexiones con la misma prioridad se enumeran en orden alfabético.
root/ConnectionType/firefox/coreSettings/restartIdleTime	Establece el tiempo en minutos antes de que el explorador web se reinicie cuando el sistema no está recibiendo la entrada del usuario. Si se establece en 0, se desactiva el reinicio.
root/ConnectionType/firefox/coreSettings/serverRequired	Establece si un nombre o dirección de servidor es `unused`, `optional` o `required` para este tipo de conexión.
root/ConnectionType/firefox/coreSettings/stopProcess	Establece el comportamiento que debería ocurrir cuando se llama `connection-mgr stop` en esta conexión. De forma predeterminada, está opción es `close`, lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como `kill`, el proceso especificado por `appName` se interrumpirá de forma forzada. Cuando se establece como `custom` se ejecutará una línea de comandos de ejecución personalizada especificada por `wrapperScript` con el argumento `stop` para finalizar el proceso correctamente.
root/ConnectionType/firefox/coreSettings/tier	Especifica la importancia relativa de este tipo de conexión y el orden en el que se enumera en el menú Crear.
root/ConnectionType/firefox/coreSettings/wrapperScript	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Este es el script principal que administra todos los ajustes de conexión y argumentos de línea de comandos para la conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/firefox/general/enableUserChanges	Si se establece en 1, los parámetros configurados en el cuadro de diálogo de Preferencias de Firefox se guardarán después de cada sesión.
root/ConnectionType/firefox/gui/FirefoxManager/name	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/firefox/gui/FirefoxManager/status	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/firefox/gui/FirefoxManager/title	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/address	Controla el estado del widget **URL** en el Administrador de conexión Web Browser. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/autoReconnect	Controla el estado del widget **Reconexión automática** en el Administrador de conexión Web Browser. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.

Tabla E-6 Claves de registro de ConnectionType/firefox (continúa)

Clave de registro	Descripción
root/ConnectionType/firefox/gui/FirefoxManager/widgets/autostart	Controla el estado del widget **Prioridad de inicio automático** en el Administrador de conexión Web Browser. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/enablePrintDialog	Controla el estado del widget **Activar cuadro de diálogo de impresión** en el Administrador de conexión Web Browser. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/fallBackConnection	Controla el estado del widget **Conexión de Seguridad** en el Administrador de conexión Web Browser. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/hasDesktopIcon	Controla el estado del widget **Mostrar icono en escritorio** en el Administrador de conexión Web Browser. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/kioskMode	Controla el estado del widget **Habilitar modo de quiosco** en el Administrador de conexión Web Browser. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/label	Controla el estado del widget **Nombre** en el Administrador de conexión Web Browser. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/showBackForwardButton	Controla el estado del widget **Mostrar el botón Anterior y Siguiente** en el Administrador de conexión Web Browser. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/showHomeButton	Controla el estado del widget **Mostrar el botón de Inicio** en el Administrador de conexión Web Browser. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/showSearchBar	Controla el estado del widget **Mostrar la barra de búsqueda** en el Administrador de conexión Web Browser. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.

Tabla E-6 Claves de registro de ConnectionType/firefox (continúa)

Clave de registro	Descripción
root/ConnectionType/firefox/gui/FirefoxManager/widgets/showTabsBar	Controla el estado del widget **Mostrar la barra de fichas** en el Administrador de conexión Web Browser. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/showTaskBar	Controla el estado del widget **Mostrar la barra de tareas** en el Administrador de conexión Web Browser. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/showUrlBarRefreshButton	Controla el estado del widget **Mostrar la barra de la URL y el botón Actualizar** en el Administrador de conexión Web Browser. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/startMode	Controla el estado del widget **Habilitar pantalla completa** en el Administrador de conexión Web Browser. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/waitForNetwork	Controla el estado del widget **Esperando por red antes de conectar** en el Administrador de conexión Web Browser. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.

freerdp

Claves de registro de ConnectionType/freerdp.

Tabla E-7 Claves de registro de ConnectionType/freerdp

Clave de registro	Descripción
root/ConnectionType/freerdp/authorizations/user/add	Si se establece en 1, un usuario final tiene permiso para agregar una nueva conexión de este tipo utilizando el Administrador de conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/freerdp/connections/<UUID>/ExtraArgs	Especifica los argumentos adicionales para el cliente xfreerdp. Ejecute xfreerdp --help desde una terminal X para ver todos los argumentos disponibles.
root/ConnectionType/freerdp/connections/<UUID>/SingleSignOn	Si se habilita, se guarda la combinación de usuario, dominio y contraseña para la conexión RDP con el fin de desbloquear el protector de pantalla.
root/ConnectionType/freerdp/connections/<UUID>/address	Establece el nombre de host o la dirección IP a la cual conectarse. El número de puerto podría agregarse al final, después de un carácter de dos puntos. Por ejemplo: servername:3389

Tabla E-7 Claves de registro de ConnectionType/freerdp (continúa)

Clave de registro	Descripción
root/ConnectionType/freerdp/connections/<UUID>/afterStoppedCommand	Establece el comando que se debe ejecutar después de que se ha detenido la conexión.
root/ConnectionType/freerdp/connections/<UUID>/application	Especifica un shell alternativo o una aplicación para ejecutarse.
root/ConnectionType/freerdp/connections/<UUID>/attachToConsole	
root/ConnectionType/freerdp/connections/<UUID>/audioLatency	Establece el promedio de milisegundos de desfase entre la transmisión de audio y la visualización de los fotogramas de video correspondientes después de la decodificación.
root/ConnectionType/freerdp/connections/<UUID>/authorizations/user/edit	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones para esta conexión.
root/ConnectionType/freerdp/connections/<UUID>/authorizations/user/execution	Si se establece en 1, un usuario final tiene permiso para ejecutar esta conexión.
root/ConnectionType/freerdp/connections/<UUID>/autoReconnect	Si se establece en 1, la conexión se reiniciará cuando se cierre o desconecte.
root/ConnectionType/freerdp/connections/<UUID>/autoReconnectDelay	Establece la cantidad de tiempo en segundos que se deben esperar antes de volver a conectar la sesión. El valor predeterminado 0 hará que la conexión se reactive inmediatamente. Esta configuración solo surte efecto cuando `autoReconnect` se establece en 1.
root/ConnectionType/freerdp/connections/<UUID>/autostart	Si se establece en un valor de 1 a 5, la conexión se iniciará automáticamente después de que arranque el sistema, con el valor de 1 con la prioridad más alta.
root/ConnectionType/freerdp/connections/<UUID>/bandwidthLimitation	Si se establece en un valor mayor que 0, el valor representa una limitación aproximada de ancho de banda para descargar y cargar en kilobytes por segundo. Si se establece en 0 (el valor predeterminado), no hay limitación.
root/ConnectionType/freerdp/connections/<UUID>/beforeStartingCommand	Establece que se ejecute el comando antes de que empiece la conexión.
root/ConnectionType/freerdp/connections/<UUID>/clipboardExtension	Cuando se establece en 1, la funcionalidad del portapapeles se activa entre diferentes sesiones de RDP y entre sesiones de RDP y el sistema local.
root/ConnectionType/freerdp/connections/<UUID>/compression	Si se establece en 1, se activa la compresión de datos RDP entre el cliente y el servidor.
root/ConnectionType/freerdp/connections/<UUID>/credentialsType	Especifica el tipo de credencial entre `sso` (inicio de sesión único), `startup` (las credenciales se solicitan en el inicio), `password` (contraseña/dominio/usuario preconfigurados), o `smartcard` (smart card preconfigurada).
root/ConnectionType/freerdp/connections/<UUID>/dependConnectionId	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/freerdp/connections/<UUID>/directory	Especifica el directorio de inicio, donde se ejecuta una aplicación shell alternativa.

Tabla E-7 Claves de registro de ConnectionType/freerdp (continúa)

Clave de registro	Descripción
root/ConnectionType/freerdp/connections/<UUID>/disableMMRwithRFX	Si se establece en 1, se desactiva la redirección de contenido multimedia en caso de que se establezca una sesión RemoteFX válida.
root/ConnectionType/freerdp/connections/<UUID>/domain	Establece el dominio predeterminado que se suministra al host remoto durante el inicio de sesión. Si no hay ningún dominio especificado, se utilizará el dominio predeterminado para el host remoto.
root/ConnectionType/freerdp/connections/<UUID>/enableMMR	Si se establece en 1, se habilita el complemento Redirección de multimedia. Esto hace que los códecs compatibles que se reproducen a través de Windows Media Player se redirijan al cliente.
root/ConnectionType/freerdp/connections/<UUID>/extraEnvValues/<UUID>/key	Establece el nombre de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/freerdp/connections/<UUID>/extraEnvValues/<UUID>/value	Establece el valor de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/freerdp/connections/<UUID>/fallBackConnection	Establece la conexión alternativa a través de su UUID.
root/ConnectionType/freerdp/connections/<UUID>/frameAcknowledgeCount	Establece el número de fotogramas de video que el servidor puede forzar sin tener que esperar el reconocimiento desde el cliente. Los números más bajos tienen como consecuencia una mayor capacidad de respuesta del escritorio pero menos fotogramas por segundo. Si se establece en 0, no se utiliza el reconocimiento de fotogramas en las interacciones del cliente y el servidor.
root/ConnectionType/freerdp/connections/<UUID>/gatewayAddress	Establece el nombre del servidor o la dirección RD Gateway.
root/ConnectionType/freerdp/connections/<UUID>/gatewayCredentialsType	Especifica el tipo de credencial entre la opción de que las credenciales las suministre `sso` (inicio de sesión único), `startup` (las credenciales se solicitan en el inicio) o `password` (contraseña/dominio/usuario preconfigurados).
root/ConnectionType/freerdp/connections/<UUID>/gatewayDomain	Establece el dominio predeterminado para suministrar al RD Gateway durante el inicio de sesión. Por lo general, este ajuste se utiliza con las aplicaciones de estilo quiosco donde se usa un nombre de usuario genérico para el inicio de sesión. Si se establece `gatewayUsesSameCredentials` en 1, este valor se desactiva.
root/ConnectionType/freerdp/connections/<UUID>/gatewayEnabled	Si se establece en 1, es de esperar que se use RD Gateway.
root/ConnectionType/freerdp/connections/<UUID>/gatewayPassword	Establece la contraseña predeterminada para suministrar al RD Gateway durante el inicio de sesión. Por lo general, este valor está encriptado. Por lo general, este ajuste se utiliza con las aplicaciones de estilo quiosco donde se usa un nombre de usuario genérico para el inicio de sesión. Si se establece `gatewayUsesSameCredentials` en 1, este valor se desactiva.
root/ConnectionType/freerdp/connections/<UUID>/gatewayPort	Establece el número de puerto que se utiliza cuando se comunica con el servidor RDP. Este valor se puede dejar vacío. El valor más común es 443.

Tabla E-7 Claves de registro de ConnectionType/freerdp (continúa)

Clave de registro	Descripción
root/ConnectionType/freerdp/connections/<UUID>/gatewayUser	Establece el nombre de usuario predeterminado para suministrar al RD Gateway durante el inicio de sesión. Por lo general, este ajuste se utiliza con las aplicaciones de estilo quiosco donde se usa un nombre de usuario genérico para el inicio de sesión. Si se establece gatewayUsesSameCredentials en 1, este valor se desactiva.
root/ConnectionType/freerdp/connections/<UUID>/gatewayUsesSameCredentials	Si se establece en 1, se utilizan las mismas credenciales para conectarse al servidor final que las que se utilizan para conectarse al RD Gateway.
root/ConnectionType/freerdp/connections/<UUID>/hasDesktopIcon	Si se establece en 1, se activa el icono del escritorio para esta conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/freerdp/connections/<UUID>/hostnameType	Si se establece en hostname, el nombre de host del sistema se envía al host remoto. Esto suele utilizarse para identificar el thin client asociado a una sesión particular de RDP. El nombre de host enviado se puede anular mediante sendHostname en la configuración específica para la conexión. Si se establece en mac, en vez del nombre de host, se envía la dirección MAC del primer adaptador de red disponible.
root/ConnectionType/freerdp/connections/<UUID>/iconPosition	Establece las coordinadas x,y de un icono de escritorio fijo. Si no se especifica, el icono queda flotante.
root/ConnectionType/freerdp/connections/<UUID>/label	Establece el nombre de conexión que se muestra en la interfaz de usuario. En Smart Zero, por lo general esta opción se establece en Default Connection y no aparece en la interfaz de usuario.
root/ConnectionType/freerdp/connections/<UUID>/loadBalanceInfo	Este valor es la cookie de equilibrio de carga enviado al servidor para fines de intermediación tras la conexión y corresponde al campo loadbalanceinfo en el archivo .rdp. De forma predeterminada, el valor está vacío.
root/ConnectionType/freerdp/connections/<UUID>/localPartitionRedirection	Si se establece en 1, las particiones de almacenamiento local no USB se redirigen al host remoto mediante la extensión Storage. Si se establece en 0, la extensión se desactiva para las particiones de almacenamiento no USB y que HP ThinPro no utiliza.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/domain	Si se establece en 1, el campo **Dominio** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el campo se muestra pero desactivado. Si se establece en 0, el campo queda oculto.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/password	Si se establece en 1, el campo **Contraseña** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el campo se muestra pero desactivado. Si se establece en 0, el campo queda oculto.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/rememberme	Si se establece en 1, la casilla de verificación **Recordarme** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, la casilla de verificación aparece pero deshabilitada. Si se establece en 0, la casilla de verificación está oculta.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/server	Si se establece en 1, el cuadro **Servidor** aparece en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el cuadro aparece pero deshabilitado. Si se establece en 0, el cuadro queda oculto. Si se establece en 3, se usan los ajustes del sistema.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/showpassword	Si se establece en 1, la casilla de verificación **Mostrar contraseña** aparece en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, la casilla de verificación aparece pero

Tabla E-7 Claves de registro de ConnectionType/freerdp (continúa)

Clave de registro	Descripción
	deshabilitada. Si se establece en 0, la casilla de verificación está oculta.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/smartcard	Si se establece en 1, la casilla de verificación **Inicio de sesión con smart card** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, la casilla de verificación aparece pero deshabilitada. Si se establece en 0, la casilla de verificación está oculta. Es posible que esta casilla de verificación no aparezca si no se detecta ninguna smart card, incluso si esta opción está habilitada.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/username	Si se establece en 1, el campo **Nombre de usuario** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el campo se muestra pero desactivado. Si se establece en 0, el campo queda oculto.
root/ConnectionType/freerdp/connections/<UUID>/mouseMotionEvents	Si se establece en 0, los eventos de movimiento del mouse no se envían al servidor. Esto puede evitar que algunos comentarios del usuario, como consejos sobre herramientas, funcionen correctamente.
root/ConnectionType/freerdp/connections/<UUID>/offScreenBitmaps	Si se establece en 0, se desactivan los mapas de bits fuera de pantalla. Esto puede aumentar el rendimiento ligeramente, pero hará que bloques de la pantalla se actualicen de forma asíncrona y, de esta forma, las transiciones de pantalla se actualizarán sin uniformidad
root/ConnectionType/freerdp/connections/<UUID>/password	Establece la contraseña predeterminada que se suministra al host remoto durante el inicio de sesión. Este valor se encriptará. Por lo general, este ajuste se utiliza con las aplicaciones de estilo quiosco donde se usa una contraseña genérica para el inicio de sesión.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagDesktopComposition	Si se establece en 1, permite la composición del escritorio (por ejemplo los bordes translúcidos) en caso de que sea compatible con el servidor. Al desactivar la composición del escritorio se puede mejorar el rendimiento de las conexiones con bajo ancho de banda. Por lo general, esto solo afecta a RemoteFX. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagFontSmoothing	Si se establece en 1, permite el suavizado de fuentes en caso de que sea compatible con el servidor y esté activado. Al desactivar el suavizado de fuentes puede mejorar el rendimiento de conexiones con bajo ancho de banda. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoCursorSettings	Si se establece en 1, se desactiva el parpadeo del cursor. Esto puede mejorar el rendimiento en conexiones RDP con bajo ancho de banda. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoCursorShadow	Si se establece en 1, se desactivan los controles remotos del cursor del mouse. Esto puede mejorar el rendimiento en conexiones RDP con bajo ancho de banda. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoMenuAnimations	Si se establece en 1, se desactivan las animaciones del menú. Esto puede mejorar el rendimiento en conexiones RDP con bajo ancho de banda. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoTheming	Si se establece en 1, se desactivan los temas de la interfaz del usuario. Esto puede mejorar el rendimiento en conexiones

Tabla E-7 Claves de registro de ConnectionType/freerdp (continúa)

Clave de registro	Descripción
	RDP con bajo ancho de banda. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoWallpaper	Si se establece en 1, se desactiva el fondo de pantalla del escritorio. Esto puede mejorar el rendimiento en conexiones RDP con bajo ancho de banda. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoWindowDrag	Si se establece en 1, se desactiva la función de arrastrar el contenido completo de la ventana. Esto puede mejorar el rendimiento en conexiones RDP con bajo ancho de banda. En su lugar se utiliza el contorno de la ventana. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.
root/ConnectionType/freerdp/connections/<UUID>/portMapping	Si se establece en 1, todos los puertos en serie y paralelos se redirigen al host remoto a través de la extensión `Puertos`. Si se establece en 0, se desactiva la extensión.
root/ConnectionType/freerdp/connections/<UUID>/printerMapping	Si se establece en 1, todas las impresoras definidas localmente a través de CUPS se redirigen al host remoto a través de la extensión de `Impresoras`. Si se establece en 0, se desactiva la extensión. Si se establece en 2, las impresoras USB se redirigen según la configuración del Administrador de USB.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/autoDisconnectTimeout	Establece la cantidad de minutos durante los que los recursos RemoteApp y Desktop no pueden ejecutarse antes de que la conexión termine automáticamente. Aparece una cuenta regresiva durante los últimos 20 segundos para brindar al usuario la oportunidad de detener el temporizador. Si se establece en 0 (el valor predeterminado), se desactiva el temporizador.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/autoStartSingleResource	Si se establece en 1 y el servidor devuelve solo un recurso publicado (el programa RemoteApp o el escritorio virtual), ese recurso se iniciará automáticamente.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/filter/<UUID>/alias	Especifica el alias de un recurso para el filtro de recursos. Los recursos del escritorio y RemoteApp con un alias coincidente estarán disponibles para los usuarios.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/filter/<UUID>/name	Especifica el nombre de un recurso para el filtro de recursos. Los recursos del escritorio y RemoteApp con un nombre coincidente estarán disponibles para los usuarios.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/keepResourcesWindowOpened	Si se establece en 0, la ventana de selección de recursos se cierra automáticamente después de que un recurso ha empezado. Si se establece en 1, la ventana de selección de recursos se mantiene abierta después de que se han iniciado los recursos. Esto permite que un usuario inicie varios recursos antes de cerrar la ventana de selección de recursos.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/trustedPublisherSha1Thumbprints	Especifica una lista separada por comas de las huellas de SHA1 referentes a los editores de recursos confiables. Tome en cuenta que no se verifican los certificados que coincidan con una de estas huellas. Para obtener más seguridad, importe la AC de la raíz del editor. Además, vea la clase de registro `verifyPublisherSignature` y el Administrador de certificados en el Panel de control.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/verifyPublisherSignature	Si se establece en 1, la firma del editor se verifica cuando está disponible en los archivos .rdp publicados. Solo se pueden ejecutar recursos con una firma válida de un editor confiable. Si se establece en 0, no se realiza la verificación de la firma. Además, vea la clave de registro `trustedPublisherSha1Thumbprints`.

Tabla E-7 Claves de registro de ConnectionType/freerdp (continúa)

Clave de registro	Descripción
root/ConnectionType/freerdp/connections/<UUID>/rdp6Buffering	Si se establece en 1, aumenta el rendimiento de gráficos que no son RemoteFX aunque las actualizaciones serán menos frecuentes.
root/ConnectionType/freerdp/connections/<UUID>/rdp8Codecs	Si se establece en 1, se utilizan códecs RDP 8 si están disponibles. Este ajuste debe desactivarse sólo en el caso de un defecto específico de los códecs RDP 8. Al desactivar este ajuste también podrían desactivarse códecs más avanzados.
root/ConnectionType/freerdp/connections/<UUID>/rdpEncryption	Si se establece en 1, la encriptación RDP estándar se utiliza para encriptar todos los datos entre el cliente y el servidor.
root/ConnectionType/freerdp/connections/<UUID>/rdpH264Codec	Si se establece en 1, se utilizan códecs RDP 8 H.264 si están disponibles. Este ajuste se ha reconocido por producir errores visuales, especialmente en configuraciones con varios monitores, y debe ser considerado experimental y no admitido. Al activar este ajuste simplemente se le informa al servidor que el thin client admite H.264 para la visualización del escritorio. El servidor también debe admitir H.264 y el servidor toma la decisión final sobre cuál códec utilizar. Este ajuste afecta a solo los códecs de escritorio. No afecta los códecs de redirección de multimedia.
root/ConnectionType/freerdp/connections/<UUID>/rdpProgressiveCodec	Si se establece en 1, se utilizan códecs progresivos RDP 8 si están disponibles. Este ajuste debe desactivarse sólo en el caso de un defecto específico en los códecs progresivos RDP 8. Al desactivar este ajuste también podrían desactivarse códecs más avanzados.
root/ConnectionType/freerdp/connections/<UUID>/redirectPreference	Para la redirección, al cliente RDP se le brindan varias posibilidades de destino. Normalmente las trata en el siguiente orden: FQDN, IP principal, Lista de IP, NetBIOS. Si no se desea FQDN, se puede probar primero una de las alternativas al configurar esta clave de registro. Si el método especificado no funciona, el cliente RDP vuelve al orden original. Una configuración `auto` fuerza el orden original.
root/ConnectionType/freerdp/connections/<UUID>/remoteApp	Especifica el nombre de una aplicación disponible para ejecutarse en el modo Aplicación remota integrada localmente (RAIL).
root/ConnectionType/freerdp/connections/<UUID>/remoteDesktopService	Si se establece en `Equipo remoto`, se realiza una conexión RDP directa a un equipo remoto. Si se establece en `RD Web Access`, primero se realiza una conexión a un servicio de RD Web Access para recuperar una alimentación de los recursos publicados de RemoteApp.
root/ConnectionType/freerdp/connections/<UUID>/remoteFx	Si se establece en 1, se utiliza RemoteFX en el estilo de RDP 7.1 si está disponible. Este ajuste está desfasado y podría desaparecer en una versión futura de HP ThinPro. Este ajuste debe desactivarse sólo en el caso de un defecto específico del protocolo RemoteFX. Al desactivar este ajuste también podrían desactivarse códecs más avanzados.
root/ConnectionType/freerdp/connections/<UUID>/requireEncryptionOracleRemediation	Si se establece en 1, el Cliente del escritorio remoto se niega a conectarse a servidores que no ofrecen protecciones adecuadas. Esto responde a la vulnerabilidad de la seguridad CVE-2018-0886 de Microsoft.
root/ConnectionType/freerdp/connections/<UUID>/scCertificate	Si se selecciona un inicio de sesión con smart card preconfigurado, se brinda un identificador que corresponde al certificado en esa smart card que se usará para la autenticación.
root/ConnectionType/freerdp/connections/<UUID>/scPin	Si se selecciona un inicio de sesión con smart card preconfigurado, se brinda el PIN o la contraseña de esa smart card.

Tabla E-7 Claves de registro de ConnectionType/freerdp (continúa)

Clave de registro	Descripción
root/ConnectionType/freerdp/connections/<UUID>/scRedirection	Si se establece en 1, todos los lectores de smart card locales se redireccionan al host remoto pero no se usan para la Autenticación en el nivel de la red (NLA) de la sesión de RDP. **NOTA:** Si credentialsType se establece en smartcard o smartcard se establece en 1, se ignora scRedirection, según la versión de HP ThinPro. En esta configuración, los lectores de smart card se redireccionan siempre.
root/ConnectionType/freerdp/connections/<UUID>/seamlessWindow	Si se establece en 1, se deshabilitan las decoraciones de la ventana. Esta opción puede ser deseable en una configuración de varios monitores para permitir que la conexión se ajuste al tamaño del monitor principal.
root/ConnectionType/freerdp/connections/<UUID>/securityLevel	Establece el nivel de seguridad del certificado. Si se establece en 0, se permiten todas las conexiones. Si se establece en 1, se seleccionan los hosts recordados y aparece un cuadro de diálogo de advertencia en caso de que no apruebe la verificación. Si se establece en 2, no se seleccionan los hosts recordados y aparece un cuadro de diálogo de advertencia en caso de que no apruebe la verificación. Si se establece en 3, se rechazan todas las conexiones inseguras.
root/ConnectionType/freerdp/connections/<UUID>/sendHostname	Establece el nombre de host del thin client que se envía al host remoto. Si se deja en blanco, se envía el nombre de host del sistema. La clave de registro root/ConnectionType/freerdp/general/sendHostname se debe establecer en hostname para que se use esta clave.
root/ConnectionType/freerdp/connections/<UUID>/showConnectionGraph	Esta es una función de diagnóstico. Si se establece en 1, cuando se inicia la sesión, se iniciará un programa separado para visualizar en un gráfico el estado de la conexión.
root/ConnectionType/freerdp/connections/<UUID>/showRDPDashboard	Si se establece en 1, cuando se inicia la sesión, una ventana separada muestra el rendimiento y el estado de RDP.
root/ConnectionType/freerdp/connections/<UUID>/smartcard	Si se establece en 1, se permite la autenticación de la Smart Card local en el host remoto. Actualmente, esto desactivará NLA o Autenticación de nivel de red.
root/ConnectionType/freerdp/connections/<UUID>/sound	Si se establece en 1, los dispositivos de reproducción y grabación se redirigen al host remoto mediante la extensión Audio. Si se establece en 0, se desactiva la extensión. Si se establece en 2, los dispositivos de audio USB se redirigen según la configuración del Administrador de USB. Por lo general, HP recomienda que establezca este valor en 1 para que se use la redirección de audio de alto nivel. Esto mejorará la calidad del audio y asegurará que el audio del cliente redirigido mediante otras extensiones (como Multimedia Redirection) coincida con la configuración de audio local.
root/ConnectionType/freerdp/connections/<UUID>/startMode	Si se ajusta en el valor predeterminado focus (concentrar) y la conexión se ha iniciado, la conexión se concentrará. De lo contrario, aparecerá un error que indica que la conexión ya se ha iniciado.
root/ConnectionType/freerdp/connections/<UUID>/timeoutError	Establece el número de milisegundos de espera después de perder la conexión antes de abandonar la reconexión con el servidor. Si se establece en 0, se reintenta la reconexión constantemente.
root/ConnectionType/freerdp/connections/<UUID>/timeoutRecovery	Establece el número de milisegundos de espera después de perder la conexión para que la red se recupere sin tratar de forzar una reconexión.

Tabla E-7 Claves de registro de ConnectionType/freerdp (continúa)

Clave de registro	Descripción
root/ConnectionType/freerdp/connections/<UUID>/timeoutWarning	Establece el número de milisegundos de espera después de perder la conexión antes de advertirle al usuario que la conexión se ha perdido.
root/ConnectionType/freerdp/connections/<UUID>/timeoutWarningDialog	Si se establece en 1, cuando se detecta que se perdió la conexión de extremo a extremo, aparece un cuadro de diálogo y la pantalla se pone gris. De lo contrario, se graban mensajes en el registro de la conexión y la sesión se congela.
root/ConnectionType/freerdp/connections/<UUID>/timeoutsEnabled	Si se establece en 1, se realizan las verificaciones de estado de la conexión de extremo a extremo.
root/ConnectionType/freerdp/connections/<UUID>/tlsVersion	Establece la versión de Transport Layer Security que se va a usar durante las fases iniciales de negociación con el servidor RDP. Establézcala de forma que coincida con la versión de TLS utilizada por su servidor RDP, o trate de establecerla en `auto`. **NOTA:** Hay algunos defectos del lado del servidor en ciertos servidores RDP sin parches que pueden hacer que el ajuste automático falle, de forma que no sea el ajuste predeterminado.
root/ConnectionType/freerdp/connections/<UUID>/usbMiscRedirection	Si se establece en 0, se desactiva la redirección para todos los otros dispositivos USB excepto los administrados por `sound`, `printerMapping`, `portMapping`, `usbStorageRedirection` y `localPartitionRedirection`. Si se establece en 2, todos los otros dispositivos USB se redirigen al host remoto según la configuración del Administrador de USB.
root/ConnectionType/freerdp/connections/<UUID>/usbStorageRedirection	Si se establece en 1, los dispositivos de almacenamiento USB se redirigen al host remoto a través de la extensión `Storage`. Si se establece en 0, se desactiva la extensión. Si se establece en 2, los dispositivos de almacenamiento USB se redirigen según la configuración del Administrador de USB.
root/ConnectionType/freerdp/connections/<UUID>/username	Establece el nombre de usuario predeterminado que se suministra al host remoto durante el inicio de sesión. Por lo general, esta configuración se utiliza con las aplicaciones al estilo quiosco donde se usa un nombre de usuario genérico para el inicio de sesión.
root/ConnectionType/freerdp/connections/<UUID>/waitForNetwork	Si se establece en 1, la conexión no se iniciará hasta que la red esté disponible. Esto garantiza que, en una red lenta, la conexión no se inicie antes de que la red esté disponible, lo que podría provocar una falla.
root/ConnectionType/freerdp/connections/<UUID>/windowMode	Si se establece en `Remote Application`, RDP se ejecutará en el modo Aplicación remota integrada localmente RAIL). Esto requiere que el servidor de RemoteApp permita que la aplicación deseada se ejecute como aplicación remota. La aplicación se mostrará en una ventana separada dentro del entorno del escritorio. De esta forma, parece que la aplicación forma parte del sistema local. Consulte también la clave de registro `remoteApp`. Si se establece en `Alternate Shell`, se invoca un shell no estándar. Consulte también las claves de registro `application` y `directory`.
root/ConnectionType/freerdp/connections/<UUID>/windowSizeHeight	
root/ConnectionType/freerdp/connections/<UUID>/windowSizePercentage	

Tabla E-7 Claves de registro de ConnectionType/freerdp (continúa)

Clave de registro	Descripción
root/ConnectionType/freerdp/connections/<UUID>/windowSizeWidth	
root/ConnectionType/freerdp/connections/<UUID>/windowType	
root/ConnectionType/freerdp/connections/<UUID>/x11Capture	Esta es una función de diagnóstico. Si se establece en 1, las operaciones de X11 se capturan para una reproducción posterior.
root/ConnectionType/freerdp/connections/<UUID>/x11CaptureDir	Esta es una función de diagnóstico. El valor establece el directorio para los archivos de la captura de X11.
root/ConnectionType/freerdp/connections/<UUID>/x11LogAutoflush	Esta es una función de diagnóstico. Si se establece en 1, el logfile X11 se descarga con más frecuencia en un disco.
root/ConnectionType/freerdp/connections/<UUID>/x11Logfile	Esta es una función de diagnóstico. El valor establece la ruta del logfile X11.
root/ConnectionType/freerdp/connections/<UUID>/x11Logging	Esta es una función de diagnóstico. Si se establece en 1, se registran las operaciones de X11.
root/ConnectionType/freerdp/connections/<UUID>/x11Synchronous	Esta es una función de diagnóstico. Si se establece en 1, no se almacenan en la memoria temporal las operaciones de X11.
root/ConnectionType/freerdp/connections/<UUID>/xkbLayoutId	Establece un ID de disposición de XKB para omitir el teclado del sistema. Para ver la lista de ID disponibles, introduzca el siguiente comando en un terminal X: `xfreerdp --kbd-list`.
root/ConnectionType/freerdp/coreSettings/USBrelevant	Especifica si este tipo de conexión es relevante para el USB. Si es así, puede tener un complemento USB para redirigir dispositivos USB.
root/ConnectionType/freerdp/coreSettings/appName	Establece el nombre de la aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/freerdp/coreSettings/className	Establece el nombre de la clase de aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/freerdp/coreSettings/disableLinkDropWarning	Si se establece en 1, el sistema operativo no genera un cuadro de diálogo que indique que la red se interrumpió porque el protocolo de conexión se encarga de estas situaciones.
root/ConnectionType/freerdp/coreSettings/editor	Establece el nombre de la aplicación interna que se utiliza cuando se inicia el Administrador de conexión para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/freerdp/coreSettings/icon	Especifica el icono del conjunto de temas de iconos que se pueden usar con esta conexión.
root/ConnectionType/freerdp/coreSettings/icon16Path	Establece la ruta al icono de 16 x 16 píxeles para esta aplicación.
root/ConnectionType/freerdp/coreSettings/icon32Path	Establece la ruta al icono de 32 x 32 píxeles para esta aplicación.
root/ConnectionType/freerdp/coreSettings/icon48Path	Establece la ruta al icono de 48 x 48 píxeles para esta aplicación.

Tabla E-7 Claves de registro de ConnectionType/freerdp (continúa)

Clave de registro	Descripción
root/ConnectionType/freerdp/coreSettings/iconActive	Reservado para uso futuro.
root/ConnectionType/freerdp/coreSettings/initialConnectionTimeout	Establece el número de segundos de espera de una respuesta inicial del servidor RDP antes de desistir.
root/ConnectionType/freerdp/coreSettings/label	Establece el nombre que se va a mostrar para este tipo de conexión en la interfaz de usuario.
root/ConnectionType/freerdp/coreSettings/priorityInConnectionLists	Establece la prioridad de este tipo de conexión cuando se muestra en el Administrador de conexión y en el Asistente de configuración que aparece durante la configuración inicial. Un valor superior moverá el tipo de conexión hacia la parte superior de la lista. Si se establece en 0, el tipo de conexión está oculto desde el Asistente de configuración y aparece de último en el Administrador de conexión. Los tipos de conexiones con la misma prioridad se enumeran en orden alfabético.
root/ConnectionType/freerdp/coreSettings/stopProcess	Establece el comportamiento que debería ocurrir cuando se llama `connection-mgr stop` en esta conexión. De forma predeterminada, está opción es `close`, lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como `kill`, el proceso especificado por `appName` se interrumpirá de forma forzada. Cuando se establece como `custom` se ejecutará una línea de comandos de ejecución personalizada especificada por `wrapperScript` con el argumento `stop` para finalizar el proceso correctamente.
root/ConnectionType/freerdp/coreSettings/tier	Especifica la importancia relativa de este tipo de conexión y el orden en el que se enumera en el menú Crear.
root/ConnectionType/freerdp/coreSettings/watchPid	Si se establece en 1, la conexión se supervisa bajo el nombre especificado por `appName`. No debería ser necesario modificar esta clave.
root/ConnectionType/freerdp/coreSettings/wrapperScript	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Este es el script principal que administra todos los ajustes de conexión y argumentos de línea de comandos para la conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/freerdp/coreSettings/wrapperScriptGeneration	Permite que el Administrador de conexiones sepa qué tipo de parámetros aprueban el script.
root/ConnectionType/freerdp/general/autoReconnectDialogTimeout	Si `autoReconnect` está activado, esta clave establece el número de segundos antes de que se agote el tiempo de cualquier cuadro de diálogo de error referente a la conexión. Si se establece en 0, los cuadros de diálogo esperan indefinidamente la interacción del usuario.
root/ConnectionType/freerdp/general/disablePasswordChange	Cuando falla un inicio de sesión remoto debido a credenciales incorrectas, el usuario verá un botón que abre un cuadro de diálogo para actualizar su contraseña. Si esta clave se establece en 1, no se muestran ese botón ni el cuadro de diálogo.
root/ConnectionType/freerdp/general/preferredAudio	Establece el backend del audio predeterminado para la redirección de audio de alto nivel (tanto de entrada como de salida).
root/ConnectionType/freerdp/general/rdWebFeedUrlPattern	Establece el patrón utilizado para crear la URL de RD Web Access. El host de la URL, por ej. Myserver.com, se sustituye por el valor

Tabla E-7 Claves de registro de ConnectionType/freerdp (continúa)

Clave de registro	Descripción
	del campo **Dirección** de la conexión. Este patrón no se utiliza cuando la dirección ya es una URL.
`root/ConnectionType/freerdp/general/serialPortsDriver`	Esta configuración garantiza una mejor compatibilidad con el controlador subyacente esperado de Windows: SerCx2.sys, SerCx.sys o Serial.sys.
`root/ConnectionType/freerdp/general/serialPortsPermissive`	Si se establece en 1, se ignorarán los errores de recursos no compatibles.

ssh

Claves de registro de SSH.

Tabla E-8 Claves de registro de SSH

Clave de registro	Descripción
`root/ConnectionType/ssh/authorizations/user/add`	Si se establece en 1, un usuario final tiene permiso para agregar una nueva conexión de este tipo utilizando el Administrador de conexión. Esta tecla no tiene efecto en Smart Zero.
`root/ConnectionType/ssh/authorizations/user/general`	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones generales para este tipo de conexión utilizando el Administrador de conexión. Esta tecla no tiene efecto en Smart Zero.
`root/ConnectionType/ssh/connections/<UUID>/address`	Establece el nombre de host o la dirección IP a la cual conectarse.
`root/ConnectionType/ssh/connections/<UUID>/afterStartedCommand`	Establece el comando que se debe ejecutar después de que se ha iniciado la conexión.
`root/ConnectionType/ssh/connections/<UUID>/afterStoppedCommand`	Establece el comando que se debe ejecutar después de que se ha detenido la conexión.
`root/ConnectionType/ssh/connections/<UUID>/application`	Especifica la aplicación a ejecutar.
`root/ConnectionType/ssh/connections/<UUID>/authorizations/user/edit`	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones para esta conexión.
`root/ConnectionType/ssh/connections/<UUID>/authorizations/user/execution`	Si se establece en 1, un usuario final tiene permiso para ejecutar esta conexión.
`root/ConnectionType/ssh/connections/<UUID>/autoReconnect`	Si se establece en 1, la conexión se reiniciará cuando se cierre o desconecte.
`root/ConnectionType/ssh/connections/<UUID>/autoReconnectDelay`	Establece la cantidad de tiempo en segundos que se deben esperar antes de volver a conectar la sesión. El valor predeterminado 0 hará que la conexión se reactive inmediatamente. Esta configuración solo surte efecto cuando `autoReconnect` se establece en 1.
`root/ConnectionType/ssh/connections/<UUID>/autostart`	Si se establece en un valor de 1 a 5, la conexión se iniciará automáticamente después de que arranque el sistema, con el valor de 1 con la prioridad más alta.

Tabla E-8 Claves de registro de SSH (continúa)

Clave de registro	Descripción
root/ConnectionType/ssh/connections/<UUID>/backgroundColor	Establece el color de fondo de la conexión.
root/ConnectionType/ssh/connections/<UUID>/beforeStartingCommand	Establece que se ejecute el comando antes de que empiece la conexión.
root/ConnectionType/ssh/connections/<UUID>/compression	Activa la compresión para una conexión SSH.
root/ConnectionType/ssh/connections/<UUID>/connectionEndAction	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/ssh/connections/<UUID>/coord	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/ssh/connections/<UUID>/dependConnectionId	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/ssh/connections/<UUID>/extraEnvValues/<UUID>/key	Establece el nombre de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/ssh/connections/<UUID>/extraEnvValues/<UUID>/value	Establece el valor de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/ssh/connections/<UUID>/fallBackConnection	Establece la conexión alternativa a través de su UUID.
root/ConnectionType/ssh/connections/<UUID>/font	Establece el tamaño de la letra de la conexión.
root/ConnectionType/ssh/connections/<UUID>/foregroundColor	Establece el color de primer plano de la conexión.
root/ConnectionType/ssh/connections/<UUID>/fork	Si se establece en 1, se activa la opción **Bifurcación en segundo plano** de la conexión.
root/ConnectionType/ssh/connections/<UUID>/hasDesktopIcon	Si se establece en 1, se activa el icono del escritorio para esta conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/ssh/connections/<UUID>/iconPosition	Establece las coordinadas x,y de un icono de escritorio fijo. Si no se especifica, el icono queda flotante.
root/ConnectionType/ssh/connections/<UUID>/isInMenu	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/ssh/connections/<UUID>/label	Establece el nombre de conexión que se muestra en la interfaz de usuario. En Smart Zero, por lo general esta opción se establece en `Default Connection` y no aparece en la interfaz de usuario.
root/ConnectionType/ssh/connections/<UUID>/loginfields/server	Si se establece en 1, el cuadro **Servidor** aparece en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el cuadro aparece pero deshabilitado. Si se establece en 0, el cuadro queda oculto. Si se establece en 3, se usan los ajustes del sistema.
root/ConnectionType/ssh/connections/<UUID>/loginfields/username	Si se establece en 1, el cuadro **Nombre de usuario** aparece en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el cuadro aparece pero deshabilitado. Si se

Tabla E-8 Claves de registro de SSH (continúa)

Clave de registro	Descripción
	establece en 0, el cuadro queda oculto. Si se establece en 3, se usan los ajustes del sistema.
root/ConnectionType/ssh/connections/<UUID>/port	Establece el número de puerto que se utiliza cuando se comunica con el servidor SSH. De forma predeterminada es 22.
root/ConnectionType/ssh/connections/<UUID>/startMode	Si se ajusta en el valor predeterminado `focus` (concentrar) y la conexión se ha iniciado, la conexión se concentrará. De lo contrario, aparecerá un error que indica que la conexión ya se ha iniciado.
root/ConnectionType/ssh/connections/<UUID>/tty	Si se establece en 1, la opción **Forzar asignación TTY** para la conexión.
root/ConnectionType/ssh/connections/<UUID>/username	Establece el nombre de usuario predeterminado que se suministra al host remoto durante el inicio de sesión. Por lo general, esta configuración se utiliza con las aplicaciones al estilo quiosco donde se usa un nombre de usuario genérico para el inicio de sesión.
root/ConnectionType/ssh/connections/<UUID>/waitForNetwork	Si se establece en 1, la conexión no se iniciará hasta que la red esté disponible. Esto garantiza que, en una red lenta, la conexión no se inicie antes de que la red esté disponible, lo que podría provocar una falla.
root/ConnectionType/ssh/connections/<UUID>/x11	Si se establece en 1, se activa la opción **Reenvío de conexión X11** para la conexión.
root/ConnectionType/ssh/coreSettings/USBrelevant	Especifica si este tipo de conexión es relevante para el USB. Si es así, puede tener un complemento USB para redirigir dispositivos USB.
root/ConnectionType/ssh/coreSettings/appName	Establece el nombre de la aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/ssh/coreSettings/className	Establece el nombre de la clase de aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/ssh/coreSettings/editor	Establece el nombre de la aplicación interna que se utiliza cuando se inicia el Administrador de conexión para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/ssh/coreSettings/icon	Especifica el icono del conjunto de temas de iconos que se pueden usar con esta conexión.
root/ConnectionType/ssh/coreSettings/icon16Path	Establece la ruta al icono de 16 x 16 píxeles para esta aplicación.
root/ConnectionType/ssh/coreSettings/icon32Path	Establece la ruta al icono de 32 x 32 píxeles para esta aplicación.
root/ConnectionType/ssh/coreSettings/icon48Path	Establece la ruta al icono de 48 x 48 píxeles para esta aplicación.
root/ConnectionType/ssh/coreSettings/iconActive	Reservado para uso futuro.
root/ConnectionType/ssh/coreSettings/label	Establece el nombre que se va a mostrar para este tipo de conexión en la interfaz de usuario.

Tabla E-8 Claves de registro de SSH (continúa)

Clave de registro	Descripción
root/ConnectionType/ssh/coreSettings/priorityInConnectionLists	Establece la prioridad de este tipo de conexión cuando se muestra en el Administrador de conexión y en el Asistente de configuración que aparece durante la configuración inicial. Un valor superior moverá el tipo de conexión hacia la parte superior de la lista. Si se establece en 0, el tipo de conexión está oculto desde el Asistente de configuración y aparece de último en el Administrador de conexión. Los tipos de conexiones con la misma prioridad se enumeran en orden alfabético.
root/ConnectionType/ssh/coreSettings/serverRequired	Establece si un nombre o dirección de servidor es `unused`, `optional` o `required` para este tipo de conexión.
root/ConnectionType/ssh/coreSettings/stopProcess	Establece el comportamiento que debería ocurrir cuando se llama `connection-mgr stop` en esta conexión. De forma predeterminada, está opción es `close`, lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como `kill`, el proceso especificado por `appName` se interrumpirá de forma forzada. Cuando se establece como `custom` se ejecutará una línea de comandos de ejecución personalizada especificada por `wrapperScript` con el argumento `stop` para finalizar el proceso correctamente.
root/ConnectionType/ssh/coreSettings/tier	Especifica la importancia relativa de este tipo de conexión y el orden en el que se enumera en el menú Crear.
root/ConnectionType/ssh/coreSettings/watchPid	Si se establece en 1, la conexión se supervisa bajo el nombre especificado por `appName`. No debería ser necesario modificar esta clave.
root/ConnectionType/ssh/coreSettings/wrapperScript	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Este es el script principal que administra todos los ajustes de conexión y argumentos de línea de comandos para la conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/ssh/gui/SshManager/name	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/ssh/gui/SshManager/status	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/ssh/gui/SshManager/title	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/ssh/gui/SshManager/widgets/address	Controla el estado del widget **Dirección** en el Administrador de conexión Secure Shell. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/application	Controla el estado del widget **Ejecutar aplicación** en el Administrador de conexión Secure Shell. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/autoReconnect	Controla el estado del widget **Reconexión automática** en el Administrador de conexión Secure Shell. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como

Tabla E-8 Claves de registro de SSH (continúa)

Clave de registro	Descripción
	inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/autostart	Controla el estado del widget **Prioridad de inicio automático** en el Administrador de conexión Secure Shell. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/backgroundColor	Controla el estado del widget **Color de segundo plano** en el Administrador de conexión Secure Shell. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/compression	Controla el estado del widget **Compresión** en el Administrador de conexión Secure Shell. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/fallBackConnection	Controla el estado del widget **Conexión de Seguridad** en el Administrador de conexión Secure Shell. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/font	Controla el estado del widget **Fuente** en el Administrador de conexión Secure Shell. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/foregroundColor	Controla el estado del widget **Color de primer plano** en el Administrador de conexión Secure Shell. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/fork	Controla el estado del widget **Bifurque en segundo plano** en el Administrador de conexión Secure Shell. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/hasDesktopIcon	Controla el estado del widget **Mostrar icono en escritorio** en el Administrador de conexión Secure Shell. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/isInMenu	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.

Tabla E-8 Claves de registro de SSH (continúa)

Clave de registro	Descripción
root/ConnectionType/ssh/gui/SshManager/widgets/label	Controla el estado del widget **Nombre** en el Administrador de conexión Secure Shell. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/port	Controla el estado del widget **Puerto** en el Administrador de conexión Secure Shell. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/tty	Controla el estado del widget **Obligue alocación TTY** en el Administrador de conexión Secure Shell. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/username	Controla el estado del widget **Nombre de usuario** en el Administrador de conexión Secure Shell. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/waitForNetwork	Controla el estado del widget **Esperando por red antes de conectar** en el Administrador de conexión Secure Shell. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/x11	Controla el estado del widget **Envío de conexión X11** en el Administrador de conexión Secure Shell. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.

telnet

Claves de registro de ConnectionType/telnet.

Tabla E-9 Claves de registro de ConnectionType/telnet

Clave de registro	Descripción
root/ConnectionType/telnet/authorizations/user/add	Si se establece en 1, un usuario final tiene permiso para agregar una nueva conexión de este tipo utilizando el Administrador de conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/telnet/authorizations/user/general	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones generales para este tipo de conexión utilizando el Administrador de conexión. Esta tecla no tiene efecto en Smart Zero.

Tabla E-9 Claves de registro de ConnectionType/telnet (continúa)

Clave de registro	Descripción
root/ConnectionType/telnet/connections/<UUID>/address	Establece el nombre de host o la dirección IP a la cual conectarse.
root/ConnectionType/telnet/connections/<UUID>/afterStartedCommand	Establece el comando que se debe ejecutar después de que se ha iniciado la conexión.
root/ConnectionType/telnet/connections/<UUID>/afterStoppedCommand	Establece el comando que se debe ejecutar después de que se ha detenido la conexión.
root/ConnectionType/telnet/connections/<UUID>/authorizations/user/edit	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones para esta conexión.
root/ConnectionType/telnet/connections/<UUID>/authorizations/user/execution	Si se establece en 1, un usuario final tiene permiso para ejecutar esta conexión.
root/ConnectionType/telnet/connections/<UUID>/autoReconnect	Si se establece en 1, la conexión se reiniciará cuando se cierre o desconecte.
root/ConnectionType/telnet/connections/<UUID>/autostart	Si se establece en un valor de 1 a 5, la conexión se iniciará automáticamente después de que arranque el sistema, con el valor de 1 con la prioridad más alta.
root/ConnectionType/telnet/connections/<UUID>/backgroundColor	Establece el color de fondo de la conexión.
root/ConnectionType/telnet/connections/<UUID>/beforeStartingCommand	Establece que se ejecute el comando antes de que empiece la conexión.
root/ConnectionType/telnet/connections/<UUID>/connectionEndAction	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/telnet/connections/<UUID>/coord	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/telnet/connections/<UUID>/dependConnectionId	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/telnet/connections/<UUID>/extraEnvValues/<UUID>/key	Establece el nombre de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/telnet/connections/<UUID>/extraEnvValues/<UUID>/value	Establece el valor de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/telnet/connections/<UUID>/fallBackConnection	Establece la conexión alternativa a través de su UUID.
root/ConnectionType/telnet/connections/<UUID>/font	Establece el tamaño de la letra de la conexión.
root/ConnectionType/telnet/connections/<UUID>/foregroundColor	Establece el color de primer plano de la conexión.
root/ConnectionType/telnet/connections/<UUID>/hasDesktopIcon	Si se establece en 1, se activa el icono del escritorio para esta conexión. Esta tecla no tiene efecto en Smart Zero.

Tabla E-9 Claves de registro de ConnectionType/telnet (continúa)

Clave de registro	Descripción
root/ConnectionType/telnet/connections/<UUID>/iconPosition	Establece las coordinadas x,y de un icono de escritorio fijo. Si no se especifica, el icono queda flotante.
root/ConnectionType/telnet/connections/<UUID>/label	Establece el nombre de conexión que se muestra en la interfaz de usuario. En Smart Zero, por lo general esta opción se establece en `Default Connection` y no aparece en la interfaz de usuario.
root/ConnectionType/telnet/connections/<UUID>/locale	Establece la ubicación de la conexión.
root/ConnectionType/telnet/connections/<UUID>/loginfields/server	Si se establece en 1, el cuadro **Servidor** aparece en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el cuadro aparece pero deshabilitado. Si se establece en 0, el cuadro queda oculto. Si se establece en 3, se usan los ajustes del sistema.
root/ConnectionType/telnet/connections/<UUID>/port	Establece el número de puerto que se utiliza cuando se comunica con el servidor. De forma predeterminada es 23.
root/ConnectionType/telnet/connections/<UUID>/startMode	Si se ajusta en el valor predeterminado `focus` (concentrar) y la conexión se ha iniciado, la conexión se concentrará. De lo contrario, aparecerá un error que indica que la conexión ya se ha iniciado.
root/ConnectionType/telnet/connections/<UUID>/waitForNetwork	Si se establece en 1, la conexión no se iniciará hasta que la red esté disponible. Esto garantiza que, en una red lenta, la conexión no se inicie antes de que la red esté disponible, lo que podría provocar una falla.
root/ConnectionType/telnet/coreSettings/USBrelevant	Especifica si este tipo de conexión es relevante para el USB. Si es así, puede tener un complemento USB para redirigir dispositivos USB.
root/ConnectionType/telnet/coreSettings/appName	Establece el nombre de la aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/telnet/coreSettings/className	Establece el nombre de la clase de aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/telnet/coreSettings/editor	Establece el nombre de la aplicación interna que se utiliza cuando se inicia el Administrador de conexión para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/telnet/coreSettings/generalSettingsEditor	Establece el nombre de la aplicación interna que se utiliza cuando se inicia el Administrador de ajustes generales para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/telnet/coreSettings/icon	Especifica el icono del conjunto de temas de iconos que se pueden usar con esta conexión.
root/ConnectionType/telnet/coreSettings/icon16Path	Establece la ruta al icono de 16 x 16 píxeles para esta aplicación.
root/ConnectionType/telnet/coreSettings/icon32Path	Establece la ruta al icono de 32 x 32 píxeles para esta aplicación.
root/ConnectionType/telnet/coreSettings/icon48Path	Establece la ruta al icono de 48 x 48 píxeles para esta aplicación.

Tabla E-9 Claves de registro de ConnectionType/telnet (continúa)

Clave de registro	Descripción
root/ConnectionType/telnet/coreSettings/iconActive	Reservado para uso futuro.
root/ConnectionType/telnet/coreSettings/label	Establece el nombre que se va a mostrar para este tipo de conexión en la interfaz de usuario.
root/ConnectionType/telnet/coreSettings/priorityInConnectionLists	Establece la prioridad de este tipo de conexión cuando se muestra en el Administrador de conexión y en el Asistente de configuración que aparece durante la configuración inicial. Un valor superior moverá el tipo de conexión hacia la parte superior de la lista. Si se establece en 0, el tipo de conexión está oculto desde el Asistente de configuración y aparece de último en el Administrador de conexión. Los tipos de conexiones con la misma prioridad se enumeran en orden alfabético.
root/ConnectionType/telnet/coreSettings/serverRequired	Establece si un nombre o dirección de servidor es `unused`, `optional` o `required` para este tipo de conexión.
root/ConnectionType/telnet/coreSettings/stopProcess	Establece el comportamiento que debería ocurrir cuando se llama `connection-mgr stop` en esta conexión. De forma predeterminada, está opción es `close`, lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como `kill`, el proceso especificado por `appName` se interrumpirá de forma forzada. Cuando se establece como `custom` se ejecutará una línea de comandos de ejecución personalizada especificada por `wrapperScript` con el argumento `stop` para finalizar el proceso correctamente.
root/ConnectionType/telnet/coreSettings/tier	Especifica la importancia relativa de este tipo de conexión y el orden en el que se enumera en el menú Crear.
root/ConnectionType/telnet/coreSettings/wrapperScript	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Este es el script principal que administra todos los ajustes de conexión y argumentos de línea de comandos para la conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/telnet/gui/TelnetManager/name	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/telnet/gui/TelnetManager/status	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/telnet/gui/TelnetManager/title	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/telnet/gui/TelnetManager/widgets/address	Controla el estado del widget **Dirección** en el Administrador de conexión Telnet. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
root/ConnectionType/telnet/gui/TelnetManager/widgets/autoReconnect	Controla el estado del widget **Reconexión automática** en el Administrador de conexión Telnet. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.

Tabla E-9 Claves de registro de ConnectionType/telnet (continúa)

Clave de registro	Descripción
root/ConnectionType/telnet/gui/TelnetManager/widgets/autostart	Controla el estado del widget **Prioridad de inicio automático** en el Administrador de conexión Telnet. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/telnet/gui/TelnetManager/widgets/backgroundColor	Controla el estado del widget **Color de segundo plano** en el Administrador de conexión Telnet. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/telnet/gui/TelnetManager/widgets/fallBackConnection	Controla el estado del widget **Conexión de Seguridad** en el Administrador de conexión Telnet. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/telnet/gui/TelnetManager/widgets/foregroundColor	Controla el estado del widget **Color de primer plano** en el Administrador de conexión Telnet. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/telnet/gui/TelnetManager/widgets/hasDesktopIcon	Controla el estado del widget **Mostrar icono en escritorio** en el Administrador de conexión Telnet. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/telnet/gui/TelnetManager/widgets/label	Controla el estado del widget **Nombre** en el Administrador de conexión Telnet. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/telnet/gui/TelnetManager/widgets/port	Controla el estado del widget **Puerto** en el Administrador de conexión Telnet. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/telnet/gui/TelnetManager/widgets/waitForNetwork	Controla el estado del widget **Esperando por red antes de conectar** en el Administrador de conexión Telnet. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.

TTerm

Claves de registro de TTerm.

Tabla E-10 Claves de registro de TTerm

Clave de registro	Descripción
root/ConnectionType/tterm/connections/<UUID>/authorizations/user/edit	Si se establece en 1, los usuarios finales tienen permiso para modificar las configuraciones para esta conexión.
root/ConnectionType/tterm/connections/<UUID>/authorizations/user/execution	Si se establece en 1, los usuarios finales tienen permiso para ejecutar esta conexión.
root/ConnectionType/tterm/connections/<UUID>/ loginfields/password	Si se establece en 1, el campo `Contraseña` se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el campo se muestra pero desactivado. Si se establece en 0, el campo queda oculto. Si se establece en 3, los ajustes del sistema tienen prioridad.
root/ConnectionType/tterm/connections/<UUID>/waitForNetwork	Si se establece en 1, la conexión no se iniciará hasta que haya una red disponible de forma que, en una red lenta, la conexión no se inicie antes de que haya una red disponible, lo que podría provocar un error.
root/ConnectionType/tterm/connections/<UUID>/autoReconnect	Si se establece en 1, la conexión se reiniciará cuando se cierre o se desconecte.
root/ConnectionType/tterm/connections/<UUID>/coord	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. No cambie este valor.
root/ConnectionType/tterm/connections/<UUID>/label	Establece el nombre de conexión que se muestra en la interfaz de usuario. En Smart Zero, por lo general esta opción se establece en `Conexión predeterminada` y no aparece en la interfaz de usuario.
root/ConnectionType/tterm/connections/<UUID>/full-screen	Ejecuta la conexión en modo de pantalla completa, si está configurado.
root/ConnectionType/tterm/connections/<UUID>/maximized	Ejecuta la conexión en el modo maximizado, si está configurado.
root/ConnectionType/tterm/connections/<UUID>/sessionPanel	Si no está en modo de pantalla completa, debe establecerse en 0 para borrar el panel de sesión en el inicio.
root/ConnectionType/tterm/connections/<UUID>/profile/name	El nombre del perfil se guarda aquí. No lo edite manualmente; utilice el Administrador de conexiones.
root/ConnectionType/tterm/connections/<UUID>/profile/ttexp	El archivo del perfil se guarda aquí. No lo edite manualmente; utilice el Administrador de conexiones.
root/ConnectionType/tterm/connections/<UUID>/iconPosition	Para los iconos del escritorio anclados, un par x,y. Para los iconos flotantes, deje esta cadena en blanco.
root/ConnectionType/tterm/connections/<UUID>/autostart	Si se establece en un valor de 1 a 5, la conexión se inicia automáticamente después de que arranque el sistema, con el valor de 1 con la prioridad más alta.

Tabla E-10 Claves de registro de TTerm (continúa)

Clave de registro	Descripción
root/ConnectionType/tterm/connections/<UUID>/address	Establece el nombre de host o la dirección IP a la cual conectarse.
root/ConnectionType/tterm/connections/<UUID>/locale	Establece la ubicación de la conexión.
root/ConnectionType/tterm/connections/<UUID>/hasDesktopIcon	Si se establece en 1, se activa el icono del escritorio para esta conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/tterm/connections/<UUID>/extraEnvValues/<UUID>/key	Establece el nombre de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/tterm/connections/<UUID>/extraEnvValues/<UUID>/value	Establece el valor de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/tterm/connections/<UUID>/afterStartedCommand	Establece el comando que se debe ejecutar después de que se ha iniciado la conexión.
root/ConnectionType/tterm/connections/<UUID>/afterStoppedCommand	Establece el comando que se debe ejecutar después de que se ha detenido la conexión.
root/ConnectionType/tterm/connections/<UUID>/beforeStartingCommand	Establece que se ejecute el comando antes de iniciar la conexión.
root/ConnectionType/tterm/connections/<UUID>/startMode	Si se ajusta en el valor predeterminado `focus` (concentrar) y la conexión se ha iniciado, la conexión se concentrará. De lo contrario, aparecerá un error que indica que la conexión ya se ha iniciado.
root/ConnectionType/tterm/connections/<UUID>/dependConnectionId	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. No cambie este valor.
root/ConnectionType/tterm/connections/<UUID>/fallBackConnection	Establece la conexión alternativa a través de su UUID.
root/ConnectionType/tterm/connections/<UUID>/ connectionEndAction	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. No cambie este valor.

view

Claves de registro de VMware Horizon View.

Tabla E-11 Claves de registro de ConnectionType/view

Clave de registro	Descripción
root/ConnectionType/view/authorizations/user/add	Si se establece en 1, un usuario final tiene permiso para agregar una nueva conexión de este tipo utilizando el Administrador de conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/view/authorizations/user/commandLineBox	Si se establece en 1, un usuario final tiene permiso para introducir argumentos de línea de comando en el Administrador de conexión VMware Horizon View.
root/ConnectionType/view/authorizations/user/general	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones generales para este tipo de conexión utilizando el Administrador de conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/view/connections/<UUID>/ExtraArgs	Especifica los argumentos adicionales para el cliente VMware Horizon View. Ejecute `view_client --help` o `vmware-view --help` desde un terminal X para ver todos los argumentos disponibles.
root/ConnectionType/view/connections/<UUID>/SingleSignOn	
root/ConnectionType/view/connections/<UUID>/afterStartedCommand	Establece el comando que se debe ejecutar después de que se ha iniciado la conexión.
root/ConnectionType/view/connections/<UUID>/afterStoppedCommand	Establece el comando que se debe ejecutar después de que se ha detenido la conexión.
root/ConnectionType/view/connections/<UUID>/allowBlacklistedDrivers	Si se establece en 1, permite que las conexiones VMware Horizon View habiliten el recurso H.264 con controladores gráficos de código abierto AMD. Si se establece en 0, las conexiones de VMware Horizon View deshabilitan la aceleración de hardware con controladores en lista negra (como AMDGPU y Radeon).
root/ConnectionType/view/connections/<UUID>/appInMenu	Si se establece en 1, todas las aplicaciones de esta conexión se mostrarán en la barra de tareas.
root/ConnectionType/view/connections/<UUID>/appOnDesktop	Si se establece en 1, todas las aplicaciones de esta conexión se mostrarán en el escritorio.
root/ConnectionType/view/connections/<UUID>/applicationSize	Establece el tamaño en el que el cliente de VMware Horizon View iniciará las aplicaciones.
root/ConnectionType/view/connections/<UUID>/attachToConsole	
root/ConnectionType/view/connections/<UUID>/authorizations/user/edit	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones para esta conexión.
root/ConnectionType/view/connections/<UUID>/authorizations/user/execution	Si se establece en 1, un usuario final tiene permiso para ejecutar esta conexión.
root/ConnectionType/view/connections/<UUID>/autoHideMenuBar	
root/ConnectionType/view/connections/<UUID>/autoReconnect	Si se establece en 1, la conexión se reiniciará cuando se cierre o desconecte.
root/ConnectionType/view/connections/<UUID>/autoReconnectDelay	Establece la cantidad de tiempo en segundos que se deben esperar antes de volver a conectar la sesión. El valor predeterminado 0 hará que la conexión se reactive

Tabla E-11 Claves de registro de ConnectionType/view (continúa)

Clave de registro	Descripción
	inmediatamente. Esta configuración solo surte efecto cuando `autoReconnect` se establece en 1.
`root/ConnectionType/view/connections/<UUID>/automaticLogin`	Si se establece en 1, el cliente de VMware Horizon View intentará iniciar sesión automáticamente si se brindan todos los campos. Si se establece en 0, los usuarios tienen que seleccionar manualmente **Conectar** en el cliente de VMware Horizon View, iniciar sesión y seleccionar un escritorio.
`root/ConnectionType/view/connections/<UUID>/autostart`	Si se establece en un valor de 1 a 5, la conexión se iniciará automáticamente después de que arranque el sistema, con el valor de 1 con la prioridad más alta.
`root/ConnectionType/view/connections/<UUID>/autostartDelay`	Reservado para uso futuro.
`root/ConnectionType/view/connections/<UUID>/beforeStartingCommand`	Establece que se ejecute el comando antes de que empiece la conexión.
`root/ConnectionType/view/connections/<UUID>/closeAfterDisconnect`	Si se establece en 1, la conexión concluye después de que se cierra el primer escritorio. Si se establece en 0, el cliente de VMware Horizon View vuelve a la pantalla de selección de escritorio. Esta opción está activada de forma predeterminada para evitar que los usuarios dejen la conexión en la pantalla de selección de escritorio accidentalmente después de cerrar la sesión.
`root/ConnectionType/view/connections/<UUID>/closeAfterRoaming`	Si se establece en 1, la conexión VMware se desconectará si se lleva a otro lugar.
`root/ConnectionType/view/connections/<UUID>/coord`	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
`root/ConnectionType/view/connections/<UUID>/credentialsType`	Especifica el tipo de credencial entre `anonymous` (acceso no autenticado), `sso` (inicio de sesión único), `startup` (las credenciales se solicitan en el inicio), `password` (contraseña/dominio/usuario preconfigurados) o `smartcard` (smart card preconfigurada).
`root/ConnectionType/view/connections/<UUID>/dependConnectionId`	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
`root/ConnectionType/view/connections/<UUID>/desktop`	Si se especifica, el escritorio nombrado se iniciará automáticamente tras iniciar sesión. De forma predeterminada, si hay solo un escritorio disponible, este iniciará sesión automáticamente sin necesidad de especificarlo.
`root/ConnectionType/view/connections/<UUID>/desktopSize`	Establece el tamaño en el que el cliente de VMware Horizon View iniciará el escritorio.
`root/ConnectionType/view/connections/<UUID>/directory`	
`root/ConnectionType/view/connections/<UUID>/disableMaximizedApp`	Si se establece en 1, se desactiva la configuración de tamaño de ventana para aplicaciones maximizadas.
`root/ConnectionType/view/connections/<UUID>/domain`	Establece el dominio que se proporciona al View Connection Server. Si no hay ningún dominio especificado, se utiliza el dominio predeterminado para el servidor.

Tabla E-11 Claves de registro de ConnectionType/view (continúa)

Clave de registro	Descripción
root/ConnectionType/view/connections/<UUID>/enableCDR	Si se establece en 1, se habilita el complemento Redirección de unidad cliente.
root/ConnectionType/view/connections/<UUID>/enableMMR	Si se establece en 1, se habilita el complemento Redirección de multimedia mediante el protocolo Blast/PCoIP. Esto hace que los códecs compatibles que se reproducen a través de Windows Media Player se redirijan al cliente. Esto mejora notablemente la reproducción de video de alta definición y en pantalla completa para códecs como WMV9, VC1 y MPEG4. El video se renderiza localmente mediante la energía de la CPU.
root/ConnectionType/view/connections/<UUID>/enableMediaProvider	Si se establece en 1, se habilita el componente VMware Horizon Virtualization Pack para Skype Empresarial. Este componente habilita a los usuarios de Linux para que redirijan las llamadas de Skype Empresarial con el cliente VMware Horizon View.
root/ConnectionType/view/connections/<UUID>/enableSeamlessWindow	Si se establece en 1, el cliente VMware Horizon View inicia las aplicaciones en el modo de ventana continua.
root/ConnectionType/view/connections/<UUID>/enableSingleMode	
root/ConnectionType/view/connections/<UUID>/extraEnvValues/<UUID>/key	Establece el nombre de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/view/connections/<UUID>/extraEnvValues/<UUID>/value	Establece el valor de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/view/connections/<UUID>/fallBackConnection	Establece la conexión alternativa a través de su UUID.
root/ConnectionType/view/connections/<UUID>/fullscreen	Si se establece en 1, el cliente de VMware Horizon View abre en modo de pantalla completa cuando inicia.
root/ConnectionType/view/connections/<UUID>/hasDesktopIcon	Si se establece en 1, se activa el icono del escritorio para esta conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/view/connections/<UUID>/hideMenuBar	Si se establece en 1, la barra de menú superior en el escritorio está oculta. Esta barra se utiliza para administrar dispositivos remotos e iniciar otros escritorios.
root/ConnectionType/view/connections/<UUID>/iconPosition	Establece las coordinadas x,y de un icono de escritorio fijo. Si no se especifica, el icono queda flotante.
root/ConnectionType/view/connections/<UUID>/isInMenu	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/view/connections/<UUID>/label	Establece el nombre de conexión que se muestra en la interfaz de usuario. En Smart Zero, por lo general esta opción se establece en `Default Connection` y no aparece en la interfaz de usuario.
root/ConnectionType/view/connections/<UUID>/lockServer	Si se establece en 1, los usuarios finales no podrán cambiar la dirección del servidor.
root/ConnectionType/view/connections/<UUID>/loginfields/domain	Si se establece en 1, el campo **Dominio** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el campo se muestra pero desactivado. Si se establece en 0, el campo queda oculto.

Tabla E-11 Claves de registro de ConnectionType/view (continúa)

Clave de registro	Descripción
root/ConnectionType/view/connections/<UUID>/loginfields/password	Si se establece en 1, el campo **Contraseña** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el campo se muestra pero desactivado. Si se establece en 0, el campo queda oculto.
root/ConnectionType/view/connections/<UUID>/loginfields/rememberme	Si se establece en 1, la casilla de verificación **Recordarme** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, la casilla de verificación aparece pero deshabilitada. Si se establece en 0, la casilla de verificación está oculta.
root/ConnectionType/view/connections/<UUID>/loginfields/server	Si se establece en 1, el cuadro **Servidor** aparece en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el cuadro aparece pero deshabilitado. Si se establece en 0, el cuadro queda oculto. Si se establece en 3, se usan los ajustes del sistema.
root/ConnectionType/view/connections/<UUID>/loginfields/showpassword	Si se establece en 1, la casilla de verificación **Mostrar contraseña** aparece en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, la casilla de verificación aparece pero deshabilitada. Si se establece en 0, la casilla de verificación está oculta.
root/ConnectionType/view/connections/<UUID>/loginfields/smartcard	Si se establece en 1, la casilla de verificación **Inicio de sesión con smart card** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, la casilla de verificación aparece pero deshabilitada. Si se establece en 0, la casilla de verificación está oculta. Es posible que esta casilla de verificación no aparezca si no se detecta ninguna smart card, incluso si esta opción está habilitada.
root/ConnectionType/view/connections/<UUID>/loginfields/username	Si se establece en 1, el campo **Nombre de usuario** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el campo se muestra pero desactivado. Si se establece en 0, el campo queda oculto.
root/ConnectionType/view/connections/<UUID>/networkCondition	Permite la selección de las condiciones de red para obtener la mejor experiencia.
root/ConnectionType/view/connections/<UUID>/password	Establece la contraseña predeterminada que se suministra al host remoto durante el inicio de sesión. Este valor se encriptará. Por lo general, este ajuste se utiliza con las aplicaciones de estilo quiosco donde se usa una contraseña genérica para el inicio de sesión.
root/ConnectionType/view/connections/<UUID>/preferredProtocol	Establece el protocolo preferido.
root/ConnectionType/view/connections/<UUID>/printerMapping	Si se establece en 1, todas las impresoras definidas localmente a través de CUPS se redirigen al host remoto mediante ThinPrint. Si se establece en 0, se deshabilita la asignación de la impresora. Si se establece en 2, las impresoras USB se redirigen según la configuración del Administrador de USB.
root/ConnectionType/view/connections/<UUID>/saveCredentials	
root/ConnectionType/view/connections/<UUID>/sendCtrlAltDelToVM	
root/ConnectionType/view/connections/<UUID>/server	Establece la dirección del host remoto al cual conectarse. Normalmente es una URL como `http://server.domain.com`.

Tabla E-11 Claves de registro de ConnectionType/view (continúa)

Clave de registro	Descripción
root/ConnectionType/view/connections/<UUID>/sessionEndAction	
root/ConnectionType/view/connections/<UUID>/singleDesktop	
root/ConnectionType/view/connections/<UUID>/smartcard	Si se establece en 1, las smart cards conectadas localmente se envían al host remoto. Esto permite que las aplicaciones del host remoto las usen. Esto sólo permite el inicio de sesión de la smart card en el host remoto, no en View Connection Server.
root/ConnectionType/view/connections/<UUID>/startMode	Si se ajusta en el valor predeterminado `focus` (concentrar) y la conexión se ha iniciado, la conexión se concentrará. De lo contrario, aparecerá un error que indica que la conexión ya se ha iniciado.
root/ConnectionType/view/connections/<UUID>/usbAutoConnectAtStartUp	
root/ConnectionType/view/connections/<UUID>/usbAutoConnectOnInsert	
root/ConnectionType/view/connections/<UUID>/useCurrentViewConfig	Si se establece en 1, los scripts de HP no crean un nuevo archivo `/etc/vmware/config` y el cliente VMware Horizon View usa el archivo `/etc/vmware/config` actual.
root/ConnectionType/view/connections/<UUID>/username	Establece el nombre de usuario predeterminado que se suministra al host remoto durante el inicio de sesión. Por lo general, esta configuración se utiliza con las aplicaciones al estilo quiosco donde se usa un nombre de usuario genérico para el inicio de sesión.
root/ConnectionType/view/connections/<UUID>/viewSecurityLevel	Si se establece como `Refuse insecure connections` el cliente de VMware Horizon View no permitirá que el usuario se conecte al View Connection Server si el certificado SSL del servidor es inválido. Si se establece como `Warn`, el cliente de VMware Horizon View mostrará una advertencia en caso de que no se pueda verificar el certificado del servidor. Si el certificado está autofirmado o expirado, el usuario no podrá conectarse. Si se establece como `Allow all connections`, certificado del servidor no se verificará y se permitirán las conexiones a cualquier servidor.
root/ConnectionType/view/connections/<UUID>/waitForNetwork	Si se establece en 1, la conexión no se iniciará hasta que la red esté disponible. Esto garantiza que, en una red lenta, la conexión no se inicie antes de que la red esté disponible, lo que podría provocar una falla.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/attachToConsole	
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/audioLatency	Establece el promedio de milisegundos de desfase entre la transmisión de audio y la visualización de los fotogramas de video correspondientes después de la decodificación.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/clipboardExtension	Cuando se establece en 1, la funcionalidad del portapapeles se activa entre diferentes sesiones de RDP y entre sesiones de RDP y el sistema local.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/colorDepth	Este ajuste no se recomienda. Se utiliza para reducir la profundidad de color de la conexión por debajo de la resolución nativa del escritorio. Con frecuencia, esto se ha utilizado para reducir el ancho de banda de la red. Reducir la profundidad de

Tabla E-11 Claves de registro de ConnectionType/view (continúa)

Clave de registro	Descripción
	color a un nivel no admitido por el controlador de video puede causar daños en la pantalla o generar fallos.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/compression	Si se establece en 1, se activa la compresión de datos RDP entre el cliente y el servidor.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/disableMMRwithRFX	Si se establece en 1, se desactiva la redirección de contenido multimedia en caso de que se establezca una sesión RemoteFX válida.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/enableMMR	Si se establece en 1, se habilita el complemento Redirección de multimedia. Esto hace que los códecs compatibles que se reproducen a través de Windows Media Player se redirijan al cliente.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/frameAcknowledgeCount	Establece el número de fotogramas de video que el servidor puede forzar sin tener que esperar el reconocimiento desde el cliente. Los números más bajos tienen como consecuencia una mayor capacidad de respuesta del escritorio pero menos fotogramas por segundo. Si se establece en 0, no se utiliza el reconocimiento de fotogramas en las interacciones del cliente y el servidor.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/general/sendHostname	Si se establece en `hostname`, el nombre de host del sistema se envía al host remoto. Esto suele utilizarse para identificar el thin client asociado a una sesión particular de RDP. El nombre de host enviado se puede anular mediante `sendHostname` en la configuración específica para la conexión. Si se establece en `mac`, en vez del nombre de host, se envía la dirección MAC del primer adaptador de red disponible.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/hostnameType	Si se establece en hostname, el nombre de host del sistema se envía al host remoto. Esto suele utilizarse para identificar el thin client asociado a una sesión particular de RDP. El nombre de host enviado se puede anular mediante `sendHostname` en la configuración específica para la conexión. Si se establece en mac, en vez del nombre de host, se envía la dirección MAC del primer adaptador de red disponible.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/loadBalanceInfo	Este valor es la cookie de equilibrio de carga enviado al servidor para fines de intermediación tras la conexión y corresponde al campo `loadbalanceinfo` en el archivo .rdp. De forma predeterminada, el valor está vacío.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/mouseMotionEvents	Si se establece en 0, los eventos de movimiento del mouse no se envían al servidor. Esto puede evitar que algunos comentarios del usuario, como consejos sobre herramientas, funcionen correctamente.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/offScreenBitmaps	Si se establece en 0, se desactivan los mapas de bits fuera de pantalla. Esto puede aumentar el rendimiento ligeramente, pero hará que bloques de la pantalla se actualicen de forma asíncrona y, de esta forma, las transiciones de pantalla se actualizarán sin uniformidad
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagDesktopComposition	Si se establece en 1, permite la composición del escritorio (por ejemplo los bordes translúcidos) en caso de que sea compatible con el servidor. Al desactivar la composición del escritorio se puede mejorar el rendimiento de las conexiones con bajo ancho de banda. Por lo general, esto solo afecta a RemoteFX. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.

Tabla E-11 Claves de registro de ConnectionType/view (continúa)

Clave de registro	Descripción
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagFontSmoothing	Si se establece en 1, permite el suavizado de fuentes en caso de que sea compatible con el servidor y esté activado. Al desactivar el suavizado de fuentes puede mejorar el rendimiento de conexiones con bajo ancho de banda. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoCursorSettings	Si se establece en 1, se desactiva el parpadeo del cursor. Esto puede mejorar el rendimiento en conexiones RDP con bajo ancho de banda. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoCursorShadow	Si se establece en 1, se desactivan los controles remotos del cursor del mouse. Esto puede mejorar el rendimiento en conexiones RDP con bajo ancho de banda. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoMenuAnimations	Si se establece en 1, se desactivan las animaciones del menú. Esto puede mejorar el rendimiento en conexiones RDP con bajo ancho de banda. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoTheming	Si se establece en 1, se desactivan los temas de la interfaz del usuario. Esto puede mejorar el rendimiento en conexiones RDP con bajo ancho de banda. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoWallpaper	Si se establece en 1, se desactiva el fondo de pantalla del escritorio. Esto puede mejorar el rendimiento en conexiones RDP con bajo ancho de banda. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoWindowDrag	Si se establece en 1, se desactiva la función de arrastrar el contenido completo de la ventana. Esto puede mejorar el rendimiento en conexiones RDP con bajo ancho de banda. En su lugar se utiliza el contorno de la ventana. Si se establece en 2, el valor se selecciona con base en el rendimiento del thin client.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/portMapping	Si se establece en 1, los siguientes puertos seriales y paralelos se redirigen al host remoto: ttyS0, ttyS1, ttyS2, ttyS3, ttyUSB0, lp0.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/printerMapping	Si se establece en 1, todas las impresoras definidas localmente a través de CUPS se redirigen al host remoto.
root/ConnectionType/freerdp/connections/<UUID>/rdp6Buffering	Si se establece en 1, aumenta el rendimiento de gráficos que no son RemoteFX aunque las actualizaciones serán menos frecuentes.
root/ConnectionType/freerdp/connections/<UUID>/rdp8Codecs	Si se establece en 1, se utilizan códecs RDP 8 si están disponibles. Este ajuste debe desactivarse sólo en el caso de un defecto específico de los códecs RDP 8. Al desactivar este ajuste también podrían desactivarse códecs más avanzados.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/rdpEncryption	Si se establece en 1, la encriptación RDP estándar se utiliza para encriptar todos los datos entre el cliente y el servidor.
root/ConnectionType/freerdp/connections/<UUID>/rdpH264Codec	Si se establece en 1, se utilizan códecs RDP 8 H.264 si están disponibles. Este ajuste se ha reconocido por producir errores visuales, especialmente en configuraciones con varios monitores, y debe ser considerado experimental y no admitido. Al activar este ajuste simplemente se le informa al servidor que el thin client admite H.264 para la visualización del escritorio. El servidor también debe admitir H.264 y el servidor toma la decisión final

Tabla E-11 Claves de registro de ConnectionType/view (continúa)

Clave de registro	Descripción
	sobre cuál códec utilizar. Este ajuste afecta a solo los códecs de escritorio. No afecta los códecs de redirección de multimedia.
root/ConnectionType/freerdp/connections/<UUID>/rdpProgressiveCodec	Si se establece en 1, se utilizan códecs progresivos RDP 8 si están disponibles. Este ajuste debe desactivarse sólo en el caso de un defecto específico en los códecs progresivos RDP 8. Al desactivar este ajuste también podrían desactivarse códecs más avanzados.
root/ConnectionType/freerdp/connections/<UUID>/redirectPreference	Para la redirección, al cliente RDP se le brindan varias posibilidades de destino. Normalmente las trata en el siguiente orden: FQDN, IP principal, Lista de IP, NetBIOS. Si no se desea FQDN, se puede probar primero una de las alternativas al configurar esta clave de registro. Si el método especificado no funciona, el cliente RDP vuelve al orden original. Una configuración `auto` fuerza el orden original.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/remoteFx	Si se establece en 1, se utiliza RemoteFX en caso de que esté disponible.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/sendHostname	Establece el nombre de host del thin client que se envía al host remoto. Si se deja en blanco, se envía el nombre de host del sistema. Debe establecerse la clave de registro `root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/general/sendHostname` en `hostname` para que se use esta clave.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/sound	Si se establece en `Bring to this computer` el sonido se redirigirá desde el host remoto al cliente mediante un canal virtual estándar. Si se establece en `Leave at remote computer`, el sonido se deja en el host remoto. Esto puede ser útil cuando utiliza un dispositivo de audio USB redirigido. Si se establece en cualquier otro valor, se desactiva el audio. Por lo general, HP recomienda configurar este valor en `Bring to this computer` y no redirigir al host remoto los dispositivos de reproducción USB. Esto mejorará la calidad del audio y asegurará que el audio del cliente redirigido por otros métodos (como `Multimedia Redirection`) coincida con la configuración de audio local.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutError	Establece el número de milisegundos de espera después de perder la conexión antes de abandonar la reconexión con el servidor. Si se establece en 0, se reintenta la reconexión constantemente.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutRecovery	Establece el número de milisegundos de espera después de perder la conexión para que la red se recupere sin tratar de forzar una reconexión.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutWarning	Establece el número de milisegundos de espera después de perder la conexión antes de advertirle al usuario que la conexión se ha perdido.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutWarningDialog	Si se establece en 1, cuando se detecta que se perdió la conexión de extremo a extremo, aparece un cuadro de diálogo y la pantalla se pone gris. De lo contrario, se graban mensajes en el registro de la conexión y la sesión se congela.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutsEnabled	Si se establece en 1, se realizan las verificaciones de estado de la conexión de extremo a extremo.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/tlsVersion	Establece la versión de Transport Layer Security que se va a usar durante las fases iniciales de negociación con el servidor RDP.

Tabla E-11 Claves de registro de ConnectionType/view (continúa)

Clave de registro	Descripción
	Establézcala de forma que coincida con la versión de TLS utilizada por su servidor RDP, o trate de establecerla en auto. **NOTA:** Hay algunos defectos del lado del servidor en ciertos servidores RDP sin parches que pueden hacer que el ajuste automático falle, de forma que no sea el ajuste predeterminado.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/xkbLayoutId`	Establece un ID de disposición de XKB para omitir el teclado del sistema. Para ver la lista de ID disponibles, introduzca el siguiente comando en un terminal X: `xfreerdp --kbd-list`.
`root/ConnectionType/view/coreSettings/USBrelevant`	Indica si este tipo de conexión es relevante para el USB. Si es así, puede tener un complemento USB para redirigir dispositivos USB.
`root/ConnectionType/view/coreSettings/appName`	Establece el nombre de la aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
`root/ConnectionType/view/coreSettings/className`	Establece el nombre de la clase de aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
`root/ConnectionType/view/coreSettings/editor`	Establece el nombre de la aplicación interna que se utiliza cuando se inicia el Administrador de conexión para este tipo de conexión. No debería ser necesario modificar esta clave.
`root/ConnectionType/view/coreSettings/icon`	Especifica el icono del conjunto de temas de iconos que se pueden usar con esta conexión.
`root/ConnectionType/view/coreSettings/icon16Path`	Establece la ruta al icono de 16 x 16 píxeles para esta aplicación.
`root/ConnectionType/view/coreSettings/icon32Path`	Establece la ruta al icono de 32 x 32 píxeles para esta aplicación.
`root/ConnectionType/view/coreSettings/icon48Path`	Establece la ruta al icono de 48 x 48 píxeles para esta aplicación.
`root/ConnectionType/view/coreSettings/iconActive`	Reservado para uso futuro.
`root/ConnectionType/view/coreSettings/label`	Establece el nombre que se va a mostrar para este tipo de conexión en la interfaz de usuario.
`root/ConnectionType/view/coreSettings/priorityInConnectionLists`	Establece la prioridad de este tipo de conexión cuando se muestra en el Administrador de conexión y en el Asistente de configuración que aparece durante la configuración inicial. Un valor superior moverá el tipo de conexión hacia la parte superior de la lista. Si se establece en 0, el tipo de conexión está oculto desde el Asistente de configuración y aparece de último en el Administrador de conexión. Los tipos de conexiones con la misma prioridad se enumeran en orden alfabético.
`root/ConnectionType/view/coreSettings/serverRequired`	Establece si un nombre o dirección de servidor es `unused`, `optional` o `required` para este tipo de conexión.
`root/ConnectionType/view/coreSettings/stopProcess`	Establece el comportamiento que debería ocurrir cuando se llama `connection-mgr stop` en esta conexión. De forma predeterminada, está opción es `close`, lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como `kill`, el proceso especificado por `appName` se interrumpirá de forma forzada. Cuando se establece como `custom` se ejecutará

Tabla E-11 Claves de registro de ConnectionType/view (continúa)

Clave de registro	Descripción
	una línea de comandos de ejecución personalizada especificada por `wrapperScript` con el argumento `stop` para finalizar el proceso correctamente.
`root/ConnectionType/view/coreSettings/tier`	Especifica la importancia relativa de este tipo de conexión y el orden en el que se enumera en el menú Crear.
`root/ConnectionType/view/coreSettings/watchPid`	Si se establece en 1, la conexión se supervisa bajo el nombre especificado por `appName`. No debería ser necesario modificar esta clave.
`root/ConnectionType/view/coreSettings/wrapperScript`	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Este es el script principal que administra todos los ajustes de conexión y argumentos de línea de comandos para la conexión. No debería ser necesario modificar esta clave.
`root/ConnectionType/view/coreSettings/wrapperScriptGeneration`	Permite que el Administrador de conexiones sepa qué tipo de parámetros aprueban el script.
`root/ConnectionType/view/general/enableComPortRedirection`	
`root/ConnectionType/view/general/rdpOptions`	Las opciones que se especifican aquí se enviarán directamente al cliente RDP si RDP se utiliza como protocolo de pantalla de la conexión de VMware Horizon View. Para ver una lista completa de opciones, introduzca el siguiente comando en un terminal X: `rdesktop --help`.
`root/ConnectionType/view/gui/viewManager/name`	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
`root/ConnectionType/view/gui/viewManager/status`	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
`root/ConnectionType/view/gui/viewManager/title`	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
`root/ConnectionType/view/gui/viewManager/widgets/autostart`	Controla el estado del widget **Prioridad de inicio automático** en el Administrador de conexión VMware Horizon View. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/ConnectionType/view/gui/viewManager/widgets/fallBackConnection`	Controla el estado del widget **Conexión de Seguridad** en el Administrador de conexión VMware Horizon View. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/ConnectionType/view/gui/viewManager/widgets/label`	Controla el estado del widget **Nombre** en el Administrador de conexión VMware Horizon View. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.

AVD

Claves de registro de AVD.

Tabla E-12 Claves de registro de AVD

Clave de registro	Descripción
root/ConnectionType/wvd/connections/<UUID>/loginfields/server	Si se establece en 1, el campo `Servidor` se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el campo se muestra pero desactivado. Si se establece en 0, el campo queda oculto. Si se establece en 3, los ajustes del sistema tienen prioridad.
root/ConnectionType/wvd/connections/<UUID>/loginfields/username	Si se establece en 1, el campo `Nombre de usuario` se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el campo se muestra pero desactivado. Si se establece en 0, el campo queda oculto. Si se establece en 3, los ajustes del sistema tienen prioridad.
root/ConnectionType/wvd/connections/<UUID>/loginfields/password	Si se establece en 1, el campo `Contraseña` se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el campo se muestra pero desactivado. Si se establece en 0, el campo queda oculto. Si se establece en 3, los ajustes del sistema tienen prioridad.
root/ConnectionType/wvd/connections/<UUID>/loginfields/showPassword	Si se establece en 1, el botón `Mostrar contraseña` se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el botón se muestra pero deshabilitado. Si se establece en 0, el botón queda oculto. Si se establece en 3, los ajustes del sistema tienen prioridad. En ThinPro 6.2 y versiones posteriores, use el ajuste de seguridad de todo el sistema.
root/ConnectionType/wvd/connections/<UUID>/loginfields/domain	Si se establece en 1, el campo `Dominio` se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el campo se muestra pero desactivado. Si se establece en 0, el campo queda oculto. Si se establece en 3, los ajustes del sistema tienen prioridad.
root/ConnectionType/wvd/connections/<UUID>/loginfields/smartcard	Si se establece en 1, la casilla de verificación `Inicio de sesión con smart card` se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, la casilla de verificación aparece pero deshabilitada. Si se establece en 0, la casilla de verificación está oculta. Si se establece en 3, los ajustes del sistema tienen prioridad. Es posible que esta casilla de verificación no aparezca si no se detecta ninguna smart card, incluso si esta opción está habilitada.
root/ConnectionType/wvd/connections/<UUID>/loginfields/domainAwareUsername	Si se establece en 1, el nombre de usuario conoce el dominio, independientemente de la visibilidad del campo de dominio. En general, el nombre de usuario puede ser una dirección de correo electrónico.
root/ConnectionType/wvd/connections/<UUID>/loginfields/rememberme	Si se establece en 1, la casilla de verificación `Recordarme` se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, la casilla de verificación aparece pero deshabilitada. Si se establece en 0, la casilla de verificación está oculta. Si se establece en 3, los ajustes del sistema tienen prioridad.
root/ConnectionType/wvd/connections/<UUID>/seamlessWindow	Si se establece en 1, se desactivan las decoraciones de ventanas, lo que puede ser útil en una configuración con múltiples monitores para permitir que la conexión se configure al tamaño del monitor principal o del escritorio completo.
root/ConnectionType/wvd/connections/<UUID>/windowType	Esta configuración se pasa por alto para Smart Zero.

Tabla E-12 Claves de registro de AVD (continúa)

Clave de registro	Descripción
root/ConnectionType/wvd/connections/<UUID>/ windowSizeWidth	Ancho fijo de la ventana. Esta configuración se pasa por alto para Smart Zero.
root/ConnectionType/wvd/connections/<UUID>/ windowSizeHeight	Altura fija de la ventana. Esta configuración se pasa por alto para Smart Zero.
root/ConnectionType/wvd/connections/<UUID>/ displayScalePercent	Valor de escala de la visualización en porcentaje. El rango es de 100% a 500%.
root/ConnectionType/wvd/connections/<UUID>/ autofillCredentials	Si se establece en 1, las credenciales se establecen automáticamente en el cuadro de diálogo de autenticación de Microsoft.
root/ConnectionType/wvd/connections/<UUID>/ rememberMe	Si se establece en 1, las credenciales se establecen automáticamente en el cuadro de diálogo de autenticación de Microsoft.
root/ConnectionType/wvd/connections/<UUID>/ headlessMode	Si se establece en 1, se intenta una autenticación con las credenciales disponibles sin mostrar el cuadro de diálogo de autenticación de Microsoft.
root/ConnectionType/wvd/connections/<UUID>/ autostartWorkspace	Especifica el espacio de trabajo desde el cual un recurso se iniciará automáticamente. No es requerido para que un recurso se inicie automáticamente.
root/ConnectionType/wvd/connections/<UUID>/ autostartResource	Especifica un recurso que se iniciará automáticamente.
root/ConnectionType/wvd/connections/<UUID>/ autoCloseAvdFeed	Si se establece en 1, la ventana de feed AVD se cierra automáticamente después de cerrar un recurso.
root/ConnectionType/wvd/connections/<UUID>/ disableMenuBar	Si se establece en 1, la barra de menús no se muestra en la ventana de la sesión.
root/ConnectionType/wvd/connections/<UUID>/ disableDropdown	Si se establece en 1, el menú desplegable que aparece en el modo de pantalla completa no estará presente.
root/ConnectionType/wvd/connections/<UUID>/ dropdownClose	Si se establece en 1, el menú desplegable tendrá un botón para cerrar la ventana.
root/ConnectionType/wvd/connections/<UUID>/ dropdownMaximize	Si se establece en 1, el menú desplegable tendrá un botón para maximizar la ventana.
root/ConnectionType/wvd/connections/<UUID>/ dropdownMinimize	Si se establece en 1, el menú desplegable tendrá un botón para minimizar la ventana.
root/ConnectionType/wvd/connections/<UUID>/ dropdownMinimize	Si se establece en 1, el menú desplegable tendrá un botón para minimizar la ventana.
root/ConnectionType/wvd/connections/<UUID>/ dropdownCtrlAltD	Si se establece en 1, el menú desplegable tendrá Ctrl +Alt + Supr como acceso directo de teclado.
root/ConnectionType/wvd/connections/<UUID>/ localTimezone	Si se establece en 1, la zona horaria de la sesión se establece de acuerdo con la zona horaria del sistema local.
root/ConnectionType/wvd/connections/<UUID>/ audioOut	Si se establece en 1, se activa la reproducción de audio mediante conexiones AVD.

Tabla E-12 Claves de registro de AVD (continúa)

Clave de registro	Descripción
root/ConnectionType/wvd/connections/<UUID>/audioIn	Si está configurado en 1, la grabación de audio (micrófono) mediante conexiones AVD está activada.
root/ConnectionType/wvd/connections/<UUID>/filesystem	Si es 0, se desactiva el redireccionamiento del sistema de archivos; si es 1, se redirige la lista en filesystemList; si es 2, solo se redirigen los sistemas de archivos multimedia extraíbles.
root/ConnectionType/wvd/connections/<UUID>/filesystemList	Una lista separada por comas de los directorios redirigidos cuando el sistema de archivos es 1.
root/ConnectionType/wvd/connections/<UUID>/scRedirection	Si se establece en 1, se puede acceder a las smartcards en esta conexión AVD.
root/ConnectionType/wvd/connections/<UUID>/clipboard	Si es 0, los portapapeles de AVD no se comparten con ThinPro; si es 1, el portapapeles se comparte con todas las aplicaciones ThinPro; si es 2, el portapapeles se comparte solo entre las sesiones de AVD.
root/ConnectionType/wvd/connections/<UUID>/virtual	Si se establece en 1, se activa el canal virtual AVD.
root/ConnectionType/wvd/connections/<UUID>/camera	Si se establece en 1, se puede acceder a las cámaras en conexiones AVD.
root/ConnectionType/wvd/connections/<UUID>/ExtraArgs	Especifica los argumentos adicionales para el cliente AVD. Ejecute wvd-feed --help desde una terminal X para ver todos los argumentos disponibles.
root/ConnectionType/wvd/connections/<UUID>/authorizations/user/edit	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones para esta conexión.
root/ConnectionType/wvd/connections/<UUID>/authorizations/user/execution	Si se establece en 1, un usuario final tiene permiso para ejecutar esta conexión.
root/ConnectionType/wvd/connections/<UUID>/waitForNetwork	Si se establece en 1, la conexión no se iniciará hasta que haya una red disponible de forma que, en una red lenta, la conexión no se inicie antes de que haya una red disponible, lo que podría provocar un error.
root/ConnectionType/wvd/connections/<UUID>/autoReconnect	Si se establece en 1, la conexión se reiniciará cuando se cierre o se desconecte.
root/ConnectionType/wvd/connections/<UUID>/autostartDelay	Establece el tiempo en segundos que se debe esperar antes de que la conexión se inicie después del arranque del sistema. El valor predeterminado 0 hace que la conexión se inicie inmediatamente. Esta configuración solo surte efecto cuando autostart se ajusta en 1.
root/ConnectionType/wvd/connections/<UUID>/autoReconnectDelay	Establece la cantidad de tiempo en segundos que se deben esperar antes de volver a conectar la sesión. El valor predeterminado 0 hace que la conexión se reactive inmediatamente. Esta configuración solo surte efecto cuando autoReconnect se establece en 1.
root/ConnectionType/wvd/connections/<UUID>/forbiddenFiles	Esta clave de registro solo funciona cuando está seleccionado Permitir que las conexiones administren sus propias configuraciones en el Administrador de configuraciones generales de la conexión Web Browser. Los archivos enumerados en el valor de esta clave de registro se eliminan antes de iniciar la conexión Web Browser. Los nombres

Tabla E-12 Claves de registro de AVD (continúa)

Clave de registro	Descripción
	de archivo deben separarse por comas y se admite un comodín. Por ejemplo: *.rdf,cookies.sqlite
root/ConnectionType/wvd/connections/<UUID>/extraEnvValues/<UUID>/key	Establece el nombre de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/wvd/connections/<UUID>/extraEnvValues/<UUID>/value	Establece el valor de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/wvd/connections/<UUID>/extraEnvValues/<UUID>/credentialsType	Especifica si las credenciales deben proporcionarse mediante el inicio de sesión único, solicitadas en el inicio, o proporcionadas como usuario, dominio y contraseña preconfigurados.
root/ConnectionType/wvd/connections/<UUID>/username	Establece el nombre de usuario predeterminado que se suministra al host remoto durante el inicio de sesión. Por lo general, esta configuración se utiliza con las aplicaciones al estilo quiosco donde se usa un nombre de usuario genérico para el inicio de sesión.
root/ConnectionType/wvd/connections/<UUID>/domain	Si `credentialsType` es una `contraseña`, esta configuración proporciona el dominio predeterminado al host remoto durante el inicio de sesión. Si no hay ningún dominio especificado, se utilizará el dominio predeterminado para el host remoto.
root/ConnectionType/wvd/connections/<UUID>/SingleSignOn	Si se habilita, se guarda la combinación de usuario, dominio y contraseña de la conexión RDP para desbloquear el protector de pantalla.
root/ConnectionType/wvd/connections/<UUID>/password	Establece la contraseña predeterminada que se suministra al host remoto durante el inicio de sesión. Este valor se encriptará. Por lo general, este ajuste se utiliza con las aplicaciones de estilo quiosco donde se usa una contraseña genérica para el inicio de sesión.
root/ConnectionType/wvd/connections/<UUID>/workspaceURL	Establece la URL del área de trabajo que desea proporcionar a wvd. Si no hay una URL especificada, se usará la predeterminada para AVD.
root/ConnectionType/wvd/connections/<UUID>/allowInsecureConnections	Si se establece en 1, se permitirá continuar con la conexión insegura.
root/ConnectionType/wvd/connections/<UUID>/securityLevelclcl	Establece el nivel de seguridad del certificado. Si se establece en 0, se permiten todas las conexiones. Si se establece en 1, se verifican los hosts recordados y aparece un cuadro de diálogo de advertencia en caso de que no apruebe la verificación. Si se establece en 2, no se verifican los hosts recordados y aparece un cuadro de diálogo de advertencia en caso de que no apruebe la verificación. Si se establece en 3, se rechazan todas las conexiones inseguras.
root/ConnectionType/wvd/connections/<UUID>/coord	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. No cambie este valor.
root/ConnectionType/wvd/connections/<UUID>/autostart	Si se establece en un valor de 1 a 5, la conexión se inicia automáticamente después de que arranque el sistema, con el valor de 1 con la prioridad más alta.
root/ConnectionType/wvd/connections/<UUID>/dependConnectionId	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. No cambie este valor.
root/ConnectionType/wvd/connections/<UUID>/fallBackConnection	Establece la conexión alternativa a través de su UUID.

Tabla E-12 Claves de registro de AVD (continúa)

Clave de registro	Descripción
root/ConnectionType/wvd/connections/<UUID>/hasDesktopIcon	Si se establece en 1, se activa el icono del escritorio para esta conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/wvd/connections/<UUID>/startMode	Si se ajusta en el valor predeterminado `focus` (concentrar) y la conexión se ha iniciado, la conexión se concentrará. De lo contrario, aparecerá un error que indica que la conexión ya se ha iniciado.
root/ConnectionType/wvd/connections/<UUID>/label	Establece el nombre de conexión que se muestra en la interfaz de usuario. En Smart Zero, por lo general esta opción se establece en `Default Connection` y no aparece en la interfaz de usuario.
root/ConnectionType/wvd/connections/<UUID>/iconPosition	Para los iconos del escritorio anclados, un par x,y. Para los iconos flotantes, deje esta cadena en blanco.
root/ConnectionType/wvd/connections/<UUID>/afterStartedCommand	Establece que se ejecute el comando después de iniciar la conexión.
root/ConnectionType/wvd/connections/<UUID>/afterStoppedCommand	Establece el comando que se debe ejecutar después de que se ha detenido la conexión.
root/ConnectionType/wvd/connections/<UUID>/beforeStartingCommand	Establece que se ejecute el comando antes de iniciar la conexión.
root/ConnectionType/wvd/connections/<UUID>/connectionEndAction	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. No cambie este valor.

xdmcp

Claves de registro de XDMCP.

Tabla E-13 Claves de registro de XDMCP

Clave de registro	Descripción
root/ConnectionType/xdmcp/authorizations/user/add	Si se establece en 1, un usuario final tiene permiso para agregar una nueva conexión de este tipo utilizando el Administrador de conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/xdmcp/authorizations/user/general	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones generales para este tipo de conexión utilizando el Administrador de conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/xdmcp/connections/<UUID>/address	Establece el nombre de host o la dirección IP a la cual conectarse.
root/ConnectionType/xdmcp/connections/<UUID>/afterStartedCommand	Establece el comando que se debe ejecutar después de que se ha iniciado la conexión.
root/ConnectionType/xdmcp/connections/<UUID>/afterStoppedCommand	Establece el comando que se debe ejecutar después de que se ha detenido la conexión.
root/ConnectionType/xdmcp/connections/<UUID>/authorizations/user/edit	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones para esta conexión.

Tabla E-13 Claves de registro de XDMCP (continúa)

Clave de registro	Descripción
root/ConnectionType/xdmcp/connections/<UUID>/authorizations/user/execution	Si se establece en 1, un usuario final tiene permiso para ejecutar esta conexión.
root/ConnectionType/xdmcp/connections/<UUID>/autoReconnect	Si se establece en 1, la conexión se reiniciará cuando se cierre o desconecte.
root/ConnectionType/xdmcp/connections/<UUID>/autostart	Si se establece en un valor de 1 a 5, la conexión se iniciará automáticamente después de que arranque el sistema, con el valor de 1 con la prioridad más alta.
root/ConnectionType/xdmcp/connections/<UUID>/beforeStartingCommand	Establece que se ejecute el comando antes de que empiece la conexión.
root/ConnectionType/xdmcp/connections/<UUID>/color	Establece la profundidad de color de la pantalla de la conexión.
root/ConnectionType/xdmcp/connections/<UUID>/connectionEndAction	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xdmcp/connections/<UUID>/coord	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xdmcp/connections/<UUID>/dependConnectionId	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xdmcp/connections/<UUID>/extraEnvValues/<UUID>/key	Establece el nombre de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/xdmcp/connections/<UUID>/extraEnvValues/<UUID>/value	Establece el valor de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/xdmcp/connections/<UUID>/fallBackConnection	Establece la conexión alternativa a través de su UUID.
root/ConnectionType/xdmcp/connections/<UUID>/fontServer	Establece la dirección del servidor de fuentes que se va a utilizar. La clave de registro `useFontServer` también debe establecerse en 1.
root/ConnectionType/xdmcp/connections/<UUID>/hasDesktopIcon	Si se establece en 1, se activa el icono del escritorio para esta conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/xdmcp/connections/<UUID>/iconPosition	Establece las coordinadas x,y de un icono de escritorio fijo. Si no se especifica, el icono queda flotante.
root/ConnectionType/xdmcp/connections/<UUID>/isInMenu	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xdmcp/connections/<UUID>/label	Establece el nombre de conexión que se muestra en la interfaz de usuario. En Smart Zero, por lo general esta opción se establece en `Default Connection` y no aparece en la interfaz de usuario.
root/ConnectionType/xdmcp/connections/<UUID>/loginfields/server	Si se establece en 1, el cuadro **Servidor** aparece en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el cuadro aparece pero deshabilitado. Si se establece en 0, el cuadro queda oculto. Si se establece en 3, se usan los ajustes del sistema.

Tabla E-13 Claves de registro de XDMCP (continúa)

Clave de registro	Descripción
root/ConnectionType/xdmcp/connections/<UUID>/refreshRate	Establece la frecuencia de actualización de la pantalla para la conexión.
root/ConnectionType/xdmcp/connections/<UUID>/startMode	Si se ajusta en el valor predeterminado focus (concentrar) y la conexión se ha iniciado, la conexión se concentrará. De lo contrario, aparecerá un error que indica que la conexión ya se ha iniciado.
root/ConnectionType/xdmcp/connections/<UUID>/type	Establece el tipo de conexión XDMCP. Si se configura en chooser, todos los hosts se enumeran y el usuario puede seleccionar el host al cual desea conectarse. Si se configura en query, se envía una solicitud XDMCP directamente al host especificado. Si se configura en broadcast, todos los hosts disponibles se enumeran y se realiza automáticamente una conexión al primer host.
root/ConnectionType/xdmcp/connections/<UUID>/useFontServer	Si se configura en 1, se desactiva el servidor de fuentes. Si se configura en 0, se usa la fuente local.
root/ConnectionType/xdmcp/connections/<UUID>/waitForNetwork	Si se establece en 1, la conexión no se iniciará hasta que la red esté disponible. Esto garantiza que, en una red lenta, la conexión no se inicie antes de que la red esté disponible, lo que podría provocar una falla.
root/ConnectionType/xdmcp/connections/<UUID>/windowSize	Establece el tamaño de ventana de la conexión.
root/ConnectionType/xdmcp/coreSettings/USBrelevant	Especifica si este tipo de conexión es relevante para el USB. Si es así, puede tener un complemento USB para redirigir dispositivos USB.
root/ConnectionType/xdmcp/coreSettings/appName	Establece el nombre de la aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/xdmcp/coreSettings/audio	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xdmcp/coreSettings/className	Establece el nombre de la clase de aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/xdmcp/coreSettings/desktopButton	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xdmcp/coreSettings/editor	Establece el nombre de la aplicación interna que se utiliza cuando se inicia el Administrador de conexión para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/xdmcp/coreSettings/generalSettingsEditor	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xdmcp/coreSettings/icon	Especifica el icono del conjunto de temas de iconos que se pueden usar con esta conexión.
root/ConnectionType/xdmcp/coreSettings/icon16Path	Establece la ruta al icono de 16 x 16 píxeles para esta aplicación.
root/ConnectionType/xdmcp/coreSettings/icon32Path	Establece la ruta al icono de 32 x 32 píxeles para esta aplicación.

Tabla E-13 Claves de registro de XDMCP (continúa)

Clave de registro	Descripción
root/ConnectionType/xdmcp/coreSettings/icon48Path	Establece la ruta al icono de 48 x 48 píxeles para esta aplicación.
root/ConnectionType/xdmcp/coreSettings/iconActive	Reservado para uso futuro.
root/ConnectionType/xdmcp/coreSettings/label	Establece el nombre que se va a mostrar para este tipo de conexión en la interfaz de usuario.
root/ConnectionType/xdmcp/coreSettings/priorityInConnectionLists	Establece la prioridad de este tipo de conexión cuando se muestra en el Administrador de conexión y en el Asistente de configuración que aparece durante la configuración inicial. Un valor superior moverá el tipo de conexión hacia la parte superior de la lista. Si se establece en 0, el tipo de conexión está oculto desde el Asistente de configuración y aparece de último en el Administrador de conexión. Los tipos de conexiones con la misma prioridad se enumeran en orden alfabético.
root/ConnectionType/xdmcp/coreSettings/serverRequired	Establece si un nombre o dirección de servidor es `unused`, `optional` o `required` para este tipo de conexión.
root/ConnectionType/xdmcp/coreSettings/stopProcess	Establece el comportamiento que debería ocurrir cuando se llama `connection-mgr stop` en esta conexión. De forma predeterminada, está opción es `close`, lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como `kill`, el proceso especificado por `appName` se interrumpirá de forma forzada. Cuando se establece como `custom` se ejecutará una línea de comandos de ejecución personalizada especificada por `wrapperScript` con el argumento `stop` para finalizar el proceso correctamente.
root/ConnectionType/xdmcp/coreSettings/tier	Especifica la importancia relativa de este tipo de conexión y el orden en el que se enumera en el menú Crear.
root/ConnectionType/xdmcp/coreSettings/watchPid	Si se establece en 1, la conexión se supervisa bajo el nombre especificado por `appName`. No debería ser necesario modificar esta clave.
root/ConnectionType/xdmcp/coreSettings/wrapperScript	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Este es el script principal que administra todos los ajustes de conexión y argumentos de línea de comandos para la conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/xdmcp/gui/XdmcpManager/name	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xdmcp/gui/XdmcpManager/status	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xdmcp/gui/XdmcpManager/title	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/address	Controla el estado del widget **Dirección** en el Administrador de conexión XDMCP. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.

Tabla E-13 Claves de registro de XDMCP (continúa)

Clave de registro	Descripción
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/autoReconnect	Controla el estado del widget **Reconexión automática** en el Administrador de conexión XDMCP. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/autostart	Controla el estado del widget **Prioridad de inicio automático** en el Administrador de conexión XDMCP. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/color	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/fontServer	Controla el estado del widget **Servidor de fuente** en el Administrador de conexión XDMCP. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/hasDesktopIcon	Controla el estado del widget **Mostrar icono en escritorio** en el Administrador de conexión XDMCP. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/isInMenu	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/label	Controla el estado del widget **Nombre** en el Administrador de conexión XDMCP. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/refreshRate	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/type	Controla el estado del widget **Tipo** en el Administrador de conexión XDMCP. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/useFontServer	Controla el estado del widget **Utilizar servidor de fuente** en el Administrador de conexión XDMCP. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/waitForNetwork	Controla el estado del widget **Esperando por red antes de conectar** en el Administrador de conexión XDMCP. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como

Tabla E-13 Claves de registro de XDMCP (continúa)

Clave de registro	Descripción
	`inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/windowSize`	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.

xen

Claves de registro de ConnectionType/xen.

Tabla E-14 Claves de registro de ConnectionType/xen

Clave de registro	Descripción
`root/ConnectionType/xen/authorizations/user/add`	Si se establece en 1, un usuario final tiene permiso para agregar una nueva conexión de este tipo utilizando el Administrador de conexión. Esta tecla no tiene efecto en Smart Zero.
`root/ConnectionType/xen/authorizations/user/general`	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones generales para este tipo de conexión utilizando el Administrador de conexión. Esta tecla no tiene efecto en Smart Zero.
`root/ConnectionType/xen/connections/<UUID>/SingleSignOn`	Si se establece en 1, la conexión comparte las credenciales con el protector de pantalla.
`root/ConnectionType/xen/connections/<UUID>/address`	Establece la dirección del host remoto al cual conectarse. Normalmente es una URL como `http://server.domain.com`.
`root/ConnectionType/xen/connections/<UUID>/afterStartedCommand`	Establece el comando que se debe ejecutar después de que se ha iniciado la conexión.
`root/ConnectionType/xen/connections/<UUID>/afterStoppedCommand`	Establece el comando que se debe ejecutar después de que se ha detenido la conexión.
`root/ConnectionType/xen/connections/<UUID>/allowSaveConnInfo`	
`root/ConnectionType/xen/connections/<UUID>/appInMenu`	Si se establece en 1, todas las aplicaciones de la conexión se muestran en el menú de la barra de tareas.
`root/ConnectionType/xen/connections/<UUID>/appInWindowOrOnDesktop`	Si se establece en 1 y se habilita `appOnDesktop`, todas las aplicaciones de la conexión se muestran en una ventana intermedia. Si se establece en 0, las aplicaciones de la conexión se mostrarán directamente en el escritorio.
`root/ConnectionType/xen/connections/<UUID>/appOnDashboard`	Si se establece en 1, todas las aplicaciones de la conexión se mostrarán en la barra de tareas.
`root/ConnectionType/xen/connections/<UUID>/appOnDesktop`	Si se establece en 1, todas las aplicaciones de la conexión se mostrarán en el escritorio.
`root/ConnectionType/xen/connections/<UUID>/authorizations/user/edit`	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones para esta conexión.

Tabla E-14 Claves de registro de ConnectionType/xen (continúa)

Clave de registro	Descripción
root/ConnectionType/xen/connections/<UUID>/authorizations/user/execution	Si se establece en 1, un usuario final tiene permiso para ejecutar esta conexión.
root/ConnectionType/xen/connections/<UUID>/autoLaunchSingleApp	Si se establece en 1 y el servidor de Citrix sólo devuelve una única aplicación publicada o un solo escritorio, ese recurso se iniciará automáticamente.
root/ConnectionType/xen/connections/<UUID>/autoReconnect	Si se establece en 1, la conexión se reiniciará cuando se cierre o desconecte.
root/ConnectionType/xen/connections/<UUID>/autoReconnectAppsOnLogin	Si se establece en 1, el sistema intentará reconectar cualquier sesión Citrix activa o desconectada después del inicio de sesión original.
root/ConnectionType/xen/connections/<UUID>/autoReconnectDelay	Establece la cantidad de tiempo en segundos que se deben esperar antes de volver a conectar la sesión. El valor predeterminado 0 hará que la conexión se reactive inmediatamente. Esta configuración solo surte efecto cuando autoReconnect se establece en 1.
root/ConnectionType/xen/connections/<UUID>/autoRefreshInterval	Controla la cantidad de tiempo en segundos antes de que se borren y se vuelvan a actualizar los recursos del servidor. Establezca en -1 para desactivarlo. Normalmente no se requiere para actualizar con frecuencia los recursos del servidor.
root/ConnectionType/xen/connections/<UUID>/autoStartDesktop	Si se establece en 1 y autoStartResource está vacío, se iniciará automáticamente el primer escritorio que esté disponible cuando se inicia la conexión.
root/ConnectionType/xen/connections/<UUID>/autoStartResource	Establece el nombre del escritorio o la aplicación que se iniciará automáticamente cuando se inicia la conexión.
root/ConnectionType/xen/connections/<UUID>/autoStartWithGuessing	Si se establece en 1, la conexión trata de iniciar primero autoStartDesktop o autoStartResource. Si no se puede abrir la conexión correctamente, trata de abrir otro recurso mediante conjeturas.
root/ConnectionType/xen/connections/<UUID>/autostart	Si se establece en un valor de 1 a 5, la conexión se iniciará automáticamente después de que arranque el sistema, con el valor de 1 con la prioridad más alta.
root/ConnectionType/xen/connections/<UUID>/autostartDelay	Reservado para uso futuro.
root/ConnectionType/xen/connections/<UUID>/beforeStartingCommand	Establece que se ejecute el comando antes de que empiece la conexión.
root/ConnectionType/xen/connections/<UUID>/connectionMode	Establece el modo de conexión Citrix para la conexión.
root/ConnectionType/xen/connections/<UUID>/connectionStopAction	Define la acción que se realizará cuando termine la conexión de Connection Manager. Las opciones disponibles son disconnect y logoff.
root/ConnectionType/xen/connections/<UUID>/continueWithNewPassword	Si se establece en 1, después de restablecer la contraseña, la conexión se sigue abriendo con la nueva contraseña. Si se establece en 0, después de restablecer la contraseña, se cierra la conexión actual.
root/ConnectionType/xen/connections/<UUID>/coord	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.

Tabla E-14 Claves de registro de ConnectionType/xen (continúa)

Clave de registro	Descripción
root/ConnectionType/xen/connections/<UUID</credentialsType	Especifica el tipo de credencial entre `anonymous` (acceso no autenticado), `sso` (inicio de sesión único), `startup` (las credenciales se solicitan en el inicio), `password` (contraseña/dominio/usuario preconfigurados) o `smartcard` (smart card preconfigurada).
root/ConnectionType/xen/connections/<UUID>/dependConnectionId	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xen/connections/<UUID>/domain	Establece el dominio que se va a proporcionar al servidor XenDesktop. Si no hay ningún dominio especificado, se utiliza el dominio predeterminado para el servidor.
root/ConnectionType/xen/connections/<UUID>/enableRSAToken	**PRECAUCIÓN:** Esta funcionalidad no es compatible. Si se establece en 1, antes de conectarse, se le pedirá al usuario un valor de token de seguridad que se utilizará cuando se autentique con NetScaler Gateway.
root/ConnectionType/xen/connections/<UUID>/extraEnvValues/<UUID>/key	Establece el nombre de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/xen/connections/<UUID>/extraEnvValues/<UUID>/value	Establece el valor de una variable de entorno adicional para su uso con la conexión.
root/ConnectionType/xen/connections/<UUID>/fallBackConnection	Establece la conexión alternativa a través de su UUID.
root/ConnectionType/xen/connections/<UUID>/folder	
root/ConnectionType/xen/connections/<UUID>/forceHttps	Si se establece en 1, solo se permiten las conexiones HTTPS.
root/ConnectionType/xen/connections/<UUID>/fullscreen	Si se establece en 1, el cliente Citrix se abre en modo de pantalla completa cuando se inicia.
root/ConnectionType/xen/connections/<UUID>/hasDesktopIcon	Si se establece en 1, se activa el icono del escritorio para esta conexión. Esta tecla no tiene efecto en Smart Zero.
root/ConnectionType/xen/connections/<UUID>/iconPosition	Establece las coordinadas x,y de un icono de escritorio fijo. Si no se especifica, el icono queda flotante.
root/ConnectionType/xen/connections/<UUID>/ignoreCertCheck	Si se establece en 1, se ignoran las verificaciones del certificado para la conexión.
root/ConnectionType/xen/connections/<UUID>/label	Establece el nombre de conexión que se muestra en la interfaz de usuario. En Smart Zero, por lo general esta opción se establece en `Default Connection` y no aparece en la interfaz de usuario.
root/ConnectionType/xen/connections/<UUID>/logOnMethod	
root/ConnectionType/xen/connections/<UUID>/loginfields/domain	Si se establece en 1, el campo **Dominio** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el campo se muestra pero desactivado. Si se establece en 0, el campo queda oculto.

Tabla E-14 Claves de registro de ConnectionType/xen (continúa)

Clave de registro	Descripción
root/ConnectionType/xen/connections/<UUID>/loginfields/password	Si se establece en 1, el campo **Contraseña** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el campo se muestra pero desactivado. Si se establece en 0, el campo queda oculto.
root/ConnectionType/xen/connections/<UUID>/loginfields/rememberme	Si se establece en 1, la casilla de verificación **Recordarme** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, la casilla de verificación aparece pero deshabilitada. Si se establece en 0, la casilla de verificación está oculta.
root/ConnectionType/xen/connections/<UUID>/loginfields/server	Si se establece en 1, el cuadro **Servidor** aparece en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el cuadro aparece pero deshabilitado. Si se establece en 0, el cuadro queda oculto. Si se establece en 3, se usan los ajustes del sistema.
root/ConnectionType/xen/connections/<UUID>/loginfields/showpassword	Si se establece en 1, el botón **Mostrar contraseña** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el botón se muestra pero deshabilitado. Si se establece en 0, el botón queda oculto.
root/ConnectionType/xen/connections/<UUID>/loginfields/smartcard	Si se establece en 1, la casilla de verificación **Inicio de sesión con smart card** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, la casilla de verificación aparece pero deshabilitada. Si se establece en 0, la casilla de verificación está oculta. Es posible que esta casilla de verificación no aparezca si no se detecta ninguna smart card, incluso si esta opción está habilitada.
root/ConnectionType/xen/connections/<UUID>/loginfields/username	Si se establece en 1, el campo **Nombre de usuario** se muestra en el cuadro de diálogo de inicio de sesión de la conexión. Si se establece en 2, el campo se muestra pero desactivado. Si se establece en 0, el campo queda oculto.
root/ConnectionType/xen/connections/<UUID>/password	Establece la contraseña predeterminada que se suministra al host remoto durante el inicio de sesión. Este valor se encriptará. Por lo general, este ajuste se utiliza con las aplicaciones de estilo quiosco donde se usa una contraseña genérica para el inicio de sesión.
root/ConnectionType/xen/connections/<UUID>/resListRequest	Si se establece en 1, una conexión solo enumera los recursos sin iniciarlos o descargar los iconos.
root/ConnectionType/xen/connections/<UUID>/saveNewUrl	Este es un valor interno. Si se establece en `ToBeAsked`, el script hace la solicitud al usuario. Si se establece en `Auto`, el script no hace la solicitud al usuario y la URL se guarda según el caso. Si se establece en `Yes`, se pide al usuario que guarde la nueva URL. Si se establece en `No`, se pide al usuario que no guarde la nueva URL.
root/ConnectionType/xen/connections/<UUID>/savePassword	
root/ConnectionType/xen/connections/<UUID>/smartCardModuleKey	Especifica el módulo de seguridad que se va a utilizar para una conexión de smart card.
root/ConnectionType/xen/connections/<UUID>/startMode	Si se ajusta en el valor predeterminado `focus` (concentrar) y la conexión se ha iniciado, la conexión se concentrará. De lo contrario, aparecerá un error que indica que la conexión ya se ha iniciado.
root/ConnectionType/xen/connections/<UUID>/subscribedOnly	Si se establece en 1, solo se muestran los recursos suscritos para la conexión.

Tabla E-14 Claves de registro de ConnectionType/xen (continúa)

Clave de registro	Descripción
root/ConnectionType/xen/connections/<UUID>/unplugSmartCardAction	Establece la acción que se realizará cuando una smart card se desconecta durante la conexión. disconnect desconectará la sesión actual. close cerrará todos los recursos abiertos. noaction no hará nada.
root/ConnectionType/xen/connections/<UUID>/useCurrentCitrixConfig	
root/ConnectionType/xen/connections/<UUID>/username	Establece el nombre de usuario predeterminado que se suministra al host remoto durante el inicio de sesión. Por lo general, esta configuración se utiliza con las aplicaciones al estilo quiosco donde se usa un nombre de usuario genérico para el inicio de sesión.
root/ConnectionType/xen/connections/<UUID>/waitForNetwork	Si se establece en 1, la conexión no se iniciará hasta que la red esté disponible. Esto garantiza que, en una red lenta, la conexión no se inicie antes de que la red esté disponible, lo que podría provocar una falla.
root/ConnectionType/xen/coreSettings/USBrelevant	Especifica si este tipo de conexión es relevante para el USB. Si es así, puede tener un complemento USB para redirigir dispositivos USB.
root/ConnectionType/xen/coreSettings/appName	Establece el nombre de la aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/xen/coreSettings/autoLogoutDelayAfterLaunch	Esta configuración se aplica a los servidores Citrix con varios recursos publicados. Si se establece en menos de 0, no se realiza el cierre de sesión automático. De lo contrario, esta opción especifica el número de segundos entre el cierre del último recurso Xen publicado y el momento en que se saca al usuario de la sesión automáticamente y se devuelve a la pantalla de inicio de sesión original. Los retrasos de procesamiento de Citrix podrían aumentar el tiempo de cierre de sesión automático.
root/ConnectionType/xen/coreSettings/autoLogoutDelayBeforeLaunch	Esta configuración se aplica a los servidores Citrix con varios recursos publicados. Si se establece en menos de 0, no se realiza el cierre de sesión automático. De lo contrario, esta configuración establece el número de segundos que se permiten mientras no se inicia ninguna aplicación, antes de sacar automáticamente al usuario y devolverlo a la pantalla de inicio de sesión original. Los retrasos de procesamiento de Citrix podrían aumentar el tiempo de cierre de sesión automático.
root/ConnectionType/xen/coreSettings/className	Establece el nombre de la clase de aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/xen/coreSettings/connectionUtil	Establece la utilidad de la conexión Citrix para la conexión.
root/ConnectionType/xen/coreSettings/credsCache	Especifica si el Administrador de conexión almacena en caché las credenciales para un mayor uso.
root/ConnectionType/xen/coreSettings/editor	Establece el nombre de la aplicación interna que se utiliza cuando se inicia el Administrador de conexión para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/xen/coreSettings/generalSettingsEditor	Establece el nombre de la aplicación interna que se utiliza cuando se inicia el Administrador de ajustes generales para este tipo de conexión. No debería ser necesario modificar esta clave.

Tabla E-14 Claves de registro de ConnectionType/xen (continúa)

Clave de registro	Descripción
root/ConnectionType/xen/coreSettings/icon	Especifica el icono del conjunto de temas de iconos que se pueden usar con esta conexión.
root/ConnectionType/xen/coreSettings/icon16Path	Establece la ruta al icono de 16 x 16 píxeles para esta aplicación.
root/ConnectionType/xen/coreSettings/icon32Path	Establece la ruta al icono de 32 x 32 píxeles para esta aplicación.
root/ConnectionType/xen/coreSettings/icon48Path	Establece la ruta al icono de 48 x 48 píxeles para esta aplicación.
root/ConnectionType/xen/coreSettings/iconActive	Reservado para uso futuro.
root/ConnectionType/xen/coreSettings/label	Establece el nombre que se va a mostrar para este tipo de conexión en la interfaz de usuario.
root/ConnectionType/xen/coreSettings/priorityInConnectionLists	Establece la prioridad de este tipo de conexión cuando se muestra en el Administrador de conexión y en el Asistente de configuración que aparece durante la configuración inicial. Un valor superior moverá el tipo de conexión hacia la parte superior de la lista. Si se establece en 0, el tipo de conexión está oculto desde el Asistente de configuración y aparece de último en el Administrador de conexión. Los tipos de conexiones con la misma prioridad se enumeran en orden alfabético.
root/ConnectionType/xen/coreSettings/retryTimeout	Esta configuración se aplica cuando una máquina virtual se reinicia y aún no está disponible para iniciar como un recurso de Citrix. Si se establece en un número negativo, no intenta reconectarse. De lo contrario, brinda el tiempo (en segundos) que HP ThinPro trata de reconectarse a la máquina virtual.
root/ConnectionType/xen/coreSettings/serverRequired	Establece si un nombre o dirección de servidor es `unused`, `optional` o `required` para este tipo de conexión.
root/ConnectionType/xen/coreSettings/stopProcess	Establece el comportamiento que debería ocurrir cuando se llama `connection-mgr stop` en esta conexión. De forma predeterminada, está opción es `close`, lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como `kill`, el proceso especificado por `appName` se interrumpirá de forma forzada. Cuando se establece como `custom` se ejecutará una línea de comandos de ejecución personalizada especificada por `wrapperScript` con el argumento `stop` para finalizar el proceso correctamente.
root/ConnectionType/xen/coreSettings/tier	Especifica la importancia relativa de este tipo de conexión y el orden en el que se enumera en el menú Crear.
root/ConnectionType/xen/coreSettings/watchPid	Si se establece en 1, la conexión se supervisa bajo el nombre especificado por `appName`. No debería ser necesario modificar esta clave.
root/ConnectionType/xen/coreSettings/wrapperScript	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Este es el script principal que administra todos los ajustes de conexión y argumentos de línea de comandos para la conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/xen/coreSettings/wrapperScriptGeneration	Permite que el Administrador de conexiones sepa qué tipo de parámetros aprueban el script.

Tabla E-14 Claves de registro de ConnectionType/xen (continúa)

Clave de registro	Descripción
root/ConnectionType/xen/general/CGPAddress	Especifica la dirección de CGP mediante la sintaxis hostname:port. Como opción, en vez de especificar el nombre de host, puede escribir un asterisco (*). Esto usará el valor de la clave de registro address de la conexión como host. Por ejemplo: *:2598 El valor del puerto es opcional. Si no especifica un valor de puerto, se usa el valor predeterminado que es 2598. Si falla la conexión en el puerto 2598, el thin client trata de establecer una conexión en el puerto 1494.
root/ConnectionType/xen/general/TWIMode	Controla de forma impecable el modo para las aplicaciones publicadas. Esta configuración se asigna directamente en la configuración del archivo .ini de Citrix TWIMode.
root/ConnectionType/xen/general/ TWIModeResizeType	Esta configuración se asigna directamente a la configuración del archivo .ini de Citrix TWIMoveResizeType.
root/ConnectionType/xen/general/ allowReadOnA ... allowReadOnZ	Si se establece en 1, un usuario puede leer la unidad asignada.
root/ConnectionType/xen/general/ allowWriteOnA ... allowWriteOnZ	Si se establece en 1, un usuario puede grabar en la unidad asignada.
root/ConnectionType/xen/general/async	Si se establece en 1, se activa el agrupamiento asíncrono. Esta configuración se asigna directamente a la configuración del archivo .ini de Citrix CommPollSize.
root/ConnectionType/xen/general/ autoReconnect	Si se establece en 1, se activa la reconexión automática de la sesión. Esto no es lo mismo que la opción autoReconnect específica de la conexión. Ocurre internamente en el cliente Citrix sin reiniciar la conexión. Esta configuración se asigna directamente a la configuración del archivo .ini de Citrix TransportReconnectEnabled.
root/ConnectionType/xen/general/ bitmapCacheSize	Establece el tamaño mínimo del cacheo de mapa de bits. Esta configuración se asigna directamente a la configuración del archivo .ini de Citrix PersistentCacheMinBitmap.
root/ConnectionType/xen/general/ bottomMonitor	Establece el área de la pantalla del monitor inferior para mostrar el escritorio virtual. Si se establece en 0, el monitor no se usará para mostrar el escritorio virtual.
root/ConnectionType/xen/general/colorDepth	Impone una profundidad de color específica para todas las conexiones. Esto se suele hacer solo en entornos especializados donde falla la selección automática de la profundidad o en redes muy lentas para reducir la congestión.
root/ConnectionType/xen/general/colorMapping	Si se establece en Shared - Approximate Colors, se usan colores aproximados del mapa de colores predeterminado. Si se establece en Private - Exact Colors, se utilizan colores precisos. Esta configuración se asigna directamente a la configuración del archivo .ini de Citrix ApproximateColors.
root/ConnectionType/xen/general/ contentRedirection	Si se establece en 1, se envían enlaces del contenido web del servidor al cliente para que éste pueda tratar de abrirlos localmente.
root/ConnectionType/xen/general/ debugLogLevel	Si se establece en 0, no se crea un registro de depuración. Si se establece en 3, se crea un registro de nivel de error. Si se establece en 4, se crea un registro de nivel de advertencia.

Tabla E-14 Claves de registro de ConnectionType/xen (continúa)

Clave de registro	Descripción
	Si se establece en 7, se crean todos los registros de nivel de depuración.
root/ConnectionType/xen/general/ defaultBrowserProtocol	Controla el protocolo utilizado para ubicar el host de la conexión. Si se especifica, se usa el valor predeterminado de la sección [WFClient] de wfclient.ini. Esta configuración se asigna directamente a la configuración del archivo .ini de Citrix BrowserProtocol.
root/ConnectionType/xen/general/ drivePathMappedOnA ... drivePathMappedOnZ	Establece el directorio filesystem local que se asigna al host remoto. Normalmente, se establece como /media para permitir que todas las unidades USB conectadas se asocien al host remoto a través de una sola letra de unidad.
root/ConnectionType/xen/general/ enableAlertSound	Si se establece en 1, se activan sonidos de alerta de Windows. Esta configuración se asigna indirectamente a la configuración de archivo .ini de Citrix DisableSound.
root/ConnectionType/xen/general/ enableClipboard	Si se establece en 1, se activa la redirección del portapapeles.
root/ConnectionType/xen/general/ enableConnectionBar	Si se establece en 1, se activa Citrix Desktop Viewer en la interfaz de usuario de la sesión. De forma predeterminada, esta configuración se establece en 0 (desactivada) en el lado del cliente porque este valor lo establece en el cliente el archivo de ICA para una sesión de escritorio.
root/ConnectionType/xen/general/ enableCursorColors	Si se establece en 1, se activan los cursores de colores. En algunos casos, si se establece en 0, podría corregirse la corrupción del cursor gráfico.
root/ConnectionType/xen/general/ enableDataCompression	Si se establece en 1, se activa la compresión de datos. Esta configuración se asigna directamente a la configuración del archivo .ini de Citrix Compress.
root/ConnectionType/xen/general/ enableDriveMapAndRedirect	Si se establece en 1, se activan la asignación y la redirección de dispositivos de almacenamiento USB.
root/ConnectionType/xen/general/ enableDriveMapping	Si se establece en 1, se pueden enviar los directorios del sistema de archivos local al host remoto a través de una unidad virtual. Normalmente, /media se asigna a Z para permitir que las unidades USB se reenvíen al host remoto. Si está activada la redirección a USB, esta configuración debe desactivarse para evitar conflictos de almacenamiento. Para poder asignase correctamente al host remoto en este modo, el dispositivo USB debe utilizar uno de los siguientes sistemas de archivos: FAT32, NTFS, ext2, ext3.
root/ConnectionType/xen/general/ enableDynamicDriveMapping	Si se establece en 1, se asignarán de forma dinámica dispositivos de almacenamiento USB en el servidor Citrix. Si se establece en 0, se desactiva la asignación dinámica de dispositivos de almacenamiento USB.
root/ConnectionType/xen/general/ enableH264Compression	Si se establece en 1, se activa la compresión H264. El códec H264 ofrece un mejor rendimiento que el códec JPEG para las aplicaciones de gráficos profesionales y llenas de recursos en las redes WAN.
root/ConnectionType/xen/general/ enableHDXFlashRedirection	**NOTA:** Este recurso solo se admite en la versión de 32 bits de HP ThinPro. Controla el comportamiento de Redireccionamiento de HDX Flash. Si se establece en Always, se usa Redireccionamiento de HDX Flash si es posible y no se avisa nada al usuario. Si se establece en

Tabla E-14 Claves de registro de ConnectionType/xen (continúa)

Clave de registro	Descripción
	Ask, se avisa al usuario. Si se establece en Never, se desactiva el recurso.
root/ConnectionType/xen/general/enableHDXFlashServerContentFetch	**NOTA:** Este recurso solo se admite en la versión de 32 bits de HP ThinPro. Controla el comportamiento de Recoger el contenido del lado del servidor HDX Flash. Si está desactivado, el cliente buscará el contenido.
root/ConnectionType/xen/general/enableHDXMediaStream	Si se establece en 1, se activa HDX MediaStream. Si se establece en 0, los archivos multimedia se reproducirán mediante transmisión estándar, pero es posible que la calidad no sea tan buena.
root/ConnectionType/xen/general/enableHWH264	Si se establece en 1 y también se establece en 1 enableH264Compression, se activa la compresión de hardware para H.264. Si se establece en 0, la compresión de H.264 se administrará por software.
root/ConnectionType/xen/general/enableMapOnA ... enableMapOnZ	Si se establece en 1, se puede asignar un directorio del sistema de archivos local a esta unidad en el host remoto. La clave de registro correspondiente drivePathMappedOn debe establecerse en un directorio local válido para que la asignación de unidades funcione correctamente.
root/ConnectionType/xen/general/enableMultiMedia	Si se establece en 1, se activa el multimedia. HDX Lync podría tener un conflicto cuando esta configuración está activada. Esta configuración se asigna directamente al multimedia en la sección de canales virtuales de las configuraciones del archivo Citrix .ini. Active esta configuración cuando HDX MediaStream está activada.
root/ConnectionType/xen/general/enableOffScreenSurface	Si se establece en 1, el servidor puede usar el formato X PixMap para dibujar fuera de la pantalla. Esto reduce el ancho de banda en los modos de color de 15 y 24 bits a expensas del tiempo del procesador y la memoria del servidor X. Esta configuración se asigna directamente a la configuración del archivo .ini de Citrix EnableOSS.
root/ConnectionType/xen/general/enableRC4128SHA	
root/ConnectionType/xen/general/enableRC4MD5	
root/ConnectionType/xen/general/enableSessionReliability	Si se establece en 1, se habilita la confiabilidad de la sesión de Citrix. La confiabilidad de la sesión cambia la forma en que las sesiones se reanudan después de perder una conexión de red. Consulte la documentación de Citrix para obtener más información acerca de la confiabilidad de la sesión.
root/ConnectionType/xen/general/enableSmallFrames	Si se establece en 1, se activan para H.264 actualizaciones rectangulares pequeñas que no son de H.264. También debe estar activado enableTextTracking para que esta opción tenga algún efecto.
root/ConnectionType/xen/general/enableSmartCard	Si se establece en 1, se activa el inicio de sesión de smart card.
root/ConnectionType/xen/general/enableTLSRSA	
root/ConnectionType/xen/general/enableTextTracking	Si se establece en 1, se habilitan superposiciones optimizadas sin pérdidas para H.264.

Tabla E-14 Claves de registro de ConnectionType/xen (continúa)

Clave de registro	Descripción
root/ConnectionType/xen/general/enableUSBRedirection	Si se establece en 1, se redirigirán los dispositivos de almacenamiento USB.
root/ConnectionType/xen/general/encryptionLevel	Establece el nivel de encriptación. Los protocolos de encriptación para todos los niveles se definen en la sección [EncryptionLevelSession] de module.ini. Esta configuración se asigna directamente a la configuración del archivo .ini de Citrix [EncryptionLevelSession].
root/ConnectionType/xen/general/fontSmoothingType	Establece el tipo de suavizado de fuentes.
root/ConnectionType/xen/general/hotKey<1thru15>Char	Establece la tecla de acceso rápido para envío a la sesión remota cuando se presionan la tecla o la combinación de teclas definidas en el correspondiente hotKeyShift.
root/ConnectionType/xen/general/hotKey<1thru15>Shift	Establece la tecla o la combinación de teclas que se usa para activar la tecla de acceso rápido definida en el correspondiente hotKeyChar.
root/ConnectionType/xen/general/httpAddresses/<UUID>/address	
root/ConnectionType/xen/general/keyPassthroughEscapeChar	Establece la tecla del teclado para desactivar el modo de teclado transparente. Esta configuración se asigna directamente a la configuración del archivo .ini de Citrix KeyPassthroughEscapeChar.
root/ConnectionType/xen/general/keyPassthroughEscapeShift	Establece la combinación de teclas del teclado para desactivar el modo de teclado transparente. Esta configuración se asigna directamente a la configuración del archivo .ini de Citrix KeyPassthroughEscapeShift.
root/ConnectionType/xen/general/keyboardMappingFile	Especifica un archivo de asignación de teclado para una sesión de Citrix. De forma predeterminada, el script de inicio selecciona un archivo de asignación de teclado basado en la disposición del teclado.
root/ConnectionType/xen/general/lastComPortNum	Establece el número de puertos seriales asignados. Si se establece en 0, se deshabilita la asignación del puerto serial.
root/ConnectionType/xen/general/leftMonitor	Establece el área de la pantalla del monitor izquierdo para mostrar el escritorio virtual. Si se establece en 0, el monitor no se usará para mostrar el escritorio virtual.
root/ConnectionType/xen/general/localTextEcho	Controla la reducción de latencia del teclado. Esta configuración se asigna indirectamente a la configuración del archivo .ini de Citrix ZLKeyboardMode.
root/ConnectionType/xen/general/monitorNetwork	Si se establece en Off, no se supervisa la conectividad de la red. Si se establece en Local network link status only, sólo se supervisa el estado del enlace de la red local. Si se establece en Server online status, se supervisan tanto el estado del enlace de la red como la conectividad del servidor.
root/ConnectionType/xen/general/mouseClickFeedback	Controla la reducción de latencia del mouse. Esta configuración se asigna indirectamente a la configuración del archivo .ini de Citrix ZLMouseMode.
root/ConnectionType/xen/general/mouseMiddleButtonPaste	Si se establece en 1, se activa la emulación de pegado del botón central del mouse para las sesiones de Windows. Esta

Tabla E-14 Claves de registro de ConnectionType/xen (continúa)

Clave de registro	Descripción
	configuración se asigna directamente a la configuración del archivo .ini de Citrix `MouseSendsControlV`.
`root/ConnectionType/xen/general/noInfoBox`	Si se establece en 1, el administrador de cliente (wfcmgr) no aparecerá cuando concluya una sesión de cliente. Esta configuración se asigna directamente a la configuración del archivo .ini de Citrix `PopupOnExit`.
`root/ConnectionType/xen/general/printerAutoCreation`	Si se establece en 0, se desactiva la asignación de la impresora. Si se establece en 1, las impresoras definidas localmente se asignarán a la conexión. Si se configura en 2, las impresoras USB se redirigen según la configuración de Administrador de USB.
`root/ConnectionType/xen/general/proxyAddress`	Establece la dirección proxy que se utilizará si se selecciona una configuración proxy manual a través de `proxyType`.
`root/ConnectionType/xen/general/proxyPassword`	Establece la contraseña proxy que se utilizará si se selecciona una configuración proxy manual a través de `proxyType`. Esta contraseña se encriptará utilizando la encriptación rc4.
`root/ConnectionType/xen/general/proxyPort`	Establece el puerto proxy que se utilizará si se selecciona una configuración proxy manual a través de `proxyType`.
`root/ConnectionType/xen/general/proxyType`	Establece el tipo de proxy que se utilizará para las conexiones XenDesktop. El valor `Use Browser settings` solo se admite si hay instalado un explorador local.
`root/ConnectionType/xen/general/proxyUser`	Establece el nombre de usuario proxy que se utilizará si se selecciona una configuración proxy manual a través de `proxyType`.
`root/ConnectionType/xen/general/rightMonitor`	Establece el área de la pantalla del monitor derecho para mostrar el escritorio virtual. Si se establece en 0, el monitor no se usará para mostrar el escritorio virtual.
`root/ConnectionType/xen/general/saveLogs`	Si se establece en 1, se guarda la información detallada de registro después de que termina la sesión. Esta información de registro se guardará en el siguiente directorio: `/tmp/debug/citrix/<date>/`
`root/ConnectionType/xen/general/selfservice/disableConfigMgr`	Si se establece en 1, las solicitudes de uso compartido de sesión se envían a otras sesiones de Citrix en la misma pantalla X. Esta configuración se asigna directamente a la configuración del archivo .ini de Citrix `EnableSessionSharingClient`.
`root/ConnectionType/xen/general/selfservice/disableConnectionCenter`	
`root/ConnectionType/xen/general/selfservice/enableKioskMode`	
`root/ConnectionType/xen/general/selfservice/sharedUserMode`	
`root/ConnectionType/xen/general/selfservice/showTaskBarInKioskMode`	
`root/ConnectionType/xen/general/serverCheckTimeout`	
`root/ConnectionType/xen/general/sessionReliabilityTTL`	Especifica el tiempo de espera de confiabilidad de la sesión en segundos. Esto configura el Session Reliability Time To Live (TTL).

Tabla E-14 Claves de registro de ConnectionType/xen (continúa)

Clave de registro	Descripción
root/ConnectionType/xen/general/showOnAllMonitors	Si se establece en 1, el escritorio virtual se mostrará en todos los monitores.
root/ConnectionType/xen/general/smartCardModuleMap/CoolKeyPK11	Especifica la ruta al módulo de seguridad de la smart card CoolKey PKCS #11.
root/ConnectionType/xen/general/smartCardModuleMap/GemaltoDotNet	Especifica la ruta al módulo de seguridad de la smart card Gemalto.NET.
root/ConnectionType/xen/general/sound	Establece la calidad del sonido. Esta configuración se asigna indirectamente a la configuración del archivo .ini de Citrix AudioBandwidthLimit.
root/ConnectionType/xen/general/speedScreen	
root/ConnectionType/xen/general/tcpAccel	
root/ConnectionType/xen/general/tcpAddresses/<UUID>/address	
root/ConnectionType/xen/general/topMonitor	Establece el área de la pantalla del monitor superior para mostrar el escritorio virtual. Si se establece en 0, el monitor no se usará para mostrar el escritorio virtual.
root/ConnectionType/xen/general/transparentKeyPassthrough	Controla cómo se administran ciertas combinaciones de teclas de Windows. Si se establece en Translated, las combinaciones de teclas se aplican al escritorio local. Si se establece Direct in full screen desktops only, las combinaciones de teclas se aplican a la sesión remota sólo cuando está en modo de pantalla completa. Si se establece en Direct, las combinaciones de teclas se aplican a la sesión remota siempre y cuando la ventana tenga enfoque. Esta configuración se asigna indirectamente a la configuración del archivo .ini de Citrix TransparentKeyPassthrough.
root/ConnectionType/xen/general/transportProtocol	Establece el protocolo de transporte. Si se establece como On (valor predeterminado), la conexión usa UDP y no usa TCP como alternativa en caso de falla. Si se establece como Off, la conexión usa TCP. Si se establece como Preferred, la conexión trata de usar primero UDP y luego usa TCP como alternativa si hay una falla.
root/ConnectionType/xen/general/twRedundantImageItems	Controla el número de áreas de la pantalla que se siguen en ThinWire para evitar dibujos redundantes de imágenes de mapa de bits. Un valor adecuado para las sesiones de 1024 x 768 es de 300.
root/ConnectionType/xen/general/useAlternateAddress	Si se establece en 1, se usa una dirección alternativa para las conexiones con firewall. Esta configuración se asigna directamente a la configuración del archivo .ini de Citrix UseAlternateAddress.
root/ConnectionType/xen/general/useBitmapCache	Si se establece en 1, se activa la caché de disco persistente. La caché de disco persistente almacena objetos gráficos comúnmente utilizados como mapas de bits en la unidad de disco duro del thin client. El uso de la caché de disco persistente aumenta el rendimiento en conexiones con bajo ancho de banda pero reduce la cantidad de espacio disponible en el disco del thin client. En el caso de thin clients en LAN de alta velocidad, el uso de la caché de disco persistente no es necesario. Esta configuración

Tabla E-14 Claves de registro de ConnectionType/xen (continúa)

Clave de registro	Descripción
	se asigna directamente a la configuración del archivo .ini de Citrix `PersistentCacheEnabled`.
`root/ConnectionType/xen/general/useEUKS`	Controla el uso de Extended Unicode Keyboard Support (EUKS) en servidores Windows. Si se establece en 0, no se usa EUKS. Si se establece en 1, EUKS se utiliza como recurso alternativo. Si se establece en 2, EUKS se utiliza cuando sea posible.
`root/ConnectionType/xen/general/useLocalIM`	Si esta configuración está activada, el método de entrada X local se utiliza para interpretar la entrada de teclado. Esto solo es compatible con idiomas europeos. Esta configuración se asigna directamente a la configuración del archivo .ini de Citrix `useLocalIME`.
`root/ConnectionType/xen/general/userAgent`	El cliente Citrix presentará la secuencia de esta clave y ayudará a los administradores a saber de dónde viene la solicitud de conexión.
`root/ConnectionType/xen/general/waitForNetwork`	Si se establece en 1, la conexión no se iniciará hasta que la red esté disponible. Esto garantiza que, en una red lenta, la conexión no se inicie antes de que la red esté disponible, lo que podría provocar una falla.
`root/ConnectionType/xen/general/webcamFramesPerSec`	Controla la variable `HDXWebCamFramesPerSec` en el archivo All_Regions.ini.
`root/ConnectionType/xen/general/webcamHeight`	Controla la variable `HDXWebCamHeight` en el archivo `All_Regions.ini`.
`root/ConnectionType/xen/general/webcamQuality`	Controla la variable `HDXWebCamQuality` en el archivo `All_Regions.ini`. Los valores válidos se varían entre el 1 y el 63.
`root/ConnectionType/xen/general/webcamSupport`	Si se establece en 0, la cámara web y el audio de la cámara web se deshabilitan. Si se establece en 1, la cámara web y el audio de la cámara web se habilitan, con compresión. Si se establece en 2, se habilita la redirección USB de la cámara web y el audio de la cámara web.
`root/ConnectionType/xen/general/webcamWidth`	Controla la variable `HDXWebCamWidth` en el archivo `All_Regions.ini`.
`root/ConnectionType/xen/general/windowHeight`	Establece la altura de la ventana en píxeles si `windowSize` se establece en `Fixed Size`.
`root/ConnectionType/xen/general/windowPercent`	Establece el tamaño de la ventana como un porcentaje si `windowSize` se establece en `Percentage of Screen Size`.
`root/ConnectionType/xen/general/windowSize`	Si se establece en `Default`, se utilizan las configuraciones del lado del servidor. Si se establece en `Full Screen`, la ventana se maximiza sin bordes en todas las pantallas disponibles. Si se establece en `Fixed Size`, se pueden utilizar las claves de registro `windowWidth` y `windowHeight` para especificar el tamaño de la ventana en píxeles. Si se establece en `Percentage of Screen Size`, puede utilizarse la clave `windowPercent` para especificar el tamaño de la ventana como un porcentaje. Para que `el Porcentaje de tamaño de la pantalla` tenga efecto, `enableForceDirectConnect` debe estar configurado en 1 y `TWIMode` debe establecerse en 0. Esta configuración funciona solo con XenApp y únicamente si el servidor permite conexiones directas. Esta configuración no funciona con XenDesktop.

Tabla E-14 Claves de registro de ConnectionType/xen (continúa)

Clave de registro	Descripción
root/ConnectionType/xen/general/windowWidth	Establece el ancho de la ventana en píxeles si windowSize se establece en Fixed Size.
root/ConnectionType/xen/gui/XenDesktopPanel/disabled	Si se establece en 1, el panel de Xen Desktop y su barra de tareas se desactivan. Esto suele utilizarse cuando autoStartResource o autoStartDesktop están activados.
root/ConnectionType/xen/gui/XenManager/name	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xen/gui/XenManager/status	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xen/gui/XenManager/title	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/xen/gui/XenManager/widgets/address	Controla el estado del widget **URL del servicio** en el Administrador de conexión Citrix. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/xen/gui/XenManager/widgets/appInMenu	Controla el estado del widget **Mostrar aplicaciones en la barra de tareas** en el Administrador de conexión Citrix. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/xen/gui/XenManager/widgets/appOnDesktop	Controla el estado del widget **Mostrar aplicaciones en el escritorio** en el Administrador de conexión Citrix. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/xen/gui/XenManager/widgets/autoReconnect	Controla el estado del widget **Reconexión automática** en el Administrador de conexión Citrix. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/xen/gui/XenManager/widgets/autoStartDesktop	Controla el estado del widget **Iniciar automáticamente el escritorio** en el Administrador de conexión Citrix. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/xen/gui/XenManager/widgets/autoStartResource	Controla el estado del widget **Iniciar recurso automáticamente** en el Administrador de conexión Citrix. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/ConnectionType/xen/gui/XenManager/widgets/autostart	Controla el estado del widget **Prioridad de inicio automático** en el Administrador de conexión Citrix. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget

Tabla E-14 Claves de registro de ConnectionType/xen (continúa)

Clave de registro	Descripción
	queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/ConnectionType/xen/gui/XenManager/widgets/domain`	Controla el estado del widget **Dominio** en el Administrador de conexión Citrix. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/ConnectionType/xen/gui/XenManager/widgets/fallBackConnection`	Controla el estado del widget **Conexión de Seguridad** en el Administrador de conexión Citrix. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/ConnectionType/xen/gui/XenManager/widgets/folder`	
`root/ConnectionType/xen/gui/XenManager/widgets/hasDesktopIcon`	Controla el estado del widget **Mostrar icono en escritorio** en el Administrador de conexión Citrix. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/ConnectionType/xen/gui/XenManager/widgets/label`	Controla el estado del widget **Nombre** en el Administrador de conexión Citrix. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/ConnectionType/xen/gui/XenManager/widgets/password`	Controla el estado del widget **Contraseña** en el Administrador de conexión Citrix. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/ConnectionType/xen/gui/XenManager/widgets/username`	Controla el estado del widget **Nombre de usuario** en el Administrador de conexión Citrix. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/ConnectionType/xen/gui/XenManager/widgets/waitForNetwork`	Controla el estado del widget **Esperando por red antes de conectar** en el Administrador de conexión Citrix. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/ConnectionType/xen/gui/fbpanel/autohide`	Si se establece como `true`, la barra de tareas se oculta automáticamente.
`root/ConnectionType/xen/gui/fbpanel/edge`	Establece la posición predeterminada de la barra de tareas cuando más de un escritorio o una aplicación publicados se encuentran disponibles.

Tabla E-14 **Claves de registro de ConnectionType/xen (continúa)**

Clave de registro	Descripción
root/ConnectionType/xen/gui/fbpanel/hidden	Si se establece en 1, la barra de tareas queda completamente oculta, pero solo si autoStartResource o autoStartDesktop están activados.

DHCP

Esta carpeta existe para admitir claves de registro temporales que se agregan cuando el sistema adquiere una asignación DHCP. No es necesaria ninguna modificación.

Dashboard

Claves de registro del panel.

NOTA: El panel es lo mismo que la barra de tareas.

Tabla E-15 **Claves de registro del panel**

Clave de registro	Descripción
root/Dashboard/GUI/Clock	Si se establece en 1, el reloj se muestra en la barra de tareas.
root/Dashboard/GUI/DomainUser	Si se establece en 1, el icono del usuario del dominio se muestra en la barra de tareas si el sistema está en modo de inicio de sesión del dominio.
root/Dashboard/GUI/PowerButton	Si se establece en 1, el botón de inicio/apagado se muestra en la barra de tareas.
root/Dashboard/GUI/Search	Si se establece en 1, el botón de Búsqueda se muestra en la barra de tareas.
root/Dashboard/GUI/SystemTray	Si se establece en 1, la bandeja del sistema se muestra en la barra de tareas.
root/Dashboard/GUI/TaskBar	Si se establece en 1, el área de aplicaciones se muestra en la barra de tareas.
root/Dashboard/General/AutoHide	Si se establece en 1, la barra de tareas se oculta automáticamente.
root/Dashboard/General/EnterLeaveTimeout	Establece la cantidad de tiempo en milisegundos antes de que la barra de tareas se oculte o muestre cuando AutoHide está activado.
root/Dashboard/General/IconSize	Establece el tamaño de los iconos de la barra de tareas. Si se establece en -1, el tamaño del icono se basa en el ancho de la barra de tareas.
root/Dashboard/General/Length	Establece la longitud de la barra de tareas.
root/Dashboard/General/LengthToScreenSide	Si se establece en 1, la longitud de la barra de tareas es fija e igual a la longitud de la parte lateral de la pantalla a la que está anclada.

Tabla E-15 Claves de registro del panel (continúa)

Clave de registro	Descripción
root/Dashboard/General/PanelDockSide	Establece el lado de la pantalla al que se acopla la barra de tareas.
root/Dashboard/General/SlidingTimeout	Establece la cantidad de tiempo en milisegundos que se requiere para que la barra de tareas oculte o muestre cuando AutoHide está activado.
root/Dashboard/General/Width	Establece el ancho de la barra de tareas. Si se establece en -1, el ancho se escala basado en la altura del monitor principal.

Imprivata

Claves de registro de Imprivata.

Tabla E-16 Claves de registro Imprivata

Clave de registro	Descripción
root/Imprivata/enableImprivata	Si se establece en 1, se habilitará Imprivata ProveID Embedded. De forma predeterminada es 0.
root/Imprivata/enableWMRightClickMenu	Si se establece en 1, el menú de clic con el botón derecho del Administrador de ventanas se activa. Esto resulta útil cuando el escritorio normal no está disponible. Los elementos del menú son ajustables de acuerdo con el Administrador de energía y la configuración del Centro de personalización.
root/Imprivata/enableWMShortcuts	Si se establece en 1, se activarán los accesos directos del Administrador de ventanas. De forma predeterminada, los accesos directos se desactivan para conservar el entorno del agente Imprivata.
root/Imprivata/ImprivataServer	URL del servidor Imprivata. Al establecer root/users/user/apps/hptc-imprivata-mgr/authorized en 1, el usuario actual podrá modificar la configuración de Imprivata.
root/Imprivata/USBr/Devices	Enumera algunos dispositivos USB con una regla de redirección predefinida, específica para las conexiones remotas iniciadas mediante el entorno Imprivata. Para cada dispositivo USB, la regla de redirección viene dada por el ajuste: forcedState. Requiere OneSign ProveID Embedded 6.2 con la capacidad de utilizar el conjunto de scripts del proveedor.
root/Imprivata/x11SessionFilter	Si enableImprivata es verdadero, /etc/X11/Xsession.d/19-imprivata-session-fork asume la sesión X. x11SessionFilter define que los archivos de la sesión X sean filtrados para exclusión de la lista de archivos de la sesión X. x11SessionFilter es una lista de archivos de sesión separados por punto y coma para excluirse. Los comodines son admitidos.
root/Imprivata/Imprivata.conf/Vdi/useVendorLaunchScript	Si se establecen en 1, los scripts de ayuda de HP se utilizan para iniciar una sesión de VDI. De lo contrario, se utilizan los scripts heredados y los scripts en desuso. Para que esta configuración tenga efecto, es necesario reiniciar la sesión X. Ajuste Imprivata.conf: use-vendor-launch-script
root/Imprivata/RdpHelper/rdpFileTemplate	Plantilla del archivo .rdp completado por la ayuda RDP con el campo "dirección completa".

Tabla E-16 Claves de registro Imprivata (continúa)

Clave de registro	Descripción
root/Imprivata/SysInfo/citrix-wfica-client	Ruta al cliente Citrix wfica.
root/Imprivata/SysInfo/device-model	La cadena devuelta por el comando hptc-hwsw-id --hw se utiliza de forma predeterminada. Establezca el valor para obtener una cadena más relevante.
root/Imprivata/SysInfo/logo	Ruta al logotipo de partner Imprivata.
root/Imprivata/SysInfo/persistent-data-folder	Ruta a una carpeta donde se pueden almacenar los componentes ProveID Embeded, por ejemplo: /writable/imprivata-sys-info-data o /writable/misc/imprivata-sys-info-data si el contenido de la carpeta necesita formar parte de un perfil.
root/Imprivata/SysInfo/primary-monitor	Si el monitor principal está vacío, será detectado automáticamente. Ajuste el valor para forzar un monitor específico, por ejemplo: DisplayPort-0.
root/Imprivata/SysInfo/rdp-client	Ruta al cliente Microsoft RDP.
root/Imprivata/SysInfo/rds-client	Ruta al cliente Microsoft RDS.
root/Imprivata/SysInfo/vmware-client	Ruta al cliente VMware Horizon View.
root/Imprivata/USBr/Devices/<class id>:<product id>/forcedState	Establece si este dispositivo es forzado a asignarse al host remoto de la siguiente forma: -1=Ignorar dispositivo; 0=No redirigir; 1=Usar valores predeterminados; 2=redirigir.
root/Imprivata/USBr/Devices/<class id>:<product id>/info	Información del dispositivo.
root/Imprivata/VmwareViewHelper/skipCrlRevocationCheck	Si se establece en 1, la conexión omitirá la verificación de lista de revocación de certificado para VMware Horizon Client 5.4 o posterior.

InputMethod

Clave de registro InputMethod.

Tabla E-17 Clave de registro InputMethod

Clave de registro	Descripción
root/InputMethod/enablelbus	

Red

Claves de registro de Red.

Tabla E-18 Claves de registro de Red

Clave de registro	Descripción
root/Network/ActiveDirectory/Domain	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.

Tabla E-18 Claves de registro de Red (continúa)

Clave de registro	Descripción
root/Network/ActiveDirectory/DynamicDNS	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/Network/ActiveDirectory/Enabled	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/Network/ActiveDirectory/Method	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/Network/ActiveDirectory/Password	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/Network/ActiveDirectory/Username	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/Network/DNSServers	Aquí se pueden especificar servidores DNS adicionales para la resolución del nombre de dominio. Los servidores especificados se utilizarán de forma adicional a los servidores recuperados por medio de DHCP. Se pueden especificar hasta tres direcciones IPv4 o IPv6, separadas por comas.
root/Network/DefaultHostnamePattern	Establece el patrón de nombre de host predeterminado que se utilizará al generar un nuevo nombre de host. Esto se usa si la clave de registro de `Hostname` y `/etc/hostname` están vacías. El patrón del nombre de host usa `%` como un delimitador. En el ejemplo `HPTC%MAC:%1-6`, `HPTC` sería el prefijo y luego vendrían los primeros seis caracteres de la dirección MAC del thin client. Por lo tanto, si la dirección MAC del thin client es `11:22:33:44:55:66`, el nombre de host generado sería `HPTC112233`. Si el patrón es `TC%MAC%`, el nombre de host generado sería `TC112233445566`. Si el patrón es `HP%MAC:7%`, el nombre de host generado sería `HP1122334`.
root/Network/EncryptWpaConfig	Si se establece en 1, la contraseña se encripta.
root/Network/FtpProxy	Establece la dirección proxy de FTP. HP recomienda usar el siguiente formato para este valor debido a que el prefijo http tiene una compatibilidad mejor: `http://ProxyServer:Port`
root/Network/Hostname	Establece el nombre de host del thin client.
root/Network/HttpProxy	Establece la dirección proxy de HTTP. HP recomienda utilizar el siguiente formato: `http://ProxyServer:Port`
root/Network/HttpsProxy	Establece la dirección proxy de HTTPS. HP recomienda usar el siguiente formato para este valor debido a que el prefijo http tiene una compatibilidad mejor: `http://ProxyServer:Port`
root/Network/IPSec/IPSecRules/<UUID>/DstAddr	Establece la dirección de destino de la regla IPSec.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethod	Establece el método de autenticación de la regla IPSec. `PSK` sirve para usar una clave compartida previamente y `Certificate` sirve para usar los archivos del certificado.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodCACert	Si el método de autenticación es `Certificate`, la ruta de archivo del certificado de CA se guarda en esta clave de registro.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodClientCert	Si el método de autenticación es `Certificate`, la ruta de archivo del certificado del cliente se guarda en esta clave de registro.

Tabla E-18 Claves de registro de Red (continúa)

Clave de registro	Descripción
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodPresharedKey	Si el método de autenticación es PSK, el valor clave compartido previamente se guarda en esta clave de registro.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodPrivateKey	Si el método de autenticación es Certificate, la ruta del archivo clave privado que corresponde al certificado del cliente se guarda en esta clave de registro.
root/Network/IPSec/IPSecRules/<UUID>/MMDHGroup	Establece el grupo Diffie-Hellman de la fase 1.
root/Network/IPSec/IPSecRules/<UUID>/MMEncryptionAlg	Establece el algoritmo de encriptación de la fase 1.
root/Network/IPSec/IPSecRules/<UUID>/MMIntegrityAlg	Establece el algoritmo de integridad de la fase 1.
root/Network/IPSec/IPSecRules/<UUID>/MMLifetimeMinutes	Establece la vida útil de la fase 1.
root/Network/IPSec/IPSecRules/<UUID>/QMAHEnable	Activa la fase 2 AH.
root/Network/IPSec/IPSecRules/<UUID>/QMAHIntegrityAlg	Establece el algoritmo de integridad de la fase 2 AH.
root/Network/IPSec/IPSecRules/<UUID>/QMESPEnable	Activa la fase 2 ESP.
root/Network/IPSec/IPSecRules/<UUID>/QMESPEncryptionAlg	Establece el algoritmo de encriptación de la fase 2 ESP.
root/Network/IPSec/IPSecRules/<UUID>/QMESPIntegrityAlg	Establece el algoritmo de integridad de la fase 2 ESP.
root/Network/IPSec/IPSecRules/<UUID>/QMLifetimeSeconds	Establece la vida útil de la fase 2.
root/Network/IPSec/IPSecRules/<UUID>/RuleDescription	Establece la descripción de la regla IPSec.
root/Network/IPSec/IPSecRules/<UUID>/RuleEnable	Si se establece en 1, se activa la regla.
root/Network/IPSec/IPSecRules/<UUID>/RuleName	Establece el nombre de la regla IPSec.
root/Network/IPSec/IPSecRules/<UUID>/SrcAddr	Establece la dirección de origen de la regla IPSec.
root/Network/IPSec/IPSecRules/<UUID>/TunnelDstAddr	Establece la dirección de destino del túnel de la regla IPSec.
root/Network/IPSec/IPSecRules/<UUID>/TunnelEnable	Activa el modo de túnel de la regla IPSec.

Tabla E-18 Claves de registro de Red (continúa)

Clave de registro	Descripción
root/Network/IPSec/IPSecRules/<UUID>/TunnelSrcAddr	Establece la dirección de origen de túnel de la regla IPSec.
root/Network/KeepPreviousDNS	Si se establece en 1, los servidores DNS configurados previamente y los dominios de búsqueda no generados por el Administrador de red se mantendrán en resolv.conf. Si se establece en 0, resolv.conf se sobrescribirá por completo.
root/Network/SearchDomains	Los dominios de búsqueda adicionales para la resolución de FQDN se pueden especificar aquí. Los dominios especificados se añadirán a las definiciones del servidor incompletas en un intento de generar un FQDN que pueda resolverse a través de DNS. Por ejemplo, un dominio de búsqueda de mydomain.com permitirá que el servidor de definición myserver resuelva adecuadamente myserver.mydomain.com, incluso si el servidor DNS no tiene myserver en sus tablas de resolución de nombre. Pueden especificarse hasta cinco dominios de búsqueda adicionales.
root/Network/VPN/AutoStart	Si se establece en 1, la VPN se inicia automáticamente cuando se inicia el sistema.
root/Network/VPN/PPTP/Domain	Establece el dominio de PPTP.
root/Network/VPN/PPTP/Gateway	Establece la gateway de PPTP.
root/Network/VPN/PPTP/Password	Establece la contraseña de usuario de PPTP.
root/Network/VPN/PPTP/Username	Establece el nombre de usuario de PPTP.
root/Network/VPN/Type	Establece el tipo de VPN.
root/Network/VPN/VPNC/DPDEndianess	Establece la "endianness" (extremidad) del número de secuencia de DPD (consulte rfc3706). 0: big endian; 1: little endian. Trate de alternar esto si la sesión se interrumpe de forma intermitente sin motivo aparente.
root/Network/VPN/VPNC/DPDInterval	Establece el intervalo de DPD (consulte rfc3706) en segundos.
root/Network/VPN/VPNC/DebugLevel	Establece el nivel de depuración en 0, 1, 2, 3 o 99. Esto genera muchos registros. Habilite esto solo cuando necesita solucionar un problema de VPN.
root/Network/VPN/VPNC/Domain	Establece el dominio de VPNC.
root/Network/VPN/VPNC/Gateway	Establece la gateway de VPNC.
root/Network/VPN/VPNC/Group	Establece el grupo de VPNC.
root/Network/VPN/VPNC/GroupPassword	Establece la contraseña de grupo de VPNC.
root/Network/VPN/VPNC/IKEDHGroup	Establece el grupo VPNC IKE Diffie-Hellman.
root/Network/VPN/VPNC/LocalUDPPort	Establece el puerto UDP local para que se utilice en VPNC. Si se establece en 0, se usará un puerto aleatorio. Este ajuste solo es válido cuando el modo transversal NAT (NATTMode) es cisco-udp.
root/Network/VPN/VPNC/NATTMode	Establece el modo transversal VPNC NAT.

Tabla E-18 Claves de registro de Red (continúa)

Clave de registro	Descripción
root/Network/VPN/VPNC/Password	Establece la contraseña de usuario de VPNC.
root/Network/VPN/VPNC/PerfectForwardSecrecy	Establece el grupo VPNC Diffie-Hellman para que se use en Perfect Forward Secrecy (PFS).
root/Network/VPN/VPNC/Security	Establece el nivel de seguridad de VPNC.
root/Network/VPN/VPNC/Username	Establece el nombre de usuario de VPNC.
root/Network/VisibleInSystray	Si se establece en 1, el icono de la red queda visible en la bandeja del sistema.
root/Network/Wired/DefaultGateway	Establece la puerta de acceso predeterminada que usará el dispositivo para comunicarse con Internet. Normalmente, esta es la dirección IP del enrutador. Este ajuste solo surte efecto cuando Method se establece en Static.
root/Network/Wired/EnableDefGatewayAsDNS	Si se establece en 1, la gateway predeterminada también será el servidor de nombres.
root/Network/Wired/EthernetSpeed	Establece la velocidad de enlace de la interfaz de red Ethernet principal. Automatic permite usar la velocidad de enlace disponible más rápida, que generalmente es de 1 Gbps o 100 Mbps/completa según el switch. La velocidad de enlace también se puede forzar a una velocidad única (100 Mbps o 10 Mbps) y al modo dúplex (Full o Half) para admitir conmutadores o concentradores que no realicen la negociación automática.
root/Network/Wired/IPAddress	Establece la dirección IPv4 del thin client. Esta configuración solo entra en efecto cuando el Method se establece en Static.
root/Network/Wired/IPv6Enable	Si se establece en 1, se activa IPv6.
root/Network/Wired/Interface	Establece la interfaz de Ethernet o NIC predeterminada.
root/Network/Wired/MTU	Establece la MTU. No importa si la dirección IP es estática o adquirida por DHCP.
root/Network/Wired/Method	Si se establece en Automatic, el thin client usará DHCP para intentar recuperar la configuración de red. Si se establece en Static, se utilizan los valores de las claves de registro de IPAddress, SubnetMask y DefaultGateway. HP no recomienda el uso de Static en un perfil genérico del cliente, ya que esto hará que todos los thin clients reciban la misma dirección IP.
root/Network/Wired/Profiles/<UUID>/AutoConnect	Si se establece en 1, se activa la conexión automática a la red.
root/Network/Wired/Profiles/<UUID>/EthernetSpeed	Establece la velocidad de enlace de la interfaz de red Ethernet principal. Automatic permite usar la velocidad de enlace disponible más rápida, que generalmente es de 1 Gbps o 100 Mbps/completa según el switch. La velocidad de enlace también se puede forzar a una velocidad única (100 Mbps o 10 Mbps) y al modo dúplex (Full o Half) para admitir switches o concentradores que no realicen la negociación automática.
root/Network/Wired/Profiles/<UUID>/IPv4/Address	Establece la dirección IPv4 del cliente. Esta configuración solo surte efecto si Method se establece en Static.

Tabla E-18 Claves de registro de Red (continúa)

Clave de registro	Descripción
root/Network/Wired/Profiles/<UUID>/IPv4/DefaultGateway	Establece la gateway predeterminada que usa el dispositivo para comunicarse con Internet. Normalmente, esta es la dirección IP del enrutador. Esta configuración solo surte efecto si Method se establece en Static.
root/Network/Wired/Profiles/<UUID>/IPv4/Enabled	Si se establece en 1, IPv4 se activa para este perfil.
root/Network/Wired/Profiles/<UUID>/IPv4/Method	Si se establece en Automatic, el cliente usa DHCP para intentar recuperar la configuración de red. Si se establece en Static, se utilizan los valores de las claves de registro de Address, SubnetMask y DefaultGateway. HP no recomienda el uso de Static en un perfil genérico del cliente, porque todos los clientes usarían la misma dirección IP.
root/Network/Wired/Profiles/<UUID>/IPv4/SubnetMask	Establece la máscara de subred del dispositivo, como 255.255.255.0 (para una subred de clase C estándar). Esta configuración solo surte efecto si Method se establece en Static.
root/Network/Wired/Profiles/<UUID>/IPv6/Address	Establece la dirección IPv6 del cliente. Esta configuración solo surte efecto si Method se establece en Static.
root/Network/Wired/Profiles/<UUID>/IPv6/DefaultGateway	Establece la gateway predeterminada que usa el dispositivo para comunicarse con Internet. Normalmente, esta es la dirección IP del enrutador. Esta configuración solo surte efecto si Method se establece en Static.
root/Network/Wired/Profiles/<UUID>/IPv6/Enabled	Si se establece en 1, se activa IPv6 para este perfil.
root/Network/Wired/Profiles/<UUID>/IPv6/Method	Si se establece en Automatic, el cliente usa DHCP para intentar recuperar la configuración de red. Si se establece en Static, se utilizan los valores de las claves de registro de Address, SubnetMask y DefaultGateway. HP no recomienda usar Static en un perfil de cliente genérico, porque todos los clientes usarían la misma dirección IP. Si se establece en Automático, el cliente utiliza DHCP para intentar recuperar la configuración de red. Si se establece en Static, se utilizan los valores de las claves de registro de Address, SubnetMask y DefaultGateway. HP no recomienda el uso de Static en un perfil genérico del cliente, porque todos los clientes usarían la misma dirección IP.
root/Network/Wired/Profiles/<UUID>/IPv6/SubnetMask	Establece la máscara de subred del dispositivo, que generalmente es la longitud del prefijo de IPv6. Esta configuración solo surte efecto si Method se establece en Static.
root/Network/Wired/Profiles/<UUID>/MTU	Establece la MTU. No importa si la dirección IP es estática o adquirida por DHCP.
root/Network/Wired/Profiles/<UUID>/Priority	Reservado para una red con cable.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/AnonyIdentity	Establece la identidad anónima para la autenticación PEAP.
root/Network/Wired/Profiles/<UUID>/EAPPEAP/CACert	Establece la ruta al archivo de certificado CA para la autenticación PEAP.

Tabla E-18 Claves de registro de Red (continúa)

Clave de registro	Descripción
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/InnerAuth	Establece el protocolo de autenticación interna PEAP.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/PEAPVer	Establece la versión de PEAP.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/Password	Establece la contraseña para la autenticación PEAP.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/Username	Establece el nombre de usuario de la autenticación PEAP.
root/Network/Wired/Profiles/<UUID>/Security/EAPTLS/CACert	Establece la ruta al archivo de certificado CA para la autenticación TLS.
root/Network/Wired/Profiles/<UUID>/Security/EAPTLS/Identity	Establece la identidad para la autenticación TLS.
root/Network/Wired/Profiles/<UUID>/EAPTLS/PrivateKey	Establece la ruta a un archivo de clave privada para la autenticación TLS.
root/Network/Wired/Profiles/<UUID>/Security/EAPTLS/PrivateKeyPassword	Establece la contraseña de un archivo de clave privada para la autenticación TLS.
root/Network/Wired/Profiles/<UUID>/EAPTLS/UserCert	Establece la ruta a un archivo de certificado de usuario para la autenticación TLS.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTLS/AnonyIdentity	Establece la identidad anónima para la autenticación TTLS.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTLS/CACert	Establece la ruta a un archivo de certificado CA para la autenticación TTLS.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTLS/InnerAuth	Establece el protocolo de autenticación interna TTLS.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTLS/Password	Establece la contraseña para la autenticación TTLS.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTLS/Username	Establece el nombre de usuario para la autenticación TTLS.
root/Network/Wired/Profiles/<UUID>/Security/Type	Establece el tipo de autenticación cableada.
root/Network/Wired/Profiles/<UUID>/WiredInterface	Establece la interfaz cableada para el perfil.
root/Network/Wired/Security/CACert	Establece la ruta al archivo de certificado de CA.
root/Network/Wired/Security/EnableMachineAuth	Si se establece en 1, se activa la autenticación por máquina de PEAP.
root/Network/Wired/Security/Identity	Establece la identidad o identidad anónima.

Tabla E-18 Claves de registro de Red (continúa)

Clave de registro	Descripción
root/Network/Wired/Security/InnerAuth	Establece el protocolo de autenticación interna PEAP.
root/Network/Wired/Security/InnerAuthTTLS	Establece el protocolo de autenticación interna TTLS.
root/Network/Wired/Security/MachineAuthName	Guarda el nombre de la cuenta de la máquina cuando se habilita la autenticación de la máquina.
root/Network/Wired/Security/MachineAuthPassword	Guarda la contraseña de la cuenta de la máquina cuando se habilita la autenticación de la máquina.
root/Network/Wired/Security/PEAPVersion	Establece la versión de PEAP.
root/Network/Wired/Security/Password	Establece la contraseña.
root/Network/Wired/Security/PrivateKey	Establece la ruta a un archivo de clave privada. Esto sólo se utiliza para la autenticación de TLS.
root/Network/Wired/Security/Type	Establece el tipo de autenticación 802.1x.
root/Network/Wired/Security/UserCert	Establece la ruta a un archivo de certificado de usuario. Esto sólo se utiliza para la autenticación de TLS.
root/Network/Wired/Security/Username	Establece el nombre de usuario.
root/Network/Wired/SubnetMask	Establece la máscara de subred del dispositivo, como 255.255.255.0 (para una subred de clase C estándar). Esta configuración solo entra en efecto cuando el `Method` se establece en `Static`.
root/Network/Wired/UseWiredProfiles	Si se establece en 1, la conexión cableada se configura en el modo de perfil, que puede conectarse a varias redes cableadas. Si se establece en 0, puede conectarse a una sola red cableada.
root/Network/WiredWirelessSwitch	Si se establece en 0, pueden conectarse de forma simultánea una red cableada y una inalámbrica. Si se establece en 1, la red cableada asume la prioridad sobre la red inalámbrica; es decir, si la red cableada no se puede conectar, se usa una red inalámbrica configurada.
root/Network/Wireless/DefaultGateway	Establece la puerta de acceso predeterminada que usará el dispositivo para comunicarse con Internet. Normalmente, esta es la dirección IP del enrutador. Esta configuración solo entra en efecto cuando el `Method` se establece en `Static`.
root/Network/Wireless/EnableDefGatewayAsDNS	Si se establece en 1, la gateway predeterminada también será el servidor de nombres.
root/Network/Wireless/EnableWireless	Si se establece en 1, se habilita la funcionalidad inalámbrica. Si se establece en 0, se deshabilita la funcionalidad inalámbrica.
root/Network/Wireless/IPAddress	Establece la dirección IPv4 del thin client. Esta configuración solo entra en efecto cuando el `Method` se establece en `Static`.
root/Network/Wireless/IPv6Enable	Si se establece en 1, se activa IPv6.
root/Network/Wireless/Interface	Establece la interfaz inalámbrica predeterminada o el adaptador de red inalámbrica.
root/Network/Wireless/Method	Si se establece en `Automatic`, el thin client usará DHCP para intentar recuperar la configuración de red. Si se establece en `Static`, se utilizan los valores de las claves de registro

Tabla E-18 Claves de registro de Red (continúa)

Clave de registro	Descripción
	de `IPAddress`, `SubnetMask` y `DefaultGateway`. HP no recomienda el uso de `Static` en un perfil genérico del cliente, ya que esto hará que todos los thin clients reciban la misma dirección IP.
`root/Network/Wireless/PowerEnable`	Si se establece en 1, se activa la administración de energía de la tarjeta de red inalámbrica.
`root/Network/Wireless/Profiles/<UUID>/AutoConnect`	Si se establece en 1, se activa la conexión automática a la SSID.
`root/Network/Wireless/Profiles/<UUID>/IPv4/Address`	Establece la dirección IPv4 del cliente. Esta configuración solo surte efecto si `Method` se establece en `Static`.
`root/Network/Wireless/Profiles/<UUID>/IPv4/DefaultGateway`	Establece la gateway predeterminada que usa el dispositivo para comunicarse con Internet. Normalmente, esta es la dirección IP del enrutador. Esta configuración solo surte efecto si `Method` se establece en `Static`.
`root/Network/Wireless/Profiles/<UUID>/IPv4/Enabled`	Si se establece en 1, IPv4 se activa para este perfil.
`root/Network/Wireless/Profiles/<UUID>/IPv4/Method`	Si se establece en `Automatic`, el cliente usa DHCP para recuperar la configuración de red. Si se establece en `Static`, se utilizan los valores de las claves de registro de `Address`, `SubnetMask` y `DefaultGateway`. HP no recomienda el uso de `Static` en un perfil genérico del cliente, porque todos los clientes usarían la misma dirección IP.
`root/Network/Wireless/Profiles/<UUID>/IPv4/SubnetMask`	Establece la máscara de subred del dispositivo, como 255.255.255.0 (para una subred de clase C estándar). Esta configuración solo surte efecto si `Method` se establece en `Static`.
`root/Network/Wireless/Profiles/<UUID>/IPv6/Address`	Establece la dirección IPv6 del cliente. Esta configuración solo surte efecto si `Method` se establece en `Static`.
`root/Network/Wireless/Profiles/<UUID>/IPv6/DefaultGateway`	Establece la gateway predeterminada que usa el dispositivo para comunicarse con Internet. Normalmente, esta es la dirección IP del enrutador. Esta configuración solo surte efecto si `Method` se establece en `Static`.
`root/Network/Wireless/Profiles/<UUID>/IPv6/Enabled`	Si se establece en 1, se activa IPv6 para este perfil.
`root/Network/Wireless/Profiles/<UUID>/IPv6/Method`	Si se establece en `Automatic`, el cliente usa DHCP para intentar recuperar la configuración de red. Si se establece en `Static`, se utilizan los valores de las claves de registro de `Address`, `SubnetMask` y `DefaultGateway`. HP no recomienda el uso de `Static` en un perfil genérico del cliente, porque todos los clientes usarían la misma dirección IP.
`root/Network/Wireless/Profiles/<UUID>/IPv6/SubnetMask`	Establece la máscara de subred del dispositivo, que generalmente es la longitud del prefijo de IPv6. Esta configuración solo surte efecto si `Method` se establece en `Static`.
`root/Network/Wireless/Profiles/<UUID>/PowerEnable`	Si se establece en 1, se activa la administración de energía de la tarjeta de red inalámbrica.

Tabla E-18 Claves de registro de Red (continúa)

Clave de registro	Descripción
root/Network/Wireless/Profiles/<UUID>/Priority	Define la prioridad de la red. En el caso de una red inalámbrica, un número mayor significa una prioridad más alta. Se prefiere la alta prioridad para una conexión a una red inalámbrica.
root/Network/Wireless/Profiles/<UUID>/SSID	Establece el punto de acceso inalámbrico que se usará a través del SSID.
root/Network/Wireless/Profiles/<UUID>/SSIDHidden	Especifica si el SSID del punto de acceso inalámbrico está oculto.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/AnonyIdentity	Establece la identidad anónima para la autenticación EAP-FAST.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/FastProvision	Establece la opción de aprovisionamiento para la autenticación EAP-FAST.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/PACFile	Establece la ruta al archivo PAC para la autenticación EAP-FAST.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/Password	Establece la contraseña para la autenticación EAP-FAST.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/Username	Establece el nombre de usuario para la autenticación EAP-FAST.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/AnonyIdentity	Establece la identidad anónima para la autenticación EAP PEAP.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/CACert	Establece la ruta al archivo de certificado CA para la autenticación EAP PEAP.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/InnerAuth	Establece el protocolo de autenticación interna PEAP.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/PEAPVer	Establece la versión de PEAP.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/Password	Establece la contraseña para la autenticación EAP PEAP.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/Username	Establece el nombre de usuario para la autenticación EAP PEAP.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/CACert	Establece la ruta al archivo de certificado CA para la autenticación TLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/Identity	Establece la identidad para la autenticación TLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/PrivateKey	Establece la ruta a un archivo de clave privada para la autenticación TLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/PrivateKeyPassword	Establece la contraseña de un archivo de clave privada para la autenticación TLS.

Tabla E-18 Claves de registro de Red (continúa)

Clave de registro	Descripción
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/UserCert	Establece la ruta a un archivo de certificado de usuario para la autenticación TLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTLS/AnonyIdentity	Establece la identidad anónima para la autenticación TTLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTLS/CACert	Establece la ruta a un archivo de certificado CA para la autenticación TTLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTLS/InnerAuth	Establece el protocolo de autenticación interna TTLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTLS/Password	Establece la contraseña para la autenticación TTLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTLS/Username	Establece el nombre de usuario para la autenticación TTLS.
root/Network/Wireless/Profiles/<UUID>/Security/PSK/HexdecimalMode	
root/Network/Wireless/Profiles/<UUID>/Security/PSK/PreSharedKey	Establece la contraseña para la autenticación PSK.
root/Network/Wireless/Profiles/<UUID>/Security/Type	Establece el tipo de autenticación inalámbrica.
root/Network/Wireless/Profiles/<UUID>/Security/WEP/AuthType	Establece el tipo de autenticación WEP.
root/Network/Wireless/Profiles/<UUID>/Security/WEP/Key	Establece la contraseña de WEP.
root/Network/Wireless/Profiles/<UUID>/Security/WEP/KeyIndex	Establece el índice de contraseñas de WEP.
root/Network/Wireless/Profiles/<UUID>/Security/WirelessBand	Especifica la selección del rango de frecuencia. Seleccione `Auto` para buscar todos los canales inalámbricos; seleccione `2.4GHz` para buscar solo los canales de 2,4 GHz; seleccione `5GHz` para buscar solo los canales de 5 GHz.
root/Network/Wireless/Profiles/<UUID>/Security/WirelessInterface	Establece la interfaz inalámbrica para el perfil.
root/Network/Wireless/Roaming/enableRoamingOptions	Si se establece en 1, las opciones de itinerancia inalámbrica son configurables.
root/Network/Wireless/Roaming/longScanInterval	Especifica la frecuencia, en segundos, con la que se busca un punto de acceso con señal más fuerte cuando la fuerza de la señal es superior al umbral de roaming. De forma predeterminada es 60.
root/Network/Wireless/Roaming/roamingNap	Especifica la frecuencia, en segundos, con la que la conexión entra en suspensión cuando cambia el estado de wpa_applicant. Esto ayuda a reducir la posibilidad de que eventos espurios de Wi-Fi interrumpan conexiones en vivo cuando hay roaming.

Tabla E-18 Claves de registro de Red (continúa)

Clave de registro	Descripción
root/Network/Wireless/Roaming/roamingThreshold	Establece la fuerza mínima de la señal, en dBm, permitida antes de irse a un punto de acceso más fuerte. Tome en cuenta que este valor es negativo.
root/Network/Wireless/Roaming/scanInterval	Establece la frecuencia, en segundos, para buscar un punto de acceso más fuerte cuando la fuerza de la señal es inferior al umbral de itinerancia.
root/Network/Wireless/SSID	Establece el punto de acceso inalámbrico que se usará a través de su SSID.
root/Network/Wireless/SSIDHidden	Especifica si el SSID del punto de acceso inalámbrico está oculto.
root/Network/Wireless/SSIDWhiteList	Especifica una lista de puntos de acceso inalámbrico autorizados. Si el valor de esta clave de registro no está vacío, sólo los SSID especificados en el valor se mostrarán en los resultados de la exploración del punto de acceso inalámbrico. Use un punto y coma para separar los SSID.
root/Network/Wireless/Security/CACert	Establece la ruta al archivo de certificado de CA.
root/Network/Wireless/Security/EAPFASTPAC	Establece la ruta al archivo PAC para la autenticación EAP-FAST.
root/Network/Wireless/Security/EAPFASTProvision	Establece la opción de aprovisionamiento para la autenticación EAP-FAST.
root/Network/Wireless/Security/Identity	Establece la identidad o identidad anónima.
root/Network/Wireless/Security/InnerAuth	Establece el protocolo de autenticación interna PEAP.
root/Network/Wireless/Security/InnerAuthTTLS	Establece el protocolo de autenticación interna TTLS.
root/Network/Wireless/Security/PEAPVersion	Establece la versión de PEAP.
root/Network/Wireless/Security/Password	Establece la contraseña.
root/Network/Wireless/Security/PrivateKey	Establece la ruta a un archivo de clave privada. Esto sólo se utiliza para la autenticación de TLS.
root/Network/Wireless/Security/Type	Establece el tipo de autenticación inalámbrica.
root/Network/Wireless/Security/UserCert	Establece la ruta a un archivo de certificado de usuario. Esto sólo se utiliza para la autenticación de TLS.
root/Network/Wireless/Security/Username	Establece el nombre de usuario.
root/Network/Wireless/Security/WEPAuth	Establece el tipo de autenticación WEP.
root/Network/Wireless/Security/WEPIndex	Establece el índice de contraseñas de WEP.
root/Network/Wireless/SubnetMask	Establece la máscara de subred del dispositivo, como 255.255.255.0 (para una subred de clase C estándar). Esta configuración solo entra en efecto cuando el `Method` se establece en `Static`.
root/Network/Wireless/UseWirelessProfiles	Si se establece en 1, la conexión inalámbrica se configura en el modo de perfil, que puede conectarse a varias redes inalámbricas.

Tabla E-18 Claves de registro de Red (continúa)

Clave de registro	Descripción
	Esto es útil para la computación móvil. Si se establece en 0, solo se puede conectar una red inalámbrica configurada.
root/Network/Wireless/WirelessBand	Especifica la selección del rango de frecuencia. Seleccione `Auto` para buscar todos los canales inalámbricos; seleccione `2.4GHz` para buscar solo los canales de 2,4 GHz; seleccione `5GHz` para buscar solo los canales de 5 GHz.
root/Network/Wireless/WpaDriver	Especifica el controlador utilizado por wpa_supplicant (`wext` de forma predeterminada). `nl80211` es el único otro controlador que se admite actualmente.
root/Network/Wireless/bcmwlCountryOverride	Sustituye el valor del país en el BIOS en caso de que el BIOS no tenga el valor necesario. El controlador bcmwl acepta la opción wl_country, que se recupera de valores del BIOS según sea necesario (actualmente solo se admite en Indonesia). Se requiere que reinicie el sistema para que los cambios entren en efecto.
root/Network/Wireless/ disableUserCreateWirelessProfile	Si se establece en 1, las cuentas de usuario no pueden crear perfiles inalámbricos desde la bandeja del sistema de conexiones inalámbricas.
root/Network/Wireless/ disableUserWirelessProfileTrayMenu	Si se establece en 1, el menú de conexiones inalámbricas del icono de la bandeja del sistema de conexiones inalámbricas se deshabilita para la cuenta del usuario.
root/Network/Wireless/ disableWirelessProfileTrayMenu	Si se establece en 1, se deshabilita el menú de conexiones inalámbricas del icono de la bandeja del sistema de conexiones inalámbricas.
root/Network/Wireless/ tryAutoWirelessIfUserFailed	Si se establece en 1, si un usuario trata de conectarse a una AP inalámbrica y no lo logra, el módulo inalámbrico trata de conectarse de forma inalámbrica usando todos los perfiles disponibles. Si se establece en 0, si un usuario trata de conectarse a una AP inalámbrica y no lo logra, el estado de la conexión inalámbrica se establece como desconectada. Esta es una función de seguridad.
root/Network/disableLeftClickMenu	Si se establece en 1, se desactiva el menú del botón izquierdo del icono de bandeja de sistema de red.
root/Network/disableRightClickMenu	Si se establece en 1, se desactiva el menú del botón derecho del icono de bandeja de sistema de red.
root/Network/enableVPNMenu	Si se establece en 1, se habilita el menú de VPN del clic izquierdo al que se puede acceder desde el icono de la barra de tareas de la red.
root/Network/userLock	Si se establece en 1 y el usuario ha modificado la configuración de red, se conserva la configuración de red al importar un perfil de cliente.
root/Network/userLockEngaged	Esta clave de registro se establece en 1 automáticamente después de que el usuario ha modificado la configuración de la red. Normalmente no necesita modificar esta configuración.

Alimentación

Claves de registro para configuraciones de energía.

Tabla E-19 Claves de registro de energía

Clave de registro	Descripción
root/Power/applet/VisibleInSystray	Si se establece en 1, aparece el icono de la batería en la bandeja del sistema.
root/Power/buttons/logout/authorized	Si se establece en 1, la función de cierre de sesión está disponible.
root/Power/buttons/power/authorized	Si se establece en 1, la función de energía está disponible.
root/Power/buttons/poweroff/authorized	Si se establece en 1, la función de apagado está disponible.
root/Power/buttons/reboot/authorized	Si se establece en 1, la función de reinicio está disponible.
root/Power/buttons/sleep/authorized	Si se establece en 1, la función de suspensión está disponible.
root/Power/currentPowerPlan	Esta clave de registro selecciona el plan de energía que se usa. Esto se establece de forma automática en la configuración predeterminada.
root/Power/default/AC/brightness	Establece el nivel del porcentaje de brillo predeterminado para el momento en que el thin client móvil está conectado.
root/Power/default/AC/cpuMode	Establece el modo de la CPU para un plan de energía mientras el equipo está conectado a la alimentación de CA. De manera predeterminada, este valor se establece en la opción de rendimiento.
root/Power/default/AC/lidAction	Establece la acción que ocurre cuando se cierra la tapa del equipo mientras éste está conectado a la alimentación de CA. De manera predeterminada, se establece en suspensión.
root/Power/default/AC/powerButtonAction	Establece la acción que ocurre cuando se presiona el botón de inicio/apagado mientras el equipo está conectado a la alimentación de CA. De manera predeterminada, este valor se establece en la opción de apagado.
root/Power/default/AC/sleep	Establece el valor (en minutos) que el equipo espera antes de entrar en estado de suspensión mientras el equipo está conectado a la alimentación de CA. De manera predeterminada, este valor se establece en 30. Si se establece en 0, el equipo nunca entra en el estado de suspensión.
root/Power/default/AC/standby	Establece el valor (en minutos) que el equipo espera antes de que la pantalla se apague mientras el equipo está conectado a la alimentación de CA. De manera predeterminada, este valor se establece en 15. Si se establece en 0, el equipo nunca entra en el modo de espera.
root/Power/default/AC/timeoutDim	Esta clave no está en uso en este momento.
root/Power/default/battery/brightness	Establece el nivel del porcentaje de brillo predeterminado para el momento en que el thin client móvil no está conectado.
root/Power/default/battery/cpuMode	Establece el modo de la CPU para un plan de energía mientras el equipo no está conectado a la alimentación de CA. De manera predeterminada, este valor se establece a pedido.
root/Power/default/battery/critical/criticalBatteryAction	Establece la acción a realizar cuando la batería alcanza un nivel crítico de carga, definido por criticalBatteryLevel.
root/Power/default/battery/critical/criticalBatteryLevel	Establece el umbral de porcentaje en el que se considera que la batería está en un nivel crítico de energía.

Tabla E-19 Claves de registro de energía (continúa)

Clave de registro	Descripción
root/Power/default/battery/lidAction	Establece la acción que ocurre cuando se cierra la tapa del equipo mientras éste no está conectado a la alimentación de CA. De manera predeterminada, se establece en suspensión.
root/Power/default/battery/low/brightness	Establece el nivel del porcentaje de brillo predeterminado para el momento en que se reduce la carga de la batería.
root/Power/default/battery/low/cpuMode	Establece el modo de CPU (rendimiento o a pedido).
root/Power/default/battery/low/lowBatteryLevel	Establece el porcentaje de carga restante en la batería en el que se considera que la batería está en un nivel bajo de energía.
root/Power/default/battery/low/sleep	Establece el valor (en minutos) que el equipo espera antes de entrar en estado de suspensión mientras el equipo no está conectado a la alimentación de CA. De manera predeterminada, este valor se establece en 30. Si se establece en 0, el equipo nunca entra en el estado de suspensión.
root/Power/default/battery/low/standby	Establece el valor (en minutos) que el equipo espera antes de que la pantalla se apague mientras el equipo no está conectado a la alimentación de CA. De manera predeterminada, este valor se establece en 15. Si se establece en 0, el equipo nunca entra en el modo de espera.
root/Power/default/battery/low/timeoutDim	Esta clave no está en uso en este momento.
root/Power/default/battery/powerButtonAction	Especifica qué hacer cuando se presiona el botón de inicio/apagado.
root/Power/default/battery/sleep	Establece cuántos minutos se debe esperar antes de entrar en el modo de suspensión. 0 = nunca.
root/Power/default/battery/standby	Establece cuántos minutos se debe esperar antes de apagar la pantalla. 0 = nunca.
root/Power/default/battery/timeoutDim	Esta clave no está en uso en este momento.

ScepMgr

Claves de registro de ScepMgr.

Tabla E-20 Claves de registro de ScepMgr

Clave de registro	Descripción
root/ScepMgr/General/AutoRenew/Enabled	Si se establece en 1, los certificados se renovarán automáticamente antes de que venzan.
root/ScepMgr/General/AutoRenew/TimeFrame	Establece la cantidad de días antes de la fecha de vencimiento de un certificado en que el administrador de SCEP intentará renovar el certificado automáticamente.
root/ScepMgr/IdentifyingInfo/CommonName	Establece el nombre común que se utilizará en la información de identificación de SCEP, como su nombre o el nombre de dominio completamente calificado (FQDN) del dispositivo. Si este valor se deja vacío, se utiliza el FDQN de forma predeterminada.

Tabla E-20 Claves de registro de ScepMgr (continúa)

Clave de registro	Descripción
root/ScepMgr/IdentifyingInfo/CountryName	Establece el país o la región que se utilizará en la información de identificación de SCEP.
root/ScepMgr/IdentifyingInfo/EmailAddress	Establece la dirección de correo electrónico que se utilizará en la información de identificación de SCEP.
root/ScepMgr/IdentifyingInfo/LocalityName	Establece el nombre de la localidad que se utilizará en la información de identificación de SCEP, como un nombre de ciudad.
root/ScepMgr/IdentifyingInfo/ OrganizationName	Establece el nombre de la organización que se utilizará en la información de identificación de SCEP, como el nombre de una compañía o el nombre de una organización gubernamental.
root/ScepMgr/IdentifyingInfo/ OrganizationUnitName	Establece el nombre de la unidad organizacional que se utilizará en la información de identificación de SCEP, como un nombre de sección o un nombre de departamento.
root/ScepMgr/IdentifyingInfo/StateName	Establece el estado o provincia que se utilizará en la información de identificación de SCEP.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/ CertFileChanged	La clave de registro se utiliza únicamente para informar a otras aplicaciones que se ha cambiado un archivo de certificado. No debería ser necesario modificar esto.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/ DontVerifyPeer	Esta clave de registro se usa solo para https. Si se establece en 1, el cliente SCEP no verificar el certificado del servidor. La clave se establece en 0 de forma predeterminada.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/ KeySize	Establece el tamaño de la clave que se utilizará en par de claves generadas.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/ ServerName	Establece el nombre del servidor de SCEP.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/ ServerUrl	Establece la URL del servidor de SCEP, que es necesaria para que el cliente de SCEP registre un certificado.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/ Status/Code	Contiene el código de estado de la inscripción de SCEP. Este valor es apenas para lectura.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/ Status/Detail	Contiene información detallada sobre la inscripción de SCEP. Este valor es apenas para lectura.

Buscar

Claves de registro de configuración de búsqueda.

Tabla E-21 Claves de registro de configuración de búsqueda

Clave de registro	Descripción
root/Search/Category/Miscellaneons/ CheckForUpdate	
root/Search/Category/Miscellaneons/Logout	

Tabla E-21 **Claves de registro de configuración de búsqueda (continúa)**

Clave de registro	Descripción
root/Search/Category/Miscellaneons/Reboot	
root/Search/Category/Miscellaneons/ShutDown	
root/Search/Category/Miscellaneons/Sleep	
root/Search/Category/Miscellaneons/SwitchToAdmin	
root/Search/Category/Regeditor/byDir	
root/Search/Category/Regeditor/byKey	
root/Search/Category/Regeditor/byValue	
root/Search/Category/Regeditor/byWhole	

Serial

Claves de registro de dispositivos seriales.

Tabla E-22 **Claves de registro de dispositivos seriales**

Clave de registro	Descripción
root/Serial/<UUID>/baud	Establece la velocidad del dispositivo serial.
root/Serial/<UUID>/dataBits	Establece la cantidad de bits de cada caracter.
root/Serial/<UUID>/device	Especifica el dispositivo serial conectado al sistema.
root/Serial/<UUID>/flow	Establece el control de flujo del dispositivo serial, que se usa para comunicar el inicio y la interrupción de la comunicación serial.
root/Serial/<UUID>/name	Especifica el puerto de dispositivo Windows usado para comunicarse con el dispositivo serial.
root/Serial/<UUID>/parity	Establece los bits de paridad del dispositivo serial. Los bits de paridad se utilizan para la detección de errores. Si se establece como none, no hay detección de paridad.

SystemInfo

Claves de registro de la información del sistema.

Tabla E-23 Claves de registro de la información del sistema

Clave de registro	Descripción
`root/SystemInfo/Pages/General`	Si se establece en 0, se oculta de los usuarios finales la ficha **General** de la ventana de información del sistema.
`root/SystemInfo/Pages/License`	Si se establece en 0, se oculta de los usuarios finales la ficha **Licencia de software** de la ventana de información del sistema.
`root/SystemInfo/Pages/NetTools`	Si se establece en 0, se oculta de los usuarios finales la ficha **Herramientas de red** de la ventana de información del sistema.
`root/SystemInfo/Pages/Network`	Si se establece en 0, se oculta de los usuarios finales la ficha **Red** de la ventana de información del sistema.
`root/SystemInfo/Pages/SoftwareInformationTab/ServicePacks`	Si se establece en 0, se oculta de los usuarios finales la ficha **Service Packs** en la sección de **Información del software** de la ventana de información del sistema.
`root/SystemInfo/Pages/SoftwareInformationTab/SoftwareInformation`	Si se establece en 0, se oculta de los usuarios finales la ficha **Información del software** de la ventana de información del sistema.
`root/SystemInfo/Pages/SoftwareInformationTab/SoftwareInstalled`	Si se establece en 0, se oculta de los usuarios finales la ficha **Software instalado** en la sección **Información del software** de la ventana de información del sistema.
`root/SystemInfo/Pages/SystemLogs`	Si se establece en 0, se oculta de los usuarios finales la ficha **Registros del sistema** de la ventana de información del sistema.
`root/SystemInfo/authorized`	Si se establece en 0, se desactiva el botón de información del sistema de la barra de tareas para los usuarios finales.

TaskMgr

Clave de registro del Administrador de tareas.

Tabla E-24 Clave de registro del Administrador de tareas

Clave de registro	Descripción
`root/TaskMgr/General/AlwaysOnTop`	Si se establece en 1, la ventana del Administrador de tareas siempre está en la parte superior.

USB

Claves de registro de USB.

Tabla E-25 Claves de registro de USB

Clave de registro	Descripción
`root/USB/Classes/<Defined at Interface level>/ClassID`	Establece el número de ID de clase USB.
`root/USB/Classes/<Defined at Interface level>/DisplayName`	Establece el nombre de clase USB.

Tabla E-25 Claves de registro de USB (continúa)

Clave de registro	Descripción
`root/USB/<Defined at Interface level>/Classes/State`	Establece si la clase está asignada al host remoto.
`root/USB/<Defined at Interface level>/Classes/Visible`	Establece si la clase se muestra en la interfaz de usuario o no, o si está desactivada.
`root/USB/Devices/<UUID>/DisplayName`	Establece el nombre que se muestra en el Administrador de USB. Si no se proporciona, el Administrador de USB intentará generar un nombre adecuado usando la información del dispositivo.
`root/USB/Devices/<UUID>/ProductID`	Establece la ID de producto del dispositivo.
`root/USB/Devices/<UUID>/State`	Establece si este dispositivo está asignado al host remoto de la siguiente forma: 0 = No redirigir; 1 = Usar valores predeterminados. 2 = Redirigir.
`root/USB/Devices/<UUID>/VendorID`	Establece el ID del proveedor del dispositivo.
`root/USB/root/autoSwitchProtocol`	Si se establece en 1, el protocolo USB remoto cambiará automáticamente según el protocolo elegido.
`root/USB/root/mass-storage/allowed`	Si se establece en 1, los dispositivos de almacenamiento masivo se montarán automáticamente cuando el protocolo sea `local`.
`root/USB/root/mass-storage/read-only`	Si se establece en 1, cuando los dispositivos de almacenamiento masivo se monten de forma automática, se montarán solo para lectura.
`root/USB/root/protocol`	Establece qué protocolo posee el USB remoto. Los valores válidos dependen de los protocolos que están instalados en el sistema, pero pueden incluir `local`, `xen`, `freerdp` y `view`.
`root/USB/root/showClasses`	Si se establece en 1, la sección **Clases** aparece en el Administrador de USB.

auto-update

Claves de registro de Actualizaciones automáticas.

Tabla E-26 Claves de registro de Actualizaciones automáticas

Clave de registro	Descripción
`root/auto-update/DNSAliasDir`	Establece el directorio raíz predeterminado para el modo de alias DNS en servidor que aloja HP Smart Client Services.
`root/auto-update/LockScreenTimeout`	Especifica el tiempo (en minutos) después del cual se desbloquea la pantalla durante una actualización automática. Si se establece en 0, la pantalla se desbloquea durante toda la actualización automática hasta que concluye.
`root/auto-update/ManualUpdate`	Si se establece en 1, se desactivan la etiqueta de DHCP, el alias DNS y los métodos de actualización de difusión para Actualización automática. Al realizar una actualización manual, las claves de registro `password`, `path`, `protocol`, `user` y `ServerURL` deben configurarse para asegurarse de que se conoce el servidor de actualización.

Tabla E-26 Claves de registro de Actualizaciones automáticas (continúa)

Clave de registro	Descripción
root/auto-update/ScheduledScan/Enabled	Si se establece en 1, el thin client realiza detecciones periódicas del servidor de actualización automática para buscar actualizaciones. Si se establece en 0, el thin client sólo buscará actualizaciones al iniciar el sistema.
root/auto-update/ScheduledScan/Interval	Establece la cantidad de tiempo de espera entre las detecciones de actualizaciones programadas. Esto se debe especificar en el formato HH: MM. se pueden especificar intervalos de más de 24 horas. Por ejemplo, para que ocurran las detecciones cada 48 horas, establezca esta opción en 48:00.
root/auto-update/ScheduledScan/Period	Los thin clients activarán de forma aleatoria sus detecciones programadas durante el período definido. El uso de un período prolongado evita casos donde todos los thin clients se actualizan exactamente al mismo tiempo, lo que podría causar una congestión en la red. El período debe especificarse en el formato HH: MM. Por ejemplo, para extender actualizaciones del thin client durante un periodo de 2,5 horas, establezca esta opción en 02:30.
root/auto-update/ScheduledScan/StartTime	Establece la hora de inicio de la primera detección de actualizaciones programadas en el formato HH:MM, con el formato de 24 horas. Por ejemplo, las 4:35 p.m. serían las 16:35.
root/auto-update/ServerURL	Establece el nombre de dominio o la dirección IP del servidor de actualización utilizado cuando se activa ManualUpdate.
root/auto-update/VisibleInSystray	Si se establece en 1, se activa el icono de la bandeja del sistema de Actualización automática.
root/auto-update/checkCertSig	Si se establece en 1, se verifica la firma del certificado.
root/auto-update/checkCustomSig	Si se establece en 1, se verifica la firma de los paquetes personalizados.
root/auto-update/checkImgSig	Reservado para uso futuro.
root/auto-update/checkPackageSig	Si se establece en 1, se verifica la firma de los paquetes.
root/auto-update/checkProfileSig	Si se establece en 1, se verifica la firma de los perfiles.
root/auto-update/enableLockScreen	Si se establece en 1, la pantalla se bloquea mientras la actualización automática está en curso.
root/auto-update/enableOnBootup	Si se establece en 1, se activa Actualización automática al iniciar el sistema.
root/auto-update/enableSystrayLeftClickMenu	Si se establece en 1, se activa el menú del botón izquierdo para el icono de la bandeja del sistema de Actualización automática.
root/auto-update/enableSystrayRightClickMenu	Si se establece en 1, se activa el menú del botón derecho para el icono de la bandeja del sistema de Actualización automática.
root/auto-update/gui/auto-update/ ManualUpdate	Controla el estado del widget **Habilitar la configuración manual** en la herramienta Actualización automática. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.
root/auto-update/gui/auto-update/ServerURL	Controla el estado del widget **Servidor** en la herramienta Actualización automática. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede

Tabla E-26 Claves de registro de Actualizaciones automáticas (continúa)

Clave de registro	Descripción
	interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/auto-update/gui/auto-update/enableLockScreen`	Controla el estado del widget **Habilitar el bloqueo de la pantalla cuando se use Actualización automática** en la herramienta Actualización automática. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/auto-update/gui/auto-update/enableOnBootup`	Controla el estado del widget **Habilitar Actualización automática al iniciarse el sistema** en la herramienta Actualización automática. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/auto-update/gui/auto-update/password`	Controla el estado del widget **Contraseña** en la herramienta Actualización automática. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/auto-update/gui/auto-update/protocol`	Controla el estado del widget **Protocolo** en la herramienta Actualización automática. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/auto-update/gui/auto-update/tag`	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
`root/auto-update/gui/auto-update/user`	Controla el estado del widget **Nombre de usuario** en la herramienta Actualización automática. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/auto-update/password`	Establece la contraseña utilizada cuando está activada `ManualUpdate`. Esto sólo se usa cuando se establece `protocol` en `ftp`. Este valor se encriptará.
`root/auto-update/path`	Establece la ruta relativa desde la URL del servidor predeterminado cuando se activa `ManualUpdate`. Normalmente, está vacía o está configurada para `actualización automática`.
`root/auto-update/preserveConfig`	Si se establece en 1, se conservará la configuración actual del thin client cuando ocurra una actualización de imagen a través de Actualización automática.
`root/auto-update/protocol`	Establece el protocolo que se utiliza cuando se activa `ManualUpdate`
`root/auto-update/tag`	Esta clave de registro es obsoleta. Establece previamente el número de etiqueta usado para DHCP (137). Esto se detecta ahora a través del nombre de la etiqueta `auto-update`.

Tabla E-26 **Claves de registro de Actualizaciones automáticas (continúa)**

Clave de registro	Descripción
root/auto-update/user	Establece el nombre de usuario utilizado cuando se activa ManualUpdate. Esto sólo se usa cuando se establece el 'protocol' en 'ftp'.

background

Claves de registro de Información del sistema en segundo plano.

Tabla E-27 **Claves de registro de Información del sistema en segundo plano**

Clave de registro	Descripción
root/background/bginfo/alignment	Establece la alineación del texto de Información del sistema en segundo plano.
root/background/bginfo/enabled	Si se establece en 1, la información del sistema aparece en el fondo del escritorio (Información del sistema en segundo plano).
root/background/bginfo/horizontalLocation	Establece la ubicación de Información del sistema en segundo plano en el eje X en un porcentaje.
root/background/bginfo/interval	Establece el intervalo de actualización del texto de Información del sistema en segundo plano en segundos.
root/background/bginfo/preset	Establece el archivo predefinido de Información del sistema en segundo plano en use. Si se establece en none, puede personalizar las configuraciones del Administrador de fondos.
root/background/bginfo/shadowColor	Establece el color de la sombra de Información del sistema en segundo plano.
root/background/bginfo/shadowOffset	Establece el intervalo de la sombra de Información del sistema en segundo plano. Si se establece en 0, se desactiva la sombra.
root/background/bginfo/text	Establece el texto de Información del sistema en segundo plano. Para obtener más información, consulte el informe técnico sobre HP ThinPro *"Login Screen Customization"* (disponible solo en inglés).
root/background/bginfo/textColor	Establece el color del texto de Información del sistema en segundo plano.
root/background/bginfo/textSize	Establece el tamaño del texto de Información del sistema en segundo plano.
root/background/bginfo/verticalLocation	Establece la ubicación de Información del sistema en segundo plano en el eje Y en un porcentaje.
root/background/desktop/color	Especifica el color fijo, el color del fondo si hay alguno visible detrás de la imagen, o el color principal en una gradiente.
root/background/desktop/color2	Si theme se establece como gradient, esta clave almacena el color inferior de la gradiente.
root/background/desktop/imagePath	Si theme se establece como none o image, esta clave almacena la ruta de imagen de fondo del escritorio utilizada por el tema definido por el usuario.
root/background/desktop/lastBrowseDir	Si se establece el theme en none, esta clave almacena el último directorio utilizado.

Tabla E-27 Claves de registro de Información del sistema en segundo plano (continúa)

Clave de registro	Descripción
root/background/desktop/style	Si se establece el theme en none, esta clave almacena la forma en que se coloca la imagen de fondo en el escritorio (por ejemplo center, tile, stretch, fit y fill).
root/background/desktop/theme	Especifica la configuración del tema del sistema. Este valor se establece mediante la herramienta Administrador de fondos en el Panel de control. Los valores válidos dependen de los temas que existan en el sistema. Esto puede establecerse como none o image para permitir que el usuario defina una imagen de fondo, como auto para que el sistema establezca de forma automática el tema del protocolo adecuado para Smart Zero, o como default para usar el tema predeterminado para ThinPro, o uno de los diversos temas predefinidos.
root/background/desktop/updateInterval	Establece el intervalo de actualización del fondo en segundos.

arrancar

Claves de registro de arranque.

Tabla E-28 Claves de registro de arranque

Clave de registro	Descripción
root/boot/enablePlymouth	
root/boot/extraCmdline	

config-wizard

Claves de registro del asistente de configuración

Tabla E-29 Claves de registro del asistente de configuración

Clave de registro	Descripción
root/config-wizard/configWizardOptions	Especifica, en una lista separada por espacios, cuáles opciones del asistente de configuración se muestran. De forma predeterminada, se enumeran todas las opciones (language, keyboard, network, datetime, end).
root/config-wizard/disableAllChecksAtStartup	Si se establece en 1, se deshabilitan todas las verificaciones en el inicio. Si se establece en 0, puede habilitar/deshabilitar cada tipo de verificación individualmente con las claves de registro enableConnectionCheck, enableNetworkCheck y enableUpdateCheck.
root/config-wizard/enableConfigWizard	Si se establece en 1, se activa el asistente de configuración al iniciar el sistema.
root/config-wizard/enableConnectionCheck	Si se establece en 1, se activa la verificación de la conexión al iniciar el sistema.

Tabla E-29 Claves de registro del asistente de configuración (continúa)

Clave de registro	Descripción
root/config-wizard/enableNetworkCheck	Si se establece en 1, se activa la verificación de la red al iniciar el sistema.
root/config-wizard/showNetworkSettingsButton	Si se establece en 1, el botón de configuraciones de la red se muestra en la ventana de verificación de la red.

desktop

Claves de registro del escritorio.

Tabla E-30 Claves de registro del escritorio

Clave de registro	Descripción
root/desktop/preferences/arrangeBy	Especifica si los iconos se organizan por nombre o por tipo.
root/desktop/preferences/fontFamily	Especifica la fuente usada para los iconos del escritorio.
root/desktop/preferences/gridSize	Especifica, en píxeles, el tamaño de cuadrícula del icono del escritorio. Si se establece en un valor inferior a 64, el tamaño se calcula como una proporción del tamaño del monitor.
root/desktop/preferences/iconGlowColor	Especifica el color que brilla detrás del icono del escritorio cuando un dispositivo señalador pasa sobre él. Las cadenas válidas tienen el estilo `QColor::setNamedColor()`. Si no se establece, el sistema elige un color que contraste con el fondo.
root/desktop/preferences/iconPercent	Especifica el porcentaje del tamaño de la cuadrícula que se va a usar para el icono. Si el valor es mayor que 0, se calcula como una proporción del tamaño de la cuadrícula.
root/desktop/preferences/iconShadowColor	Especifica el color de la sombra detrás del texto y el icono del escritorio. Las cadenas válidas tienen el estilo `QColor::setNamedColor()`. Si no se establece, el sistema elige un color que contraste con el fondo.
root/desktop/preferences/menu/arrange/authorized	Especifica si los usuarios pueden usar la función de organización en el escritorio.
root/desktop/preferences/menu/create/authorized	Especifica si los usuarios pueden crear conexiones desde el menú de clic derecho en el escritorio.
root/desktop/preferences/menu/drag/authorized	Especifica si los usuarios pueden arrastrar y soltar los iconos en el escritorio.
root/desktop/preferences/menu/lockScreen/authorized	Especifica si los usuarios pueden bloquear la pantalla desde el menú de clic de derecho en el escritorio.
root/desktop/preferences/menu/logout/authorized	Especifica si los usuarios pueden cerrar sesión desde el menú de clic derecho en el escritorio.
root/desktop/preferences/menu/modeSwitch/authorized	Especifica si los usuarios pueden cambiar al modo de administrador desde el menú de clic derecho en el escritorio.

Tabla E-30 Claves de registro del escritorio (continúa)

Clave de registro	Descripción
root/desktop/preferences/menu/power/authorized	Especifica si los usuarios pueden acceder al submenú de energía desde el menú de clic derecho en el escritorio.
root/desktop/preferences/menu/poweroff/authorized	Especifica si los usuarios pueden apagar el sistema desde el menú de clic derecho en el escritorio.
root/desktop/preferences/menu/reboot/authorized	Especifica si los usuarios pueden reiniciar el sistema desde el menú de clic derecho en el escritorio.
root/desktop/preferences/menu/sleep/authorized	Especifica si los usuarios pueden poner el sistema en estado de suspensión desde el menú de clic derecho en el escritorio.
root/desktop/preferences/menuTextSize	Especifica la altura del texto del menú del escritorio en píxeles. Si no es positivo, la altura se calcula como una proporción del tamaño del monitor.
root/desktop/preferences/screenMargin	Especifica el margen entre los bordes de la pantalla y los iconos.
root/desktop/preferences/textBold	Especifica si el texto queda en negrita.
root/desktop/preferences/textColor	Especifica el color del texto para los iconos del escritorio. Las cadenas válidas tienen el estilo `QColor::setNamedColor()`. Si no se establece, el sistema elige un color que contraste con el fondo.
root/desktop/preferences/textShadowColor	Especifica el color de la sombra detrás del texto y los iconos del escritorio. Las cadenas válidas tienen el estilo `QColor::setNamedColor()`. Si no se establece, el sistema elige un color que contraste con el color del texto.
root/desktop/preferences/textSize	Especifica la altura del texto en el icono del escritorio en píxeles. Si no es positivo, la altura se calcula como una proporción del tamaño del monitor.
root/desktop/shortcuts/<action>/command	Establece el comando que ejecuta el acceso directo.
root/desktop/shortcuts/<action>/enabled	Si se establece en 1, se activa el acceso directo.
root/desktop/shortcuts/<action>/shortcut	Especifica el nombre del acceso directo.
root/desktop/shortcuts/<action>/shortcutsMode	Establece el modo de acceso directo.

domain

Claves de registro de dominio.

Tabla E-31 Claves de registro de dominio

Clave de registro	Descripción
root/domain/OU	Especifica la unidad organizacional asociada con la membresía de dominio del thin client.

Tabla E-31 Claves de registro de dominio (continúa)

Clave de registro	Descripción
root/domain/allowSmartcard	Esta clave no se usa en el momento.
root/domain/cacheDomainLogin	Si se habilita, se guarda en el disco un hash de credenciales de inicio de sesión del dominio, de modo que los inicios de sesión subsiguientes pueden ocurrir incluso si no se puede acceder al servidor de Active Directory.
root/domain/ddns	Si se habilita, el thin client trata de actualizar el servidor de DNS con su nombre de usuario y la dirección IP durante cada renovación de DHCP.
root/domain/domain	Especifica el dominio al que se integró este thin client o contra el que se está autenticando este thin client.
root/domain/domainAdminGroup	Si se habilita enableDomainAdmin, los miembros de este grupo de AD pueden pasar el thin client al modo de administrador.
root/domain/domainControllers	Especifica una lista separada por comas de las controladoras del dominio que se van a usar con este dominio. Si se deja en blanco (lo que se recomienda), se realiza una búsqueda automática de controladoras de dominio mediante DNS.
root/domain/domainJoined	Indica si el thin client se ha agregado formalmente al dominio.
root/domain/domainUsersGroup	Si se habilita enableDomainUsers, los inicios de sesión en el dominio se limitan a los miembros directos de este grupo. Los grupos anidados no se admiten en este recurso.
root/domain/enableDomainAdmin	Si se establece en 1, los miembros del grupo enumerados en domainAdminGroup pueden pasar el thin client al modo de administrador. Si se establece en 0, se debe usar la cuenta de raíz local para realizar las tareas administrativas locales.
root/domain/enableDomainUsers	Si se establece en 1, los inicios de sesión del dominio se limitan a los miembros del grupo enumerados en domainUserGroup. Si se establece en 0, se permite cualquier credencial de dominio válida para iniciar sesión en el thin client.
root/domain/enablePasswordChange	Si se establece en 1, el usuario puede cambiar su contraseña de dominio directamente desde el thin client.
root/domain/enableSSO	Si se habilita, las credenciales actuales encriptadas se almacenan en caché en la memoria y se pueden volver a utilizar al iniciar conexiones remotas.
root/domain/loginAtStart	Si se establece en 1, y el thin client se ha agregado a un dominio, aparece una pantalla de inicio de sesión cuando se inicia el thin client. De lo contrario, aparece en el inicio el escritorio compartido de ThinPro heredado.
root/domain/retainUserRegistry	Si se establece en 1, entre las sesiones de inicio de sesión se conserva cualquier cambio que el usuario haya hecho en la configuración personalizada.
root/domain/workgroup	Especifica el grupo de trabajo o el "dominio corto" asociado con la membresía de dominio del thin client. Esto también se conoce como el nombre de dominio de NetBIOS durante la creación del dominio de Active Directory. Por lo general este valor se detecta de forma automática durante la autenticación del dominio al buscar el valor desde una controladora de dominio.

entries

Claves de registro de entradas.

Tabla E-32 Claves de registro de entradas

Clave de registro	Descripción
root/entries/<UUID>/command	
root/entries/<UUID>/folder	
root/entries/<UUID>/icon	
root/entries/<UUID>/label	
root/entries/<UUID>/metaInfo	
root/entries/<UUID>/onDesktop	
root/entries/<UUID>/onMenu	

firewall

Claves de registro para configuración del firewall.

Tabla E-33 Claves del registro para configuración del firewall

Clave de registro	Descripción
root/firewall/direct/pptp-rule	
root/firewall/icmp-blocks	
root/firewall/interfaces	
root/firewall/masquerade	
root/firewall/ports	
root/firewall/services/<service>/checked	
root/firewall/services/<service/description	
root/firewall/services/<service>/ destinations/ipv4	
root/firewall/services/<service>/ destinations/ipv6	
root/firewall/services/<service>/modules	

Tabla E-33 Claves del registro para configuración del firewall (continúa)

Clave de registro	Descripción
root/firewall/services/<service>/port-protocols	
root/firewall/services/<service>/short	
root/firewall/sources	
root/firewall/startAtBoot	

hwh264

Clave de registro de hwh264.

Tabla E-34 Clave de registro de hwh264

Clave de registro	Descripción
root/hwh264/force2x4k	HP no recomienda cambiar el valor de esta clave. En algunas configuraciones de escritorio de Citrix H264, las transmisiones grandes del escritorio con dos monitores causan un efecto de parpadeo. H264 por lo general de deshabilita para transmisiones grandes debido a es problema.

teclado

Claves de registro para configuraciones de teclado.

Tabla E-35 Claves de registro para configuraciones de teclado

Clave de registro	Descripción
root/keyboard/DrawLocaleLetter	Si se establece en 1, el icono de bandeja del sistema del teclado dibujará la secuencia regional de idioma en lugar de utilizar las imágenes estáticas.
root/keyboard/SystrayMenu/keyboardLayout	Si se establece en 1, el menú del botón derecho en el icono de la bandeja del sistema del teclado ofrece la opción de abrir la herramienta Formato de Teclado en el Panel de control.
root/keyboard/SystrayMenu/languages	Si se establece en 1, el menú del botón derecho en el icono de la bandeja del sistema del teclado ofrece la opción de abrir la herramienta Idioma en el Panel de control.
root/keyboard/SystrayMenu/virtualKeyboard	Si se establece en 1, el menú del botón derecho en el icono de la bandeja del sistema del teclado ofrece la opción de abrir el teclado virtual.
root/keyboard/VisibleInSystray	Si se establece en 1, se muestra el icono de la bandeja del sistema del teclado e indica la disposición actual del teclado.

Tabla E-35 Claves de registro para configuraciones de teclado (continúa)

Clave de registro	Descripción
root/keyboard/XkbLayout	Esta es una clave interna utilizada para asignarse a una disposición de teclado XKB. No debería ser necesario modificar esta clave.
root/keyboard/XkbModel	Esta es una clave interna utilizada para asignarse a un modelo de teclado XKB. No debería ser necesario modificar esta clave.
root/keyboard/XkbOptions	Esta es una clave interna utilizada para asignarse a opciones de teclado XKB. No debería ser necesario modificar esta clave.
root/keyboard/XkbVariant	Esta es una clave interna utilizada para asignarse a una variante de teclado XKB. No debería ser necesario modificar esta clave.
root/keyboard/enable2	Si se establece en 1, puede cambiarse la disposición del teclado secundario mediante el acceso directo del teclado, definido por switch.
root/keyboard/layout	Establece la disposición del teclado principal.
root/keyboard/layout2	Establece la disposición del teclado secundario.
root/keyboard/model	Establece el modelo de teclado principal.
root/keyboard/model2	Establece el modelo de teclado secundario.
root/keyboard/numlock	Si se establece en 1, se activa la función Bloq Num al iniciar el sistema. Esta clave de registro se ignora intencionalmente en los thin clients móviles.
root/keyboard/switch	Establece el acceso directo para alternar entre la disposición del teclado principal y secundario (enable2 también se debe establecer en 1). Los valores válidos son los siguientes: grp:ctrl_shift_toggle, grp:ctrl_alt_toggle, grp:alt_shift_toggle.
root/keyboard/variant	Establece la variante de teclado principal.
root/keyboard/variant2	Establece la variante de teclado secundario.

license

Claves de registro para la configuración de notificación de licencia.

Tabla E-36 Claves de registro para la configuración de notificación de licencia

Clave de registro	Descripción
root/license/courtesyNotificationEnable	Si se establece en 1, las notificaciones de la bandeja del sistema se habilitan a medida que se acerca la expiración de la licencia.
root/license/courtesyNotificationInterval	Si es positivo, cantidad de horas entre las notificaciones de cortesía.
root/license/courtesyNotificationStart	Si es positivo, las notificaciones de cortesía empiezan estos días antes de la fecha de expiración.

Tabla E-36 **Claves de registro para la configuración de notificación de licencia (continúa)**

Clave de registro	Descripción
`root/license/courtesyNotificationText`	Si no está en blanco, este texto se utiliza en notificaciones de cortesía. %1 se sustituye por la cantidad de días que quedan antes de la expiración; %2 se sustituye por la fecha de expiración.
`root/license/watermark`	Este valor es apenas para lectura.

logging

Claves de registro de logging.

Tabla E-37 **Claves de registro de logging**

Clave de registro	Descripción
`root/logging/general/debugLevel`	Establece el nivel de depuración. Este valor será aprovechado por otros módulos para generar los registros correspondientes.
`root/logging/general/showDebugLevelBox`	Si se establece en 1, la opción **Nivel de depuración** en la ficha **Registros del sistema** de la ventana **Información del sistema** estará disponible para los usuarios finales. Si se establece en 0, la opción está disponible sólo para administradores.

login

Claves de registro de las configuraciones de inicio de sesión.

Tabla E-38 **Claves de registro de las configuraciones de inicio de sesión**

Clave de registro	Descripción
`root/login/buttons/configure/authorized`	Si se establece en 1, el botón Configuración está disponible en la pantalla de inicio de sesión.
`root/login/buttons/info/authorized`	Si se establece en 1, el botón Información del sistema está disponible en la pantalla de inicio de sesión.
`root/login/buttons/keyboard/authorized`	Si se establece en 1, los ajustes de disposición del teclado se pueden configurar en la pantalla de inicio de sesión.
`root/login/buttons/locale/authorized`	Si se establece en 1, los ajustes de idioma se pueden configurar en la pantalla de inicio de sesión.
`root/login/buttons/mouse/authorized`	Si se establece en 1, los ajustes del mouse se pueden configurar en la pantalla de inicio de sesión.
`root/login/buttons/onscreenKeyboard/authorized`	Si se establece en 1, el teclado en la pantalla está disponible en la pantalla de inicio de sesión.
`root/login/buttons/power/authorized`	Si se establece en 1, el botón de inicio/apagado está disponible en la pantalla de inicio de sesión.
`root/login/buttons/poweroff/authorized`	Si se establece en 1, la función de apagado está disponible en la pantalla de inicio de sesión.

Tabla E-38 Claves de registro de las configuraciones de inicio de sesión (continúa)

Clave de registro	Descripción
root/login/buttons/reboot/authorized	Si se establece en 1, la función de reinicio está disponible en la pantalla de inicio de sesión.
root/login/buttons/show/authorized	Si se establece en 1, la lista con opciones adicionales del botón está disponible en la pantalla de inicio de sesión.
root/login/buttons/sleep/authorized	Si se establece en 1, la función de suspensión está disponible en la pantalla de inicio de sesión.
root/login/buttons/touchscreen/authorized	Si se establece en 1, los ajustes de la pantalla táctil se pueden configurar en la pantalla de inicio de sesión. La clave de registro root/touchscreen/enabled también debe activarse.
root/login/rememberedDomain	
root/login/rememberedUser	

mouse

Claves de registro de la configuración del mouse.

Tabla E-39 Claves de registro de la configuración del mouse

Clave de registro	Descripción
root/mouse/MouseHandedness	Si se establece en 0, el mouse es para diestros. Si se establece en 1, el mouse es para zurdos.
root/mouse/MouseSpeed	Establece la aceleración del puntero del mouse. Normalmente, el rango utilizable es de 0 a 25. Un valor de 0 desactiva completamente la aceleración, lo que hace que el mouse se mueva a un ritmo lento constante, pero medible.
root/mouse/MouseThreshold	Establece la cantidad de píxeles antes de que se activa la aceleración del mouse. Un valor de 0 establece la aceleración en una curva natural que aumenta gradualmente la aceleración, lo que permite realizar movimientos precisos y rápidos.
root/mouse/disableTrackpadWhileTyping	Si se establece en 1, el trackpad se desactivará temporalmente mientras se escribe. Si se establece en 0, el trackpad no se desactivará temporalmente mientras se escribe.
root/mouse/enableNaturalScrolling	Si se establece en 1 (predeterminado), el desplazamiento natural se habilita en el trackpad. Si se establece en 0, el desplazamiento natural se deshabilita en el trackpad.
root/mouse/enableTrackpad	Si se establece en 1, se habilita el trackpad. Si se establece en 0, se deshabilita el trackpad.
root/mouse/enableTrackpadTapping	Si se establece en 0 (valor predeterminado), se deshabilita el comportamiento de pulsación para hacer clic en el trackpad. Si se establece en 1, se habilita el comportamiento de pulsación para hacer clic.
root/mouse/enableTwoFingerScrolling	Si se establece en 1 (predeterminado), el desplazamiento con dos dedos se habilita en el trackpad. Si se establece en 0, el desplazamiento con dos dedos se deshabilita en el trackpad.

Tabla E-39 Claves de registro de la configuración del mouse (continúa)

Clave de registro	Descripción
root/mouse/gui	

restore-points

Clave de registro para puntos de restauración.

Tabla E-40 Ajustes del registro para puntos de restauración

Clave de registro	Descripción
root/restore-points/factory	Especifica cuál instantánea se va a utilizar para un restablecimiento de fábrica.

protector de pantalla

Claves de registro de Configuración del protector de pantalla.

Tabla E-41 Claves de registro de Configuración del protector de pantalla

Clave de registro	Descripción
root/screensaver/SlideShowAllMonitors	Si se establece en 1, la presentación del protector de pantalla se mostrará en todos los monitores. Si se establece en 0, la presentación se mostrará solo en el primer monitor.
root/screensaver/SlideShowInterval	Establece el intervalo en segundos para el cambio de imágenes en la presentación del protector de pantalla.
root/screensaver/SlideShowPath	Especifica el directorio que contiene las imágenes para la presentación del protector de pantalla.
root/screensaver/buttons/configure/authorized	Si se establece en 1, el botón Configuración está disponible cuando la pantalla está bloqueada.
root/screensaver/buttons/info/authorized	Si se establece en 1, el botón Información del sistema está disponible cuando la pantalla está bloqueada.
root/screensaver/buttons/keyboard/authorized	Si se establece en 1, los ajustes de disposición del teclado se pueden configurar cuando la pantalla está bloqueada.
root/screensaver/buttons/locale/authorized	Si se establece en 1, los ajustes de idioma se pueden configurar cuando la pantalla está bloqueada.
root/screensaver/buttons/mouse/authorized	Si se establece en 1, los ajustes del mouse se pueden configurar cuando la pantalla está bloqueada.
root/screensaver/buttons/onscreenKeyboard/authorized	Si se establece en 1, el teclado de la pantalla está disponible cuando la pantalla está bloqueada.
root/screensaver/buttons/power/authorized	Si se establece en 1, el botón de inicio/apagado está disponible cuando la pantalla está bloqueada.

Tabla E-41 Claves de registro de Configuración del protector de pantalla (continúa)

Clave de registro	Descripción
root/screensaver/buttons/poweroff/authorized	Si se establece en 1, la función de apagado está disponible cuando la pantalla está bloqueada.
root/screensaver/buttons/reboot/authorized	Si se establece en 1, la función de reinicio está disponible cuando la pantalla está bloqueada.
root/screensaver/buttons/show/authorized	Si se establece en 1, la lista con opciones adicionales del botón está disponible cuando la pantalla está bloqueada.
root/screensaver/buttons/sleep/authorized	Si se establece en 1, la función de suspensión está disponible cuando la pantalla está bloqueada.
root/screensaver/buttons/touchscreen/authorized	Si se establece en 1, los ajustes de la pantalla táctil se pueden configurar cuando la pantalla está bloqueada. La clave de registro root/touchscreen/enabled también debe activarse.
root/screensaver/enableCustomLogo	Si se establece en 1, se usa la imagen personalizada definida en logoPath para el protector de pantalla.
root/screensaver/enableDPMS	Si se establece en 0, se desactiva la administración de energía del monitor. Esto hace que el monitor permanezca siempre encendido a menos que se apague manualmente.
root/screensaver/enableScreensaver	Si se establece en 1, se activa el protector de pantalla.
root/screensaver/enableSleep	Si se establece en 1, se activa la suspensión.
root/screensaver/lockScreen	Si se establece en 1 y ha iniciado sesión en el modo de administrador, se requiere una contraseña para volver al escritorio desde el protector de pantalla.
root/screensaver/lockScreenDomain	Si se establece en 1 y el sistema está en modo de dominio, se requiere una contraseña para volver al escritorio desde el protector de pantalla.
root/screensaver/lockScreenUser	Si se establece en 1 y no ha iniciado sesión como administrador y el sistema no está en el modo de dominio, se requiere una contraseña para volver al escritorio desde el protector de pantalla.
root/screensaver/logoPath	Establece la ruta a una imagen personalizada que se utiliza para el protector de pantalla.
root/screensaver/mode	Establece el modo de renderización para la imagen del protector de pantalla (como Center, Tile, Expand y Stretch). Si se establece en Default, la imagen se muestra sin ningún procesamiento. Si se establece en SlideShow, el protector de pantalla circulará imágenes del directorio especificado por SlideShowPath.
root/screensaver/off	Establece el intervalo de espera en minutos antes de que se apague el monitor.
root/screensaver/origImageCopyPath	Esta es la ruta donde se guarda la imagen personalizada cuando el mode se establece en Default.
root/screensaver/solidColor	Si useSolidColor está activado y enableCustomLogo está desactivado, este color fijo se usa para el protector de pantalla.
root/screensaver/standby	Establece el intervalo de espera en minutos antes de que el monitor entre en modo de espera.
root/screensaver/suspend	Establece el intervalo de espera en minutos antes de que el monitor entre en modo de suspensión.

Tabla E-41 Claves de registro de Configuración del protector de pantalla (continúa)

Clave de registro	Descripción
`root/screensaver/timeoutScreensaver`	Establece el intervalo de espera en minutos antes de que se inicie el protector de pantalla.
`root/screensaver/timeoutSleep`	Establece el intervalo de espera en minutos antes de que el thin client entre en estado de suspensión.
`root/screensaver/useSolidColor`	Si se establece en 1 y `enableCustomLogo` está desactivado, el protector de pantalla usa el valor de la clave `solidColor`.

seguridad

Claves de registro de los ajustes de seguridad.

Tabla E-42 Claves de registro de los ajustes de seguridad

Clave de registro	Descripción
`root/security/SecurityFeaturs/SpeculativeStoreBypassControl`	Controla si se habilitan las mitigaciones de Speculative Store Bypass (CVE-2018-3639). De forma predeterminada, estas mitigaciones no están habilitadas. Para habilitarlas, establezca en valor de la clave como activada. Para que entren en efecto los cambios a esta clave, reinicie el equipo.
`root/security/authenticationFailDelay`	Establece el tiempo aproximado, en milisegundos, que se debe demorar después de un intento fallido de inicio de sesión. El tiempo real varía más o menos 25 % de este valor. Por ejemplo, use un valor de 3000 para obtener una demora de aproximadamente 3 segundos.
`root/security/domainEntryMode`	Si se establece en 1, se espera que se introduzca el dominio en un campo de texto separado con la etiqueta **Dominio**. Si se establece en 0, se espera que se introduzca el dominio como parte del campo **Usuario**.
`root/security/enableLockOverride`	Si se establece en 1, los administradores pueden anular el bloqueo de la pantalla de un escritorio local.
`root/security/enableSecretPeek`	Si se establece en 1, los cuadros de diálogo de la contraseña y el PIN tendrán un botón que, al seleccionarse, mostrará la contraseña/el PIN introducidos en texto legible.
`root/security/encryption/identity/encryptedSecretCipher`	Establece el algoritmo para la encriptación simétrica de un secreto. Todos los algoritmos usan una cantidad adecuada de semilla aleatoria, que se regenera cada vez que se almacena el secreto. La clave de encriptación es diferente en cada thin client y la encriptación y la desencriptación solo están disponibles para programas autorizados. La lista de cifrados admitidos incluye la mayoría de cifrados de OpenSSL y ChaCha20–Poly1305.
`root/security/encryption/identity/encryptedSecretTTL`	Establece la cantidad de segundos desde que se considera válido el último inicio de sesión correcto que almacenó un secreto encriptado. Si se establece un número negativo, los secretos encriptados no tendrán tiempo de validez.
`root/security/encryption/identity/encryptedSecretTTLnonSSO`	Especifica la cantidad de segundos que un secreto encriptado no SSO almacenado se considera válido. Si se establece un número no positivo, los secretos encriptados no tendrán tiempo de validez.

Tabla E-42 Claves de registro de los ajustes de seguridad (continúa)

Clave de registro	Descripción
root/security/encryption/identity/secretHashAlgorithm	Establece el algoritmo para la creación de un hash de un secreto. Las Funciones de derivación de clave (KDF, por sus siglas en inglés) como scrypt o argon2 son mejores que hashes directos porque no se puede calcular rápidamente un diccionario de arco iris mediante una KDF. Todos los algoritmos usan una cantidad adecuada de semilla aleatoria, que se regenera cada vez que se oculta con hash el secreto. La lista admitida incluye scrypt, Argon2, SHA-256 y SHA-512 (aunque los últimos dos no son KDF).
root/security/encryption/identity/secretHashTTL	Establece la cantidad de segundos desde que se considera válido el último inicio de sesión correcto que almacenó hashes de secretos. Si se establece un número negativo, los hashes de secretos no tendrán tiempo de validez.
root/security/mustLogin	Si se establece en 1, se obliga a todos los los usuarios a iniciar sesión antes de acceder al escritorio.

apagado

Claves de registro de configuración de apagado.

Tabla E-43 Claves de registro de configuración de apagado

Clave de registro	Descripción
root/shutdown/enableAutomaticShutdownTimeout	Si se establece en 1, aparece una barra de progreso en el cuadro de diálogo de apagar/reiniciar/cerrar sesión. Si la pregunta no se responde a tiempo, automáticamente se apaga/reinicia/cierra sesión.
root/shutdown/timeOfAutomaticShutdownTimeout	Establece el tiempo de espera del apagado automático.

sshd

Claves de registro sshd.

Tabla E-44 Claves de registro sshd

Clave de registro	Descripción
root/sshd/disableWeakCipher	Si se establece en 1, se desactiva el cifrado del modo CBC, así como otros cifrados débiles conocidos, como 3DES, arcfour, etc.
root/sshd/disableWeakHmac	Si se establece en 1, se desactiva hmac de 96 bits, así como cualquier hmac basado en sha1 y en md5.
root/sshd/disableWeakKex	Si se establece en 1, se desactivan los algoritmos de intercambio de clave que tienen DH con SHA1.
root/sshd/enabled	Si se establece en 1, se activa el daemon SSH y se puede acceder al thin client a través de SSH.
root/sshd/userAccess	Si se establece en 1, los usuarios finales pueden conectarse al thin client a través de SSH.

time

Claves de registro de configuración de hora y fecha.

Tabla E-45 Claves de registro de hora

Clave de registro	Descripción
root/time/NTPServers	Especifica los servidores NTP que se van a utilizar a través de una lista separada por comas. Los servidores NTP privados o clústeres NTP virtuales grandes como pool.ntp.org son las mejores opciones para minimizar la carga del servidor. Borre este valor para volver a utilizar los servidores DHCP (etiqueta 42) en lugar de una lista fija.
root/time/dateFormatLong	Es una forma opcional de anular el formato de fecha largo utilizado en varias herramientas de ThinPro. Para obtener información sobre el formateo, busque en la web QDate::toString. Si se deja en blanco, por lo general se usa una cadena específica del lugar.
root/time/dateFormatShort	Es una forma opcional de anular el formato de fecha corto utilizado en varias herramientas de ThinPro. Para obtener información sobre el formateo, busque en la web QDate::toString. Si se deja en blanco, por lo general se usa una cadena específica del lugar.
root/time/dateTimeFormatLong	Es una forma opcional de anular el formato de fecha y hora largo utilizado en varias herramientas de ThinPro. Para obtener información sobre el formateo, busque en la web QDate::toString. Si se deja en blanco, por lo general se usa una cadena específica del lugar.
root/time/dateTimeFormatShort	Es una forma opcional de anular el formato de fecha y hora corto utilizado en varias herramientas de ThinPro. Para obtener información sobre el formateo, busque en la web QDate::toString. Si se deja en blanco, por lo general se usa una cadena específica del lugar.
root/time/hideCountries	Es una lista separada por puntos y comas de los países que quiere ocultar en la GUI de selección de zona horaria.
root/time/hideMap	Si se establece en 1, el mapa no se dibuja. Esto puede ser preferible en instancias donde los límites están en disputa.
root/time/hideWinZones	Es una lista separada por puntos y comas de las zonas horarias en formato Windows, como “(UTC+2:00) Tripoli”, que quiere ocultar en la GUI de selección de zona horaria.
root/time/hideZones	Es una lista separada por puntos y comas de las zonas horarias en formato Linux, como “America/Denver”, que quiere ocultar en la GUI de selección de zona horaria.
root/time/timeFormatLong	Es una forma opcional de anular el formato de hora largo utilizado en varias herramientas de ThinPro. Para obtener información sobre el formateo, busque en la web QDate::toString. Si se deja en blanco, por lo general se usa una cadena específica del lugar.
root/time/timeFormatShort	Es una forma opcional de anular el formato de hora corto utilizado en varias herramientas de ThinPro. Para obtener información sobre el formateo, busque en la web QDate::toString. Si se deja en blanco, por lo general se usa una cadena específica del lugar.

Tabla E-45 Claves de registro de hora (continúa)

Clave de registro	Descripción
root/time/timezone	Establece la zona horaria. Las zonas horarias se deben especificar tal y como las define **Zona horaria de Linux** en la herramienta de **Fecha y Hora** en el Panel de control y deben seguir este formato: <región>/<subregión>.
root/time/use24HourFormat	Si se establece en -1, el sistema selecciona el formato automáticamente según la configuración regional. Si se establece en 0, se usa el formato a.m./p.m. Si se establece en 1, se usa el formato de 24 horas.
root/time/useADDNSTimeServers	Si se establece en 1, el thin client tratará de establecer la zona horaria mediante las controladoras de dominio de Active Directory detectadas de forma automática en la red local. Lo hace a través de la siguiente consulta de DNS para los registros de SRV: _ldap._tcp.dc._msdcs.domain.
root/time/useDHCPTimezone	Si se establece en 1, el thin client intenta establecer la zona horaria a través de DHCP. Para establecer correctamente la zona horaria mediante esta clave de registro, asegúrese de que el servidor DHCP del thin client reenvíe la etiqueta DHCP tcode (que suele ser la etiqueta 101, aunque la 100 y la 2 también pueden funcionar).
root/time/useNTPServers	Si se establece en 1, se activa el uso de los servidores horarios NTP para sincronizar el reloj del thin client. Si está activado, asegúrese de que se especifique un servidor NTP a través de DHCP o de NTPServers.

touchscreen

Claves de registro de la configuración de la pantalla táctil.

Tabla E-46 Claves de registro de la configuración de la pantalla táctil

Clave de registro	Descripción
root/touchscreen/beep	Define si el thin client produce un bip cuando se usa la pantalla táctil.
root/touchscreen/calibrated	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/touchscreen/enabled	Si se establece en 1, se activa la entrada táctil.
root/touchscreen/maxx	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/touchscreen/maxy	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/touchscreen/minx	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/touchscreen/miny	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/touchscreen/port	Especifica el puerto que está conectado a la pantalla táctil.

Tabla E-46 Claves de registro de la configuración de la pantalla táctil (continúa)

Clave de registro	Descripción
root/touchscreen/swapx	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/touchscreen/swapy	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/touchscreen/type	Especifica el tipo de controladora de la pantalla táctil.

translation

Claves de registro de las configuraciones de traducción.

Tabla E-47 Claves de registro de las configuraciones de traducción

Clave de registro	Descripción
root/translation/coreSettings/localeMapping/<LanguageCode>	Se trata de teclas internas utilizadas para brindar la secuencia de texto junto al idioma adecuado en el selector de idioma. No debería ser necesario modificar estas claves.
root/translation/coreSettings/localeSettings	Establece la configuración regional del thin client. Esta configuración local también se enviará a la conexión remota. Las configuraciones regionales válidas son en_US (inglés), de_DE (alemán), es_ES (español), fr_FR (francés), ru_RU (ruso), ja_JP (japonés), ko_KR (coreano), zh_CN (chino simplificado) y zh_TW (chino tradicional).
root/translation/gui/LocaleManager/name	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/translation/gui/LocaleManager/status	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/translation/gui/LocaleManager/title	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/translation/gui/LocaleManager/widgets/localeSettings	Controla el estado del widget de configuración local en la herramienta Idioma. Si se establece como active, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como inactive, el widget queda oculto. Si se establece como read-only, el widget puede verse en el modo de solo lectura.

usb-update

Claves de registro de actualización de USB.

Tabla E-48 Claves de registro de actualización de USB.

Clave de registro	Descripción
root/usb-update/authentication	Si se establece en 1, se requiere una contraseña de administrador para las actualizaciones USB.

Tabla E-48 Claves de registro de actualización de USB. (continúa)

Clave de registro	Descripción
root/usb-update/enable	Si se establece en 1, se activa la detección automática de actualizaciones USB.
root/usb-update/height	Establece la altura de la ventana de USB Update (Actualización USB) en píxeles.
root/usb-update/searchMaxDepth	Establece la profundidad de los subdirectorios donde se buscarán las actualizaciones. Si se establece una profundidad de búsqueda alta podrían producirse retrasos en las unidades flash USB que cuentan con miles de directorios.
root/usb-update/width	El ancho de la ventana de Actualización USB en píxeles.

users

Claves de registro de Configuraciones de usuario.

Tabla E-49 Claves de registro de Configuraciones de usuario

Clave de registro	Descripción
root/users/root/enablePassword	Si está activado, se habilitan los inicios de sesión en la cuenta de administrador raíz local. Si está desactivado, solo los administradores de Active Directory pueden pasar el thin client al modo de administrador.
root/users/root/password	Establece la contraseña de administrador. Si está vacía, el modo de administrador está bloqueado.
root/users/root/timeout	Especifica el tiempo de inactividad (en minutos) después del cual se cancela el modo de administrador. Si se establece en 0 o en número negativo, el modo de administrador nunca se cancelará de forma automática.
root/users/user/SSO	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/users/user/WOL	Si se establece en 1, se activa Wake-On-LAN (WOL).
root/users/user/XHostCheck	Si establece en 1, sólo se permite el control remoto del thin client a los sistemas enumerados en root/users/usuario/xhosts.
root/users/user/apps/hptc-ad-change-password/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Cambiar contraseña de dominio** en el Panel de control.
root/users/user/apps/hptc-ad-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Active Directory** en el Panel de control.
root/users/user/apps/hptc-agent-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Agente HPDM** en el Panel de control.
root/users/user/apps/hptc-auto-update/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Actualización automática** en el Panel de control.
root/users/user/apps/hptc-background-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Administrador de fondos** en el Panel de control.

Tabla E-49 Claves de registro de Configuraciones de usuario (continúa)

Clave de registro	Descripción
root/users/user/apps/hptc-cert-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Administrador de certificados** en el Panel de control.
root/users/user/apps/hptc-compatibility/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Verificación de compatibilidad** en el Panel de control.
root/users/user/apps/hptc-component-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Administrador de componentes** en el Panel de control.
root/users/user/apps/hptc-config-wizard/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Asistente de configuración inicial** en el Panel de control.
root/users/user/apps/hptc-connection-wizard/authorized	Si se establece en 1, los usuarios finales pueden acceder a **Crear una conexión**.
root/users/user/apps/hptc-control-panel/authorized	Si se establece en 1, los usuarios finales pueden acceder al **Panel de control**.
root/users/user/apps/hptc-date-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Fecha y Hora** en el Panel de control.
root/users/user/apps/hptc-dhcp-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Opciones de DHCP** en el Panel de control.
root/users/user/apps/hptc-display-prefs/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Pantalla** en el Panel de control.
root/users/user/apps/hptc-easy-update/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Easy Update** en el Panel de control.
root/users/user/apps/hptc-factory-reset/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Restablecimiento de fábrica** en el Panel de control.
root/users/user/apps/hptc-firewalld-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Administrador de firewall** en el Panel de control.
root/users/user/apps/hptc-i18n-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Idioma** en el Panel de control.
root/users/user/apps/hptc-ibus-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Método de entrada Ibus** en el Panel de control.
root/users/user/apps/hptc-imprivata-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Configuración de Imprivata** en el Panel de control.
root/users/user/apps/hptc-keyboard-layout/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Disposición de Teclado** en el Panel de control.
root/users/user/apps/hptc-kiosk/authorized	Si se establece en 1, los usuarios estándares pueden acceder al **Administrador de conexión**.
root/users/user/apps/hptc-licenses/authorized	Si se establece en 1, los usuarios finales pueden acceder al **Contrato de licencia de HP**.
root/users/user/apps/hptc-mixer/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Sonido** en el Panel de control.

Tabla E-49 Claves de registro de Configuraciones de usuario (continúa)

Clave de registro	Descripción
root/users/user/apps/hptc-mouse/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Mouse** en el Panel de control.
root/users/user/apps/hptc-network-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Administrador de redes** en el Panel de control.
root/users/user/apps/hptc-power-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Administrador de energía** en el Panel de control.
root/users/user/apps/hptc-printer-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Impresoras** en el Panel de control.
root/users/user/apps/hptc-regeditor/authorized	Si se establece en 1, los usuarios finales pueden acceder al **Editor de registro**.
root/users/user/apps/hptc-restore/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Instantáneas** en el Panel de control.
root/users/user/apps/hptc-scep-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Administrador de SCEP** en el Panel de control.
root/users/user/apps/hptc-security/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Seguridad** en el Panel de control.
root/users/user/apps/hptc-serial-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Administrador de serie** en el Panel de control.
root/users/user/apps/hptc-shortcut-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Acessos directos del teclado** en el Panel de control.
root/users/user/apps/hptc-snipping-tool/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Recortes** en el Panel de control.
root/users/user/apps/hptc-sshd-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Administrador de SSHD** en el Panel de control.
root/users/user/apps/hptc-switch-admin/authorized	Si se establece en 1, los usuarios finales pueden acceder a **Cambiar a Administrador/Usuario**.
root/users/user/apps/hptc-sysinfo/authorized	Si se establece en 1, los usuarios finales pueden acceder a la **Información del sistema**.
root/users/user/apps/hptc-task-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Administrador de tareas** en el menú de Inicio.
root/users/user/apps/hptc-text-editor/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Editor de texto** en el menú de Inicio.
root/users/user/apps/hptc-thinstate/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **ThinState** en el Panel de control.
root/users/user/apps/hptc-touchscreen/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento **Pantalla Táctil** en el Panel de control.
root/users/user/apps/hptc-update/authorized	Si se establece en 1, los usuarios finales pueden acceder a **Buscar actualizaciones**.

Tabla E-49 **Claves de registro de Configuraciones de usuario (continúa)**

Clave de registro	Descripción
`root/users/user/apps/hptc-usb-mgr/authorized`	Si se establece en 1, los usuarios finales pueden acceder al elemento **Administrador de USB** en el Panel de control.
`root/users/user/apps/hptc-user-rights/authorized`	Si se establece en 1, los usuarios finales pueden acceder al elemento **Centro de personalización** en el Panel de control.
`root/users/user/apps/hptc-vncshadow/authorized`	Si se establece en 1, los usuarios finales pueden acceder al elemento **Sombreamiento VNC** en el Panel de control.
`root/users/user/apps/hptc-wlsstat/authorized`	Si se establece en 1, los usuarios finales pueden acceder a **Estadísticas de conexión inalámbrica**.
`root/users/user/apps/hptc-xen-general-mgr/authorized`	Si se establece en 1, los usuarios finales pueden acceder a los ajustes generales de Citrix.
`root/users/user/apps/hptc-xterm/authorized`	Si se establece en 1, los usuarios finales pueden acceder al **Terminal X**. **PRECAUCIÓN:** La habilitación del acceso al terminal X constituye un riesgo a la seguridad y no se recomienda en un entorno de producción. El terminal X solo debe habilitarse si se utiliza en la depuración de un entorno protegido y no de producción.
`root/users/user/desktopScaling`	Especifica el porcentaje en que aumenta o se reduce el tamaño de los elementos del escritorio. Si se establece en 100 (predeterminado), se usa la escala estándar. Si se establece en 50, se usa la mitad del tamaño de la escala estándar. Si se establece en 200, se duplica el tamaño de la escala estándar.
`root/users/user/enablePassword`	Si está habilitado, se habilitan los inicios de sesión en el `user` de la cuenta compartida local.
`root/users/user/hideDesktopPanel`	Si se establece en 1, los paneles del escritorio como la barra de tareas no se inician o se muestran en el escritorio.
`root/users/user/kioskMode`	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
`root/users/user/launchConnectionManager`	Si se establece en 1, el Administrador de conexión se abre al iniciar el sistema.
`root/users/user/rightclick`	Si se establece en 1, se activa el menú del botón derecho para el escritorio.
`root/users/user/ssoconnectiontype`	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
`root/users/user/switchAdmin`	Si se establece en 1, se habilita el cambio al modo de administrador.
`root/users/user/theme`	Reservado para uso futuro.
`root/users/user/xhosts/<UUID>/xhost`	Especifica la dirección IP o el nombre de host de un sistema al que se permitirá controlar de forma remota el thin client cuando esté habilitado `XHostCheck`.

vncserver

Claves de registro de vncserver.

Tabla E-50 Claves de registro de vncserver

Clave de registro	Descripción
root/vncserver/coreSettings/enableVncShadow	Si se establece en 1, se activa el servidor de control remoto de VNC para el thin client.
root/vncserver/coreSettings/userNotificationMessage	Establece el mensaje de notificación que se muestra al usuario cuando alguien intenta conectarse al thin client mediante VNC.
root/vncserver/coreSettings/vncAllowLoopbackOnly	Si se establece en 1, solo se permite una dirección de loopback o host local para las conexiones VNC.
root/vncserver/coreSettings/vncDefaultNumLockStatus	Si se establece en 1, Bloq Núm está activado de forma predeterminada. Si se establece en 0, Bloq Núm está desactivado de forma predeterminada.
root/vncserver/coreSettings/vncNotifyShowTimeout	Si se establece en 1, se aplica un intervalo de espera al cuadro de diálogo de notificación que se muestra al usuario cuando alguien intenta conectarse al thin client mediante VNC.
root/vncserver/coreSettings/vncNotifyTimeout	Establece el tiempo de espera en segundos del cuadro de diálogo de notificación que se muestra al usuario cuando alguien intenta conectarse al thin client mediante VNC.
root/vncserver/coreSettings/vncNotifyUser	Si se establece en 1, se muestra al usuario una notificación cuando alguien intenta conectarse al thin client mediante VNC.
root/vncserver/coreSettings/vncPassword	Establece la contraseña para la duplicación de VNC. También debe activarse la clave `vncUsePassword`.
root/vncserver/coreSettings/vncReadOnly	Si se establece en 1, la duplicación de VNC funcionará en modo de sólo vista.
root/vncserver/coreSettings/vncRefuseInDefault	Si se establece en 1, las solicitudes de VNC se rechazarán automáticamente si el usuario no interactúa con el cuadro de diálogo de notificación antes de que termine el intervalo de espera.
root/vncserver/coreSettings/vncStopButton	Si se establece en 1, aparece un botón siempre visible en la esquina izquierda de la pantalla. Si selecciona ese botón, se desconecta la sesión de VNC.
root/vncserver/coreSettings/vncTakeEffectRightNow	Si se establece en 1, la configuración de VNC tendrá efecto inmediatamente después de que se modifique.
root/vncserver/coreSettings/vncUseHTTP	Si se establece en 1, se abre el puerto HTTP 5800 para las conexiones de VNC.
root/vncserver/coreSettings/vncUsePassword	Si se establece en 1, se requiere la contraseña especificada en `vncPassword` para la duplicación VNC.
root/vncserver/coreSettings/vncUseSSL	Si se establece en 1, se utiliza SSL para las conexiones de VNC.
root/vncserver/gui/VNCShadowManager/name	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/vncserver/gui/VNCShadowManager/status	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/vncserver/gui/VNCShadowManager/title	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/vncserver/gui/VNCShadowManager/widgets/enableVncShadow	Controla el estado del widget **Permitir Sombreamiento VNC** en la herramienta Sombreamiento VNC. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget

Tabla E-50 Claves de registro de vncserver (continúa)

Clave de registro	Descripción
	queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/vncserver/gui/VNCShadowManager/widgets/userNotificationMessage`	Controla el estado del widget **Mensaje de Notificación de Usuario** en la herramienta Sombreamiento VNC. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/vncserver/gui/vncAllowLoopbackOnly`	Controla el estado del widget **Permitir solo conexiones de loopback** en la utilidad Duplicación VNC. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/vncserver/gui/VNCShadowManager/widgets/vncNotifyShowTimeout`	Controla el estado del widget **VNC Mostrar tiempo de espera para notificación** en la herramienta Sombreamiento VNC. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/vncserver/gui/VNCShadowManager/widgets/vncNotifyTimeout`	Controla el estado del widget numérico en la herramienta Sombreamiento VNC. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/vncserver/gui/VNCShadowManager/widgets/vncNotifyUser`	Controla el estado del widget **VNC Notifique Usuario para Negar** en la herramienta Sombreamiento VNC. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/vncserver/gui/VNCShadowManager/widgets/vncPassword`	Controla el estado del widget **Defina Contraseña** en la herramienta Sombreamiento VNC. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/vncserver/gui/VNCShadowManager/widgets/vncReadOnly`	Controla el estado del widget **VNC solo de lectura** en la herramienta Sombreamiento VNC. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/vncserver/gui/VNCShadowManager/widgets/vncRefuseInDefault`	Controla el estado del widget **Rechazar conexiones predeterminadas** en la herramienta Sombreamiento VNC. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/vncserver/gui/vncStopButton`	Controla el estado del botón **Detener duplicación de VNC** en la utilidad Duplicación VNC. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget

Tabla E-50 Claves de registro de vncserver (continúa)

Clave de registro	Descripción
	queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/vncserver/gui/VNCShadowManager/widgets/vncTakeEffectRightNow`	Controla el estado del widget **Restablecer el servidor VNC inmediatamente** en la herramienta Sombreamiento VNC. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/vncserver/gui/VNCShadowManager/widgets/vncUseHTTP`	Controla el estado del widget **Puerto 5800 http de uso de VNC** en la herramienta de duplicación VNC. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/vncserver/gui/VNCShadowManager/widgets/vncUsePassword`	Controla el estado del widget **Contraseña de uso de VNC** en la herramienta Duplicación VNC. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.
`root/vncserver/gui/VNCShadowManager/widgets/vncUseSSL`	Controla el estado del widget **VNC Utilice SSL** en la herramienta Sombreamiento VNC. Si se establece como `active`, el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como `inactive`, el widget queda oculto. Si se establece como `read-only`, el widget puede verse en el modo de solo lectura.

zero-login

Claves de registro de Smart Zero.

Tabla E-51 Claves de registro de Smart Zero

Clave de registro	Descripción
`root/zero-login/buttons/configure/authorized`	Si se establece en 1, el botón **Configurar** está disponible en el cuadro de diálogo de las credenciales de Smart Zero o de inicio de sesión.
`root/zero-login/buttons/info/authorized`	Si se establece en 1, el botón **Información del sistema** está disponible en el cuadro de diálogo de las credenciales de Smart Zero o de inicio de sesión.
`root/zero-login/buttons/keyboard/authorized`	Si se establece en 1, la selección **Disposición del teclado** está disponible en el cuadro de diálogo de las credenciales de Smart Zero o de inicio de sesión.
`root/zero-login/buttons/locale/authorized`	Si se establece en 1, la selección **Local** está disponible en el cuadro de diálogo de las credenciales de Smart Zero o de inicio de sesión.
`root/zero-login/buttons/mouse/authorized`	Si se establece en 1, la selección **Mouse** está disponible en el cuadro de diálogo de las credenciales de Smart Zero o de inicio de sesión.

Tabla E-51 Claves de registro de Smart Zero (continúa)

Clave de registro	Descripción
root/zero-login/buttons/onscreenKeyboard/authorized	Si se establece en 1, la opción de teclado en la pantalla está disponible en el cuadro de diálogo de las credenciales de Smart Zero o de inicio de sesión.
root/zero-login/buttons/power/authorized	Si se establece en 1, el botón de **Inicio/apagado** está disponible en el cuadro de diálogo de las credenciales de Smart Zero o de inicio de sesión.
root/zero-login/buttons/poweroff/authorized	Si se establece en 1, la opción de **Apagado** está disponible en el cuadro de diálogo de las credenciales de Smart Zero o de inicio de sesión.
root/zero-login/buttons/reboot/authorized	Si se establece en 1, la opción **Reinicio** está disponible en el cuadro de diálogo de las credenciales de Smart Zero o de inicio de sesión.
root/zero-login/buttons/show/authorized	Si se establece en 1, los botones aparecen en el cuadro de diálogo de las credenciales de Smart Zero o de inicio de sesión.
root/zero-login/buttons/sleep/authorized	Si se establece en 1, la opción **Suspender** está disponible en el cuadro de diálogo de las credenciales de Smart Zero o de inicio de sesión.
root/zero-login/buttons/touchscreen/authorized	Si se establece en 1, la selección **Pantalla táctil** está disponible en el cuadro de diálogo de las credenciales de Smart Zero o de inicio de sesión. **NOTA:** La clave root/touchscreen/enabled también debe establecerse.

SNMP

Esta tabla describe las claves de registro de SNMP.

Tabla E-52 SNMP

Clave de registro	Descripción
root/snmp/agentBehaviour/enable	Si se establece en 1, se activa el daemon SNMP y spermite acceder al thin client a través de SNMP. Asegúrese de tener una configuración SNMP de seguridad o de trabajar en un entorno de red seguro.
root/snmp/agentBehaviour/usePrivateConfFile	Si se establece en 1, el daemon SNMP utiliza un archivo de configuración personalizado por el usuario para algunos recursos avanzados pero no genera snmpd.conf desde el registro.
root/snmp/agentBehaviour/listenInterface	Esta opción no funciona bien con el servicio DHCP, así que deje esta área en blanco cuando utilice solamente una tarjeta de interfaz cableada, o utilice una tarjeta inalámbrica. Establezca este valor en interfaz de escucha de daemon SNMP para seguridad; solo la interfaz especificada en el sistema puede acceder a ThinPro mediante SNMP. **NOTA:** Si este área está en blanco, el agente está escuchando todas las interfaces de red.
root/snmp/agentBehaviour/communityList/{UUID}/ communityName	Nombre de la comunidad; solo el nombre de la comunidad especificado puede acceder a ThinPro.

Tabla E-52 SNMP (continúa)

Clave de registro	Descripción
root/snmp/agentBehaviour/communityList/{UUID}/ permission	Se ha especificado un permiso de la comunidad. La opción de solo lectura permite únicamente obtener la información del sistema y la opción de lectura y escritura permite cambiar la configuración de ThinPro.
root/snmp/agentBehaviour/communityList/{UUID}/ accessibleOID	Solo es posible acceder a un inicio de OID con este valor.

Índice