



Guía del administrador

HP ThinPro 6.2

© Copyright 2017 HP Development Company, L.P.

Citrix y XenDesktop son marcas comerciales de Citrix Systems, Inc. y/o una o más de sus subsidiarias y pueden estar registradas en la Oficina de Patentes y Marcas Registradas de los Estados Unidos y en otros países. Linux® es la marca comercial registrada de Linus Torvalds en los EE. UU. 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. UNIX es una marca comercial registrada de The Open Group. VMware y Horizon 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 para los productos y servicios de HP están estipuladas en las declaraciones expresas de garantía que acompañan a dichos productos y servicios. La información contenida en este documento no debe interpretarse como una garantía adicional. HP no se responsabilizará por errores técnicos o de edición ni por omisiones contenidas en el presente documento.

Primera edición: agosto de 2017

Número de referencia del documento: 940268-E51

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: <ftp://ftp.hp.com/pub/tcdebian/pool/thinpro620/>.

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`.

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

Tabla de contenido

1 Pasos iniciales	1
Obtener más información	1
Elegir una configuración de SO	1
Elegir un servicio de administración remota	3
Iniciar el thin client por primera vez	3
Alternar entre el modo administrador y el modo usuario	3
2 Descripción general de la GUI	4
Escritorio	4
Barra de tareas	5
Administrador de conexión (solo en ThinPro)	7
3 Configuración de la conexión	8
Ajustes de conexión avanzada	8
Modo quiosco	9
4 Tipos de conexión	10
Citrix	10
Ajustes generales de Citrix	10
Opciones	10
Recursos locales	11
Ventana	11
Firewall	12
Accesos directos del teclado	12
Sesión	13
Ajustes por conexión de Citrix	14
Conexión	14
Configuración	14
Avanzada	15
RDP	15
Ajustes generales de RDP	15
Ajustes por conexión RDP	16
Red	16
Servicio	16
Ventana	17
Opciones	18

Recursos locales	19
Experiencia	19
Diagnóstico	20
Avanzada	20
RemoteFX	20
Sesiones con varios monitores de RDP	21
Redirección de multimedia de RDP	21
Redirección de dispositivo de RDP	22
Redirección de USB de RDP	22
Redirección de almacenamiento masivo en RDP	22
Redirección de impresora de RDP	23
Redirección de audio de RDP	23
Redirección de smart card de RDP	25
VMware Horizon View	25
Ajustes de VMware Horizon View por conexión	25
Red	25
General	26
Seguridad	26
Opciones RDP	27
Experiencia RDP	28
Avanzada	29
Sesiones con varios monitores de VMware Horizon View	29
Accesos directos del teclado de VMware Horizon View	29
Redirección de multimedia de VMware Horizon View	29
Redirección de dispositivo de VMware Horizon View	29
Redirección de USB de VMware Horizon View	29
Redirección de almacenamiento masivo de VMware Horizon View	30
Redirección de impresora de VMware Horizon View	30
Redirección de audio de VMware Horizon View	30
Redirección de smart card de VMware Horizon View	31
Redirección de cámara web de VMware Horizon View	31
Cambio del protocolo de VMware Horizon View	31
HTTPS y requisitos de administración de certificados de VMware Horizon View	32
Web Browser	33
Ajustes generales de Web Browser	33
Configuraciones de Web Browser por conexión	33
Configuración	33
Avanzada	34
Tipos de conexión adicionales (solo en ThinPro)	34
TeemTalk	34
Configuración	34

Asistente de sesión de TeemTalk	34
Avanzada	36
XDMCP	36
Configuración	36
Avanzada	36
SSH	36
Configuración	36
Avanzada	37
Telnet	37
Configuración	37
Avanzada	37
Custom	37
Configuración	38
Avanzada	38
5 HP True Graphics	39
Requisitos con respecto al servidor	39
Requisitos con respecto al cliente	39
Configuración del lado del cliente	39
Ajustes de compresión	39
Ajustes de la ventana	40
Limitaciones de hardware y disposición del monitor	40
Activación de HP True Graphics para varios monitores en el HP t420	40
Consejos y mejores prácticas	41
6 Integración de Active Directory	42
Pantalla de inicio de sesión	42
Inicio de sesión único	42
Escritorio	43
Bloquear la pantalla	43
Modo de administrador	43
Configuraciones y usuario del dominio	43
7 Panel de control	44
Periféricos	44
Agrupamiento de cliente	45
Configuración del agrupamiento de cliente	46
Configurar los clientes de agrupamiento	46
Configurar el servidor de agrupamiento	47
Preferencias de pantalla	47

Configuración de impresoras	48
Redirección de dispositivos USB	48
Configuración	49
Ajustes de la red	49
Ajustes para la red cableada	50
Ajustes para la red inalámbrica	50
Configuración de DNS	52
Reglas de IPSec	53
Configuración de los ajustes de VPN	53
Configuración de HP Velocity	53
Configuraciones de seguridad	54
Cuentas locales	54
Encriptación	54
Opciones	55
Centro de personalización	55
Administración	56
Administrador de componentes	56
Eliminación de componentes	57
Deshacer un cambio	57
Aplicar los cambios de forma permanente	57
Configuración de Active Directory	58
Ficha de Estado	58
Ficha Opciones	58
HP ThinState	59
Administración de una imagen de HP ThinPro	59
Capturar una imagen de HP ThinPro en un servidor FTP	59
Implementación de una imagen de HP ThinPro usando FTP o HTTP	59
Capturar una imagen de HP ThinPro en una unidad flash USB	60
Implementación de una imagen de HP ThinPro con una unidad flash USB	60
Administración de un perfil de cliente	61
Guardar un perfil de cliente en un servidor FTP	61
Restauración de un perfil de cliente usando FTP o HTTP	61
Guardar un perfil de cliente en una unidad flash USB	61
Restaurar un perfil de cliente desde una unidad flash USB	62
Duplicación VNC	62
Avanzada	63
Certificados	63
Administrador de certificados	63
Administrador de SCEP	64
Opciones DHCP	64

8 Información del sistema	65
9 HP Smart Client Services	66
Sistemas operativos compatibles	66
Requisitos previos para HP Smart Client Services	66
Obtención de HP Smart Client Services	67
Visualización del sitio web de Actualización automática	67
Creación de un perfil de Actualización automática	67
Perfiles específicos de la dirección MAC	67
Actualizar thin clients	68
Uso del método de actualización por transmisión	68
Uso del método de actualización de la etiqueta DHCP	68
Ejemplo de realización de etiquetado DHCP	68
Uso del método de actualización mediante alias de DNS	69
Uso del método de actualización manual	69
Realización de una actualización manual	69
10 Profile Editor	71
Abrir Profile Editor	71
Carga de un perfil de cliente	71
Personalización del perfil de cliente	71
Selección de la plataforma para un perfil de cliente	71
Configuración de una conexión predeterminada para un perfil de cliente	72
Modificación de las configuraciones de registro de un perfil de cliente	72
Agregar archivos a un perfil de cliente	72
Agregar un archivo de configuración a un perfil de cliente	72
Agregar certificados a un perfil de cliente	73
Agregar un enlace simbólico a un perfil de cliente	73
Guardar el perfil de cliente	74
Configuración de impresora en serie o paralela	74
Cómo obtener los ajustes de la impresora	74
Configuración de los puertos de la impresora	74
Instalación de impresoras en el servidor	75
11 Solución de problemas	76
Solución de problemas de conectividad de red	76
Solución de problemas sobre expiración de contraseñas de Citrix	76
Uso de los diagnósticos del sistema para solucionar problemas	77
Guardar los datos de diagnóstico del sistema	77
Descompresión de los archivos de diagnóstico del sistema	77

Descompresión de los archivos de diagnóstico del sistema en sistemas basados en Windows	77
Descompresión de los archivos de diagnóstico del sistema en sistemas basados en Linux o Unix	77
Visualización de los archivos de diagnóstico del sistema	77
Visualización de archivos en la carpeta Comandos	77
Visualización de archivos en la carpeta var/log	78
Visualización de archivos en la carpeta /etc	78

Apéndice A Actualizaciones desde una unidad USB 79

HP ThinUpdate	79
---------------------	----

Apéndice B Herramientas del BIOS (solo thin clients de escritorio) 80

Herramienta de ajustes del BIOS	80
Herramienta de copia del BIOS	80

Apéndice C Cambiar el tamaño de la partición de la unidad flash 81

Apéndice D Claves de registro 82


Audio	82
CertMgr	83
ComponentMgr	83
ConnectionManager	83
ConnectionType	84
custom	84
firefox	87
freerdp	92
ssh	102
teemtalk	107
telnet	110
view	113
xdmcp	122
xen	126
DHCP	139
Dashboard	139
Display	140
Domain	142
Network	143
Power	154
SCIM	155

ScepMgr	155
Search	156
Serial	157
SystemInfo	158
TaskMgr	158
USB	158
auto-update	159
background	161
config-wizard	162
desktop	163
entries	163
keyboard	164
logging	165
login	165
mouse	166
restore-points	166
screensaver	166
security	168
shutdown	168
sshd	169
time	169
touchscreen	170
translation	171
usb-update	171
users	172
vncserver	174

Índice	178
---------------------	------------


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 [Elegir 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 55](#).

Obtener más información

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

Recurso	Índice de contenido
Sitio web de soporte de HP http://www.hp.com/support	Guías del administrador, guías de referencia de hardware, informes técnicos 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

Elegir 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 55](#)).

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 9](#).

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

Configuración de SO	Tipos de conexión disponibles predeterminados
ThinPro	<ul style="list-style-type: none"> • Citrix® • RDP • VMware® Horizon® View™ • Web Browser (Firefox) • TeamTalk • XDMCP • SSH • Telnet • Custom
Smart Zero	<ul style="list-style-type: none"> • Citrix • RDP • VMware Horizon View • Web Browser (Firefox)

Elegir 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 66](#). Para descargar HP Smart Client Services, vaya al sitio web de soporte de HP (consulte [Obtener más información en la página 1](#)).

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. Cuando termina el programa de configuración, si no hay conexiones configuradas, se abre un asistente para ayudarlo a configurar una conexión.

-  **SUGERENCIA:** Si quiere modificar la configuración de un único thin client y luego copiar e implementar la configuración en otros thin clients, use primero el Panel de control para alterar la configuración. Para obtener más información, consulte [Descripción general de la GUI en la página 4](#) o [Panel de control en la página 44](#) y luego implemente la configuración usando HPDM o HP ThinState. Para obtener más información sobre HP ThinState, consulte [HP ThinState en la página 59](#).

Alternar entre el modo administrador y el modo usuario


- ▲ Haga clic con el botón derecho en el escritorio y luego seleccione **Cambio de modo Administrador/Usuario** en el menú.

Para obtener más información sobre el escritorio, consulte [Escritorio en la página 4](#).

O bien:

Seleccione **Cambio de modo Administrador/Usuario** en el Panel de control.


Para obtener más información sobre el Panel de control, consulte [Barra de tareas en la página 5](#) y [Panel de control en la página 44](#).

-  **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 Descripción general de la GUI

Escritorio

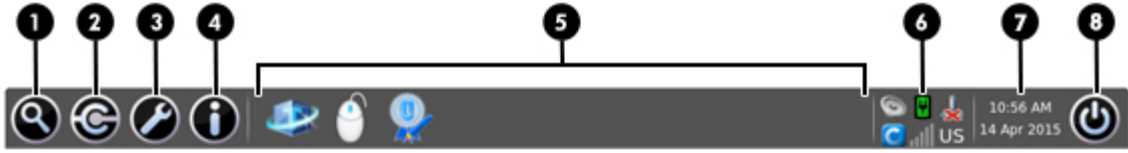
 **NOTA:** La siguiente imagen muestra el escritorio de ThinPro con una configuración local para los EE. UU. En el caso de Smart Zero, la barra de tareas es vertical y viene alineada a la derecha de forma predeterminada; además, el tema del escritorio varía según el tipo de conexión. El formato de la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



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.
(3) Barra de tareas	Brinda acceso rápido a programas y funciones del sistema (consulte Barra de tareas en la página 5 para obtener más información).

Barra de tareas


NOTA: La siguiente imagen muestra 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.



Elemento	Descripción
(1) Buscar	Le permite buscar y ejecutar las conexiones configuradas, los administradores de conexión, los elementos del Panel de control y las funciones de energía.
(2) Administrador de conexión	<p>En ThinPro, este botón abre el Administrador de conexión en una nueva ventana. Consulte Administrador de conexión (solo en ThinPro) en la página 7 para obtener más información.</p> <p>En Smart Zero, este botón muestra un menú que le permite agregar o editar una conexión.</p>
(3) Panel de control	Le permite configurar el thin client, alternar entre el modo administrador y el modo usuario y buscar actualizaciones de software. Consulte Panel de control en la página 44 para obtener más información.
(4) Información del sistema	Le permite ver la información del sistema, de la red y del software del thin client. Consulte Información del sistema en la página 65 para obtener más información.
(5) Área de aplicación	<p>Muestra los iconos de las aplicaciones abiertas en el momento.</p> <p>SUGERENCIA: Puede mantener presionadas las teclas Ctrl+Alt y luego presionar Tab varias veces para seleccionar una aplicación y que aparezca en primer plano.</p>
(6) Bandeja del sistema	<p>Brinda acceso rápido o información acerca de ciertas funciones y servicios. Entre los elementos de la bandeja del sistema pueden incluirse los siguientes (es posible que algunos elementos no aparezcan según la configuración del sistema):</p> <ul style="list-style-type: none"> • Mezclador de audio • Teclado virtual • Estado de la red: puede seleccionar 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. • Estado de Actualización automática: un icono verde con una marca de verificación indica que Actualización automática concluyó correctamente. Un icono amarillo con un signo de exclamación indica que no se encontró el servidor de Actualización automática o que hay algunos problemas con la configuración del lado del servidor. Un icono rojo con una X indica que Actualización automática falló, por ejemplo, cuando un paquete o un perfil es inválido. Un icono azul con una flecha que gira indica que Actualización automática está buscando actualizaciones. • Controles de Smart Common Input Method (SCIM) • Icono de conexiones Citrix • Icono de la batería: para abrir el Administrador de energía, haga clic con el botón derecho en este icono y seleccione Ajustar configuraciones de energía.

Elemento	Descripción
(7) Fecha y hora	Muestra la fecha y la hora actuales y abre las configuraciones de fecha y hora.
(8) Botón de inicio/apagado	Le permite cerrar sesión, reiniciar o apagar el thin client.

Administrador de conexión (solo en ThinPro)

 **NOTA:** La siguiente imagen muestra el Administrador de conexión con una configuración local para los EE.UU.



Elemento		Descripción
(1)	Lista de conexiones	Enumera las conexiones configuradas y especifica si cada conexión está activa o inactiva.
(2)	Iniciar	Inicia la conexión seleccionada.
(3)	Detener	Detiene la conexión seleccionada.
(4)	Editar	Le permite editar la conexión seleccionada.
(5)	Eliminar	Elimina la conexión seleccionada.
(6)	Añadir	Le permite agregar una nueva conexión. NOTA: Consulte Elegir una configuración de SO en la página 1 para ver una lista de los tipos de conexión disponibles.
(7)	Ajustes	Le permite editar los ajustes generales de las conexiones Citrix, RDP o Web Browser. Estos ajustes se aplican a todas las conexiones de ese tipo.

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

- [Configuración de la conexión en la página 8](#)
- [Tipos de conexión en la página 10](#)

3 Configuración de la conexión

Ajustes de conexión avanzada

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




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

Opción	Descripción
Conexión de seguridad	<p>Especifica la conexión de seguridad. Si la conexión no se arranca, la conexión de seguridad intentará iniciarse en su lugar.</p> <p>NOTA: Esta opción no está disponible para el tipo de conexión VMware Horizon View.</p>
Prioridad de inicio automático	<p>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.</p>
Compartir las credenciales con el protector de pantalla	<p>Permite que los usuarios desbloqueen el protector de pantalla local usando sus credenciales para dicha conexión.</p> <p>NOTA: Esta opción solo está disponible para los tipos de conexión Citrix, RDP y VMware Horizon View.</p>
Reconexión automática	<p>Si la opción está activada y la conexión se interrumpe, esta conexión intentará volverse a conectar de forma automática.</p> <p>NOTA: Si detiene una conexión mediante el Administrador de conexión no funcionará la reconexión automática.</p>
Esperando por red antes de conectar	<p>Desactive esta opción si su conexión no necesita una red para iniciarse o si no desea esperar la red para iniciar la conexión.</p>
Mostrar icono en escritorio	<p>Si está activada, se creará un icono de escritorio para esta conexión.</p>
Permitir al usuario iniciar esta conexión	<p>Si está activada, un usuario final puede iniciar esta conexión.</p>
Permitir al usuario editar esta conexión	<p>Si está activada, un usuario final puede modificar esta conexión.</p>
Opciones del cuadro de diálogo de inicio de sesión	<p>Active o desactive estas opciones para configurar el cuadro de diálogo de inicio de sesión para la conexión.</p> <p>NOTA: Esta opción solo está disponible para los tipos de conexión Citrix, RDP y VMware Horizon View.</p> <p>Se encuentran disponibles las siguientes opciones:</p> <ul style="list-style-type: none">● Mostrar campo de nombre de usuario● Mostrar campo de contraseña● Mostrar el campo dominio● Mostrar casilla de verificación "Recordarme" <p>NOTA: Esta opción guarda el nombre de usuario y el dominio, pero la contraseña debe introducirse cada vez.</p>

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 55](#)) 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.
- Restablecer 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 con el 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 las credenciales con el protector de pantalla**, si está disponible.
 - Para una conexión Web Browser únicamente, seleccione la opción **Habilitar 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**.

4 Tipos de conexión

Citrix

La siguiente tabla describe los backends admitidos de Citrix XenApp.

Tipo de acceso	Versión de XenApp
Direct (heredado)	4.5 / 5 / 6 / 6.5
PNAgent (heredado)	4.5 / 5 / 6 / 6.5 / 7.X
Web browser	4.5 / 5 / 6 / 6.5 / 7.X
StoreFront	4.5 / 5 / 6 / 6.5 / 7.X

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

Tipo de acceso	Versión de XenApp
PNAgent (heredado)	4.5 / 5.5 / 5.6.5 / 7.X
Web browser	4.5 / 5.5 / 5.6.5 / 7.X
StoreFront	4.5 / 5.5 / 5.6.5 / 7.X

La siguiente tabla describe los backends admitidos de Citrix VDI-in-a-box.

Tipo de acceso	Versión de XenApp
PNAgent (heredado)	5.x
Web browser	5.x
StoreFront	5.x

Ajustes generales de Citrix

 **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.

Opción	Descripción
Habilitar HDX MediaStream	Activa HDX MediaStream.
Habilitar MultiMedia	Activa multimedia

Opción	Descripción
Habilitar la barra de conexión	Activa la barra de conexión.
Habilitar la Reconexión automática	Permite la reconexión automática de conexiones interrumpidas.
Habilitar la confiabilidad de la sesión	Activa el recurso Confiabilidad de la sesión de Citrix. Consulte la documentación de Citrix para obtener más información.
Habilitar la redirección del portapapeles	Activa la redirección del portapapeles.
Usar la compresión de datos	Utiliza compresión de datos para esta conexión.
Habilitar la compresión 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.
Habilitar Pegar con el botón central	Habilita la función de pegar del botón central del mouse.
Cadena de Agente de usuario	Especifica una secuencia de Agente de usuario 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.
Nivel de encriptación	Especifica el nivel de encriptación de una sesión ICA.

Recursos locales

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

Opción	Descripción
Impresoras	Controla la forma en que se maneja la redirección de la impresora.
Cámara web/entrada de audio	Controla la forma en que se maneja la redirección de la entrada de audio y la cámara web local.
Redirección de USB	Activa la redirección de USB.
Asignación dinámica de unidad	Activa la asignación de unidad dinámica.
Asignación estática de unidad (heredada)	Activa la asignación de unidad estática, lo que le permite especificar las asignaciones de unidad a rutas locales.

Ventana

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

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 la ventana	Cuando el Modo TWI se establece en Interruptor integrado desactivado se controla el tamaño predeterminado de la ventana.

Opción	Descripción
Colores predeterminados de la ventana	Establece la profundidad de color predeterminada.
Monitor izquierdo	Cuando está desactivado Mostrar el Escritorio virtual en todos los monitores , estos campos le permiten especificar cómo aparece el escritorio virtual en monitores específicos.
Monitor derecho	
Monitor superior	
Monitor inferior	

Firewall

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

Opción	Descripción
Tipo de proxy	Especifica el tipo de proxy.
Dirección proxy	La dirección IP del servidor proxy.
Puerto proxy	El puerto para conexión al servidor proxy.
Usuario	El nombre de usuario que se va a utilizar para conexión al servidor proxy.
Contraseña	La contraseña que se va a utilizar para conexión al servidor proxy.
Usar dirección alternativa para la conexión del firewall	El Citrix ICA Client solicitará la dirección alterna definida para el servidor cuando se comunique con servidores dentro del firewall. La dirección alterna debe especificarse para cada servidor en una granja de servidores.

Accesos directos del teclado

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

Opción	Descripción
Habilitar UseLocalIM	Utiliza el método de entrada local para interpretar la entrada de teclado. Esto solo es compatible con los idiomas europeos.
Usar el número de EUKS	Controla el uso de Extended Unicode Keyboard Support (EUKS) en servidores Windows. Las opciones válidas se describen a continuación: <ul style="list-style-type: none"> • 0: EUKS no se utiliza. • 1: EUKS se utiliza como recurso alternativo. • 2: EUKS se utiliza cuando es posible.
Manipulación de los accesos directos del teclado	Especifica cómo deben manejarse los accesos directos del teclado. Las siguientes configuraciones están disponibles: <ul style="list-style-type: none"> • Traducido: los accesos directos del teclado se aplican al escritorio local (lado del cliente) • Directo solo en modo de 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

Opción	Descripción
	<ul style="list-style-type: none"> 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 la manipulación directa del teclado	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.

Opción	Descripción
Demora del cierre de sesión automático antes del inicio de 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 del cierre de sesión automático después del cierre de 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.
Tiempo de espera de comprobación 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.

Ajustes por conexión de Citrix



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

Conexión

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

Opción	Descripción
Nombre	El nombre de la conexión.
Modo de conexión	Establece el modo de conexión en una de las siguientes opciones: <ul style="list-style-type: none">• PNAgent• StoreFront• Direct <p>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.</p> <p>NOTA: Puede probar los ajustes de conexión al seleccionar el botón Probar la conexión.</p>
URL	Nombre de host o dirección IP del servidor Citrix. Si está configurando una conexión a un servidor en un sitio HTTPS, introduzca el FDQN del sitio y el certificado de 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 el certificado	Omite la verificación del certificado del servidor Citrix.
Credenciales	Establece el modo de autenticación en una de las siguientes opciones: <ul style="list-style-type: none">• 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.

Opción	Descripción
Reconectar automáticamente aplicaciones al iniciar sesión	<p>Con esta opción seleccionada, los recursos que estaban abiertos la última vez que el usuario terminó la sesión se vuelven a abrir cuando se arranca sesión nuevamente.</p> <p>SUGERENCIA: Si no está utilizando el recurso SmoothRoaming de Citrix, desactive esta opción para aumentar la velocidad de su conexión.</p>
Modo de inicio automático	<p>Le permite establecer que un escritorio o una aplicación específica se inicien de forma automática cuando se arranca la conexión de Citrix. Si se establece en Iniciar automáticamente un único recurso y, hay un único recurso publicado, ese recurso se arranca de forma automática.</p> <p>NOTA: Esta opción queda sin efecto si se selecciona Reconectar automáticamente aplicaciones al iniciar sesión y hay aplicaciones a las que es posible reconectarse.</p> <p>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 el Administrador de conexiones de Citrix, lo que le permite seleccionar los recursos automáticamente tras la conexión.</p> <p>Si seleccionó Inicio automático de un solo recurso, seleccione el botón Enumeración para recuperar la cantidad de recursos. Si hay un único recurso, se arranca automáticamente tras la conexión.</p>
Mostrar recursos en el escritorio	Con esta opción seleccionada, los recursos remotos de la conexión se mostrarán en el escritorio local de ThinPro.
Mostrar recursos en la barra de tareas	Con esta opción seleccionada, los recursos remotos de la conexión se mostrarán en la barra de tareas local de ThinPro.
Mostrar solo los recursos suscritos	Si se selecciona, solo se muestran los recursos suscritos durante una conexión de Citrix.

Avanzada



NOTA: Consulte [Ajustes de conexión avanzada en la página 8](#) para obtener información sobre los ajustes disponibles en la categoría Avanzada 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 generales de RDP

La siguiente tabla describe los ajustes generales de RDP.



NOTA: Estos ajustes afectan todas las conexiones de RDP.

Opción	Descripción
Enviar nombre de host como	Especifica si desea enviar al sistema remoto el nombre de host o dirección MAC del thin client como nombre de host especificado.
Activar la redirección multimedia	Permite redirigir contenido multimedia.

Ajustes por 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.

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 <code>https://</code> . De forma predeterminada, esto se agrega automáticamente tal y como lo especifica la clave de registro de <code>rdWebFeedUrlPattern</code> , que define el patrón de la URL.
Credenciales	<ul style="list-style-type: none">• 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 puerta de enlace.
Exploración de 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.

Opción	Descripción
Servicio	Establece el servicio de RDP para una de las siguientes opciones: <ul style="list-style-type: none">• 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:<ul style="list-style-type: none">• Si se establece el Modo en Aplicación remota, el campo Aplicación especifica la ruta de la aplicación que se va a ejecutar.

Opción	Descripción
	<p>SUGERENCIA: Si utiliza el modo Windows RDP continuo, escriba la ruta <code>seamlessrdpshell.exe</code> en su servidor, seguido de un espacio y luego la ruta de la aplicación que va a ejecutar. Consulte el siguiente ejemplo:</p> <pre>c:\seamless\seamlessrdpshell.exe c:\Program Files\Microsoft\Word.exe</pre> <ul style="list-style-type: none"> 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 <code>Word.exe</code>. <p>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 <code>C:\Program Files\Microsoft</code>.</p> <ul style="list-style-type: none"> 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 arranca cuando se selecciona un recurso. Las siguientes opciones adicionales están disponibles para RD Web Access: <ul style="list-style-type: none"> Dejar 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 disponible: con esta opción seleccionada, y si hay un único recurso publicado, ese recurso se iniciará automáticamente tras la conexión. Filtro de recursos y Explorador de canal web: pueden usarse para limitar los recursos remotos que se pondrán a la disposición del usuario en la ventana de selección de recursos. <p>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.</p> <p>Para obtener más información, consulte el informe técnico sobre HP ThinPro «<i>RD Web Access Deployment Example</i>» (disponible solo en inglés).</p>

Ventana

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

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.
Tamaño de la ventana	Ajusta el tamaño de la ventana a completo , fijo o porcentaje .
Tamaño de porcentaje	Si Tamaño de la ventana se establece como porcentaje , esta opción establece el porcentaje de la pantalla que ocupa una ventana del escritorio.
	<p>NOTA: Los tamaños resultantes podrían redondearse.</p> <p>NOTA: RemoteFX admite solo una lista fija de resoluciones.</p>
Tamaño fijo	Si Tamaño de la 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.

Opción	Descripción
Permitir eventos de movimiento	Si está activado, los movimientos del mouse se transmiten continuamente al servidor RDP.
Habilitar la compresión de datos	Activa la compresión masiva de datos entre el servidor de RDP y el cliente de RDP.
Habilitar encriptación RDP obsoleta	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 administrativa	Establece la conexión con el puerto de consola de administrador.
Copiar/pegar sesión cruzada	Si está activado, las opciones copiar y pegar están activadas entre diferentes sesiones RDP.
Activar almacenamiento en búfer de primitivos 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.
Política de verificación de certificados	Seleccione una de las siguientes opciones: <ul style="list-style-type: none">● Aceptar todos los certificados de servidor RDP● Usar los hosts recordados; avisar en caso de certificado desconocido o no válido● Omitir hosts recordados; avisar en caso de certificado desconocido o no válido● Conectarse solo a servidores RDP preaprobados
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.
Nombre de host para 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 ? al lado de esta opción para obtener más información.
Información del equilibrio de carga	Utilice esta opción con una conexión RDP intermediada. SUGERENCIA: Seleccione el icono ? al lado de esta opción para obtener más información.



NOTA: Para obtener más información sobre las opciones **Habilitar encriptación RDP obsoleta** 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 (USB). Para obtener más información, consulte el informe técnico sobre HP ThinPro «*USB Manager*» (disponible solo en inglés).

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 en serie/paralelos	Determinan si los puertos seriales y paralelos están redirigidos o desactivados para esta conexión.
Almacenamiento USB	Determina si los dispositivos de almacenamiento USB, como las unidades flash y ópticas, están redirigidos por una redirección de almacenamiento de alto nivel o una redirección USB de bajo nivel, o si están desactivados para esta conexión.
Particiones locales	Determinan si las particiones locales de la unidad flash del thin client están redirigidas o desactivadas para esta conexión.
Otros dispositivos USB	Determinan si otras clases de dispositivos USB (como cámaras web y tablets) están redirigidas por redirección USB de nivel bajo, o si están desactivadas para esta conexión.

Experiencia

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

Opción	Descripción
Seleccione la velocidad de su conexión para optimizar el rendimiento	<p>Si selecciona una velocidad de conexión (LAN, Banda ancha o Módem) activará o desactivará las siguientes opciones para optimizar el rendimiento:</p> <ul style="list-style-type: none">• Fondo de escritorio• Suavizado de fuentes• Composición del escritorio• Mostrar contenido de la ventana al arrastrar• Animación de menús y ventanas• Temas <p>La selección de Configuración preferida del cliente permite que el cliente de RDP elija qué opciones utilizará para proporcionar la mejor experiencia de RDP.</p> <p>También puede seleccionar su propia combinación personalizada de opciones.</p>
Controlar el estado de la conexión de extremo a extremo	<p>Seleccione esta alternativa para activar las opciones de intervalo de espera.</p> <p>NOTA: Para obtener más información, consulte el informe técnico sobre HP ThinPro «<i>RDP Connection Drop Detection</i>» (disponible solo en inglés).</p>

Opción	Descripción
Tiempo de espera de advertencia	<p>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.</p> <p>Con la opción Mostrar cuadro de 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.</p> <p>SUGERENCIA: HP recomienda que aumente el valor del tiempo de espera para redes con períodos muy ocupados o interrupciones momentáneas frecuentes.</p>
Tiempo de espera para recuperación	<p>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.</p>
Tiempo de espera para error	<p>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.</p> <p>SUGERENCIA: Seleccione el icono ? al lado de este campo para obtener más información.</p>

Diagnóstico

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

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

Avanzada



NOTA: Consulte [Ajustes de conexión avanzada en la página 8](#) para obtener información sobre los ajustes disponibles en la categoría Avanzada 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 obtener 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) compatible con 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.

Para desactivar MMR en el thin client en todas las conexiones RDP, establezca la siguiente clave de registro en 0:

```
root/ConnectionType/freerdp/general/enableMMR
```

Como RemoteFX ya ofrece un rendimiento multimedia aceptable, puede desactivar MMR con RemoteFX si establece la siguiente clave de registro en 1:

```
root/ConnectionType/freerdp/connections/<UUID>/disableMMRwithRFX
```

 **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.

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 reintente 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 ya instalada en ese host remoto. No hay ningún ajuste que administrar localmente.
- **Redirección de alto nivel:** si la redirección 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.

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 RDP necesita especificar al host remoto cuál controlador 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.



NOTA: Consulte [Configuración de impresora en serie o paralela en la página 74](#) 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 video nativos disponibles en RDP. Es posible que los videos más largos no se sincronicen con el audio. MMR o Remotefx pueden resolver este problema.
- HP recomienda la redirección de audio de alto nivel, pero la redirección USB de dispositivos de 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

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

Para activar el inicio de sesión de smart card para una conexión RDP:

- ▲ Seleccione **Permitir inicio de sesión a través de Smart Card** 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 smart card.

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



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.

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	<ul style="list-style-type: none">● 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.

Opción	Descripción
Inicio de sesión automático	Cuando está activado, el usuario inicia sesión automáticamente cuando se establece la conexión. NOTA: HP recomienda activar esta opción.
Permitir inicio de sesión a través de Smart Card	Permitir iniciar sesión con Smartcard. NOTA: Para obtener más información acerca de las smart cards, consulte Redirección de smart card de VMware Horizon View en la página 31 .
No inicie la aplicación maximizada	Si está activada, las aplicaciones no se inician en ventanas maximizadas.
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 .

Seguridad

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

Opción	Descripción
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 diseñado 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 de cerrar una sesión y no desean volver a pasar por el proceso de inicio de sesión completo.
Ocultar barra de menú superior	La barra de menú superior se torna invisible para los usuarios. Esta opción está 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.
Nivel de seguridad de la conexión	Utilice la opción Nivel de seguridad de la conexión para ajustar el nivel de seguridad que utiliza el cliente de VMware Horizon View al conectarse al servidor. NOTA: Para obtener más información, consulte HTTPS y requisitos de administración de certificados de VMware Horizon View en la página 32 para obtener detalles sobre cómo se comportan los niveles de seguridad de la conexión.

Opciones RDP

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

Opción	Descripción
Habilitar las acciones de movimiento	Permite eventos de movimiento para esta conexión.
Habilitar la compresión de datos	Utiliza compresión de datos para esta conexión.
Habilitar encriptación RDP obsoleta	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 administrativa	Establece la conexión con el puerto de consola de administrador.
Copiar/pegar sesión cruzada	Si está activado, las opciones copiar y pegar están activadas entre diferentes sesiones RDP.
Activar almacenamiento en búfer de primitivos 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.
Política de verificación de certificados	Seleccione una de las siguientes opciones: <ul style="list-style-type: none">● Aceptar todos los certificados de servidor RDP● Usar los hosts recordados; avisar en caso de certificado desconocido o no válido● Omitir hosts recordados; avisar en caso de certificado desconocido o no válido● Conectarse solo a servidores RDP preaprobados
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.
Nombre de host para 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 ? al lado de esta opción para obtener más información.
Información del equilibrio de carga	Utilice esta opción con una conexión RDP intermediada. SUGERENCIA: Seleccione el icono ? al lado de esta opción para obtener más información.
Sonido del equipo remoto	Especifica dónde debe reproducirse el sonido del equipo remoto (de forma local o remota) o si no se debe reproducir en absoluto.
Habilitar asignación de dispositivos	Asigna los puertos en serie y paralelos del thin client a la sesión remota.
Habilitar asignación de impresoras	Asigna la cola de impresión 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.

Opción	Descripción
	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.

Opción	Descripción
Habilitar MMR	Permite redirigir contenido multimedia.
Seleccione la velocidad de su conexión para optimizar el rendimiento	<p>Si selecciona una velocidad de conexión (LAN, Banda ancha o Módem) activará o desactivará las siguientes opciones para optimizar el rendimiento:</p> <ul style="list-style-type: none"> • Fondo de escritorio • Suavizado de fuentes • Composición del escritorio • Mostrar contenido de la ventana al arrastrar • Animación de menús y ventanas • Temas <p>Al seleccionar Configuración preferida del cliente, el cliente de VMware Horizon View puede elegir qué opciones utilizar.</p> <p>También puede seleccionar su propia combinación personalizada de opciones.</p>
Controlar el estado de la conexión de extremo a extremo	Seleccione esta alternativa para activar las opciones de intervalo de espera.
Tiempo de espera de advertencia	<p>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.</p> <p>Con la opción Mostrar cuadro de 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.</p> <p>SUGERENCIA: HP recomienda que aumente el valor del tiempo de espera para redes con períodos muy ocupados o interrupciones momentáneas frecuentes.</p>
Tiempo de espera para 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.
Tiempo de espera para error	<p>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.</p> <p>SUGERENCIA: Seleccione el icono ? al lado de este campo para obtener más información.</p>

Avanzada



NOTA: Consulte [Ajustes de conexión avanzada en la página 8](#) para obtener información sobre los ajustes disponibles en la categoría Avanzada 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 VMware predeterminadas utilizan pantalla completa y abarcan todos los monitores. Para elegir otro tamaño de ventana diferente, seleccione **Pantalla completa - Todos los monitores** en el tipo de protocolo del grupo de escritorios para la conexión y luego elija otra opción en la lista de tamaños de ventana. La próxima vez que se conecte a una sesión se abrirá la ventana en el tamaño seleccionado.

Accesos directos del teclado de VMware Horizon View

Accesos directos del teclado de Windows

A fin de ayudar a administrar los sistemas Windows, VMware Horizon View es compatible con los accesos directos del 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 los programas multimedia como Windows Media Player.

Redirección de multimedia de VMware Horizon View

Las conexiones VMware Horizon View son compatibles con la funcionalidad MMR cuando se utilizan con el protocolo RDP de Microsoft.

Para obtener más información, consulte [Redirección de multimedia de RDP en la página 21](#).

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 22](#).

Redirección de almacenamiento masivo de VMware Horizon View

Debe utilizar el protocolo de conexión RDP para utilizar la redirección de almacenamiento masivo con una conexión VMware Horizon View.

Para realizar la redirección de unidades de una unidad USB o unidad SATA interna:

- ▲ Agregue `-xfreerdpoptions='/drive:$foldname,shared folder path, share device'` en la opción de argumentos de línea de comandos.

Por ejemplo, `-xfreerdpoptions='/drive:myfolder,/home/user,/dev/sda2' comparte /home/user en la unidad /dev/sda2 como myfolder en una conexión VMware Horizon View.`

Para obtener más detalles, consulte [Redirección de almacenamiento masivo en RDP en la página 22](#).

Redirección de impresora de VMware Horizon View

En el caso de las conexiones realizadas con el protocolo PCoIP en unidades x86, las impresoras pueden compartirse con USBR o redirección de la impresora de alto nivel de VMware Horizon View. Las conexiones de PCoIP en unidades ARM solo admiten la redirección de impresora USBR. En el caso de las conexiones realizadas con el protocolo RDP, consulte [Redirección de impresora de RDP en la página 23](#) para obtener más información.

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, de un set de auriculares y micrófono USB si está conectado. Utilice el administrador de audio local para ajustar el nivel de entrada/salida, seleccionar reproducción y dispositivos de captura.

El cliente de VMware Horizon View admite la redirección de grabación de audio de alto nivel solo a través del tipo de conexión de PCoIP en unidades x86 al conectarse a un servidor que ejecuta VMware Horizon View 5.2 Pack 2 o superior. Si necesita grabación de audio y está utilizando una configuración diferente, use uno de los siguientes métodos:

- Si el sistema usa VMware Horizon View Client 1.7 o superior, utilice el protocolo RDP para permitir la redirección de audio de alto nivel a través del conector de 3,5 mm o de 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 VMware Horizon View:

1. Asegúrese de que el inicio de sesión de smart card 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, escriba el PIN correspondiente para el servidor.

 **NOTA:** Después de proporcionar el PIN correcto, se utilizará junto con las credenciales del usuario para iniciar la sesión en el servidor de VMware Horizon View. Consulte la documentación de VMware Horizon View para obtener más información acerca de cómo configurar el servidor para admitir el inicio de sesión a través de smart card. Siempre que el servidor esté configurado para permitir el inicio de sesión con smart card, las credenciales del usuario lo atravesarán y se transferirán directamente y se iniciará la sesión en el escritorio sin tener que introducir su 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 25](#) 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 redirigir 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 simplemente no funcione. Consulte [Redirección de USB de RDP en la página 22](#) para obtener más información.

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.

HTTPS y requisitos de administración de certificados de VMware Horizon View

VMware Horizon View Client 1.5 y VMware Horizon View Server 5.0 y posteriores requieren HTTPS. De forma predeterminada, el cliente 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 (CA) y la CA no es de confianza, la conexión indicará un error y al usuario no se le permitirá conectar.

HP recomienda que se use en el servidor de VMware Horizon View Manager un certificado firmado, verificado por una CA de raíz estándar que sea confiable. Esto garantiza que los usuarios podrán conectarse al servidor sin que se les pida que realicen ninguna configuración. Si utiliza una CA interna, el cliente de VMware Horizon View indica un error hasta que realice una de las tareas siguientes:

- Utilice el Administrador de certificados para importar el certificado desde un archivo o URL.
- Utilice la actualización remota de perfiles para importar un certificado.
- En el Administrador de conexión VMware Horizon View, establezca el **Nivel de seguridad de la 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**.

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**.

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**.

Confianza del certificado	Resultado
De confianza	De confianza
Autofirmado	No de confianza

Confianza del certificado	Resultado
Expirado	No de confianza
No confiable	No de confianza

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

Resultado	Descripción
De confianza	Se conecta sin un diálogo de advertencia de certificado y muestra un icono de bloqueo verde
No de confianza	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

Web Browser

Ajustes generales de Web Browser

La siguiente tabla describe los ajustes generales de Web Browser.



NOTA: Estos ajustes afectan todas las conexiones de Web Browser.

Opción	Descripción
Preferencias de navegador web	Abre el cuadro de diálogo de las preferencias de Firefox.
Permitir que las conexiones gestionen sus propias configuraciones	Cuando está activado, los ajustes de Firefox se guardan para cada conexión Web Browser. De lo contrario, los ajustes se restablecen cada vez que se inicie la conexión.

Configuraciones de Web Browser por 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 los ajustes generales de Web Browser.

Opción	Descripción
Nombre	El nombre de la conexión.
URL	La URL para la conexión.
Uso planeado	Le permite establecer el uso previsto de la conexión en Citrix , RDP o Internet .
Habilitar modo quiosco	Habilita modo de quiosco.

Opción	Descripción
Habilitar pantalla completa	Utiliza el modo de pantalla completa para la conexión.
Activar cuadro de diálogo de impresión	Activa el cuadro de diálogo de impresión.

Avanzada

 **NOTA:** Consulte [Ajustes de conexión avanzada en la página 8](#) para obtener información sobre los ajustes disponibles en la categoría Avanzada al editar una conexión.

Tipos de conexión adicionales (solo en ThinPro)

 **NOTA:** De forma predeterminada, estos tipos de conexión no están disponibles en Smart Zero. Para obtener más información, consulte [Elegir una configuración de SO en la página 1](#).

TeemTalk

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

Para obtener más información acerca de HP TeemTalk, consulte la *Guía del usuario* de HP TeemTalk.

Configuración

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

Opción	Descripción
Nombre	El nombre de la conexión.
Asistente de creación de Teemtalk	Abre al asistente de sesión de TeemTalk. Consulte las otras tablas en esta sección para obtener más información.
Sonido de sistema	Permite la emisión de sonido de sistema.

Asistente de sesión de TeemTalk

La siguiente tabla describe las configuraciones disponibles en la categoría Información de conexión en el Asistente de sesión de TeemTalk.

Opción	Descripción
Nombre de sesión	El nombre de la sesión.
Transporte	El transporte de red que se va a utilizar para esta conexión. Transportes válidos son: TCP/IP, En serie, SSH2 y SSL.
Conexión	El método de conexión que se va a ser utilizado. Las opciones avanzadas de conexión pueden configurarse a través del botón.
Emulación	Los tipos de emulación son: hp70092, IBM 3151, monitor IBM3270, impresora IBM3270, monitor IBM5250, impresora IBM5250, MD prism, TA6530, Serie VT y Wyse.

La siguiente tabla describe las configuraciones disponibles en la categoría Opciones avanzadas en el Asistente de sesión de TeemTalk.

Opción	Descripción
Impresora de emulación	Configuración de la impresora de emulación de HP TeemTalk.
Inicio de sesión automático	Configuración de inicio de sesión automático de HP TeemTalk.
Macros de clave	Configuración de las macros de teclado de HP TeemTalk.
Acciones de mouse	Configuración de las acciones del mouse de HP TeemTalk.
Botones configurables	Configuración de los botones programables de HP TeemTalk.
Atributos	Configuración de atributos de HP TeemTalk.
Puertos auxiliares	Configuración de puertos auxiliares de HP TeemTalk.
Puntos de acceso	Configuración de las zonas activas de HP TeemTalk.


La siguiente tabla describe las configuraciones disponibles en la categoría Preferencias en el Asistente de sesión de TeemTalk.

Opción	Descripción
Iniciar sesión conectada	Inicia la sesión conectada.
Mostrar barra de estado	Muestra la barra de estado de la conexión.

La siguiente tabla describe las configuraciones adicionales disponibles en la categoría Preferencias en el Asistente de sesión de TeemTalk.

Opción	Descripción
Mostrar barra de configuración	Muestra la barra de configuración.
Guardar posición actual de la ventana	Guarda la posición y el tamaño actuales de la ventana al seleccionar Guardar preferencias . Se restaurará en el siguiente inicio del sistema. NOTA: Seleccione Guardar preferencias cada vez que cambie la posición o el tamaño de la ventana para guardar los nuevos valores.
Ejecutar a pantalla completa	Seleccione esta opción para que se muestre en pantalla completa y desaparezcan el marco, los botones programables, el menú y las barras de configuración. NOTA: Esta opción no surtirá efecto hasta la próxima vez que inicie el sistema y cancela las opciones Mostrar barra de configuración y Guardar posición actual de la ventana .
Comando de explorador	En el cuadro, escriba el comando que ejecuta su explorador web; por ejemplo: <code>/ show Firefox html links</code>
Opciones de inicio de línea de comandos	Utilícelo para especificar una ubicación alternativa para as opciones de inicio. NOTA: Para obtener información específica sobre las opciones de inicio en la línea de comandos de HP TeemTalk, consulte la <i>HP TeemTalk Terminal Emulator User Guide</i> (Guía del usuario de HP TeemTalk Terminal Emulator).

Avanzada

 **NOTA:** Consulte [Ajustes de conexión avanzada en la página 8](#) para obtener información sobre los ajustes disponibles en la categoría Avanzada al editar una 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.

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 visualización	Seleccione para definir la configuración de la pantalla para la conexión. Si no define esta configuración, se utilizará la configuración predeterminada.

Avanzada

 **NOTA:** Consulte [Ajustes de conexión avanzada en la página 8](#) para obtener información sobre los ajustes disponibles en la categoría Avanzada al editar una conexión.

SSH

 **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 SSH.

Opción	Descripción
Nombre	El nombre de la conexión.
Dirección	La dirección IP del sistema remoto.
Puerto	El puerto remoto que se va a utilizar para la conexión.
Nombre de usuario	El nombre de usuario que se va a utilizar para la conexión.
Ejecutar aplicación	La aplicación que se va a ejecutar para hacer la conexión.
Compresión	Seleccione esta opción si desea comprimir los datos enviados entre el servidor y el thin client.

Opción	Descripción
Envío 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 el thin client.
Forzar asignación 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.
Fuente	Las opciones válidas son: 7X14, 5X7, 5X8, 6X9, 6X12, 7X13, 8X13, 8X16, 9X15, 10X20 y 12X24.

Avanzada

 **NOTA:** Consulte [Ajustes de conexión avanzada en la página 8](#) para obtener información sobre los ajustes disponibles en la categoría Avanzada al editar una 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.

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

Avanzada

 **NOTA:** Consulte [Ajustes de conexión avanzada en la página 8](#) para obtener información sobre los ajustes disponibles en la categoría Avanzada al editar una conexión.

Custom

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.

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

Avanzada



NOTA: Consulte [Ajustes de conexión avanzada en la página 8](#) para obtener información sobre los ajustes disponibles en la categoría Avanzada al editar una conexión.

5 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).


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.

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

 **NOTA:** La información de esta sección solo corresponde a Citrix. En el caso de VMware, basta usar el protocolo 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, pueden enviarse utilizando métodos que no sean 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 40](#) 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 **Integrated Graphics** (Gráficos integrados) como **Force** (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.

6 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

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: desbloqueo de la 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.

7 Panel de control

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

 **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, seleccione el botón del Panel de control, seleccione **Configuración**, seleccione **Centro de personalización** y luego seleccione o desmarque elementos de la lista de **Aplicaciones**.

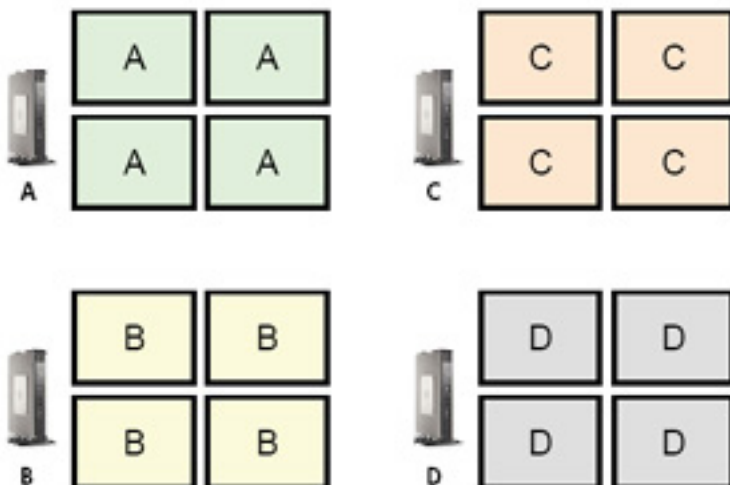
Periféricos

Opción de menú	Descripción
Agrupamiento de cliente	Le permite combinar thin clients para crear espacio adicional de pantalla. Para obtener más información, consulte Agrupamiento de cliente en la página 45 .
Preferencias de video	Le permite configurar y probar las opciones de pantalla. Para obtener más información, consulte Preferencias de pantalla en la página 47 .
Formato de teclado	Le permite cambiar la disposición del teclado para que se adapte al idioma utilizado por el teclado.
Sonido	Le permite controlar los niveles de audio de entrada y de reproducción.
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.
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 48 .
Pantalla táctil	Le permite configurar las opciones de la pantalla táctil.
Administrador de USB	Le permite configurar las opciones de redirección para los dispositivos USB. Para obtener más información, consulte Redirección de dispositivos USB en la página 48 .
Configuración de método de entrada SCIM	Le permite configurar el Smart Common Input Method (SCIM) para introducir información en coreano, japonés y chino. Para obtener más información acerca de este programa de código abierto, visite http://sourceforge.net/apps/mediawiki/scim/index.php?title=Main_Page .

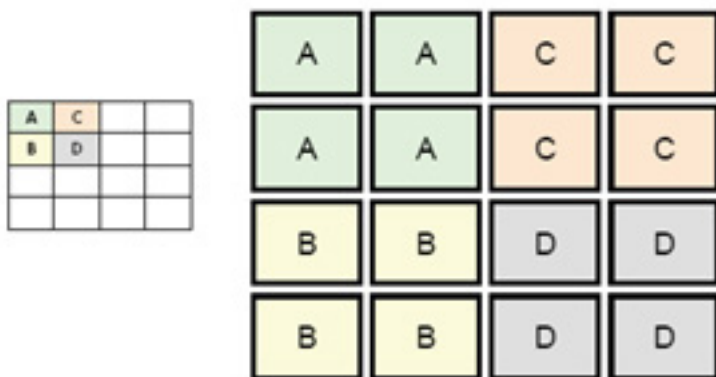
Agrupamiento de cliente

Los thin clients basados en HP ThinPro pueden admitir hasta cuatro monitores, según el modelo del hardware. Si necesita un estado real de pantalla adicional, el agrupamiento de cliente le permite combinar hasta cuatro thin clients al mismo tiempo. De esta manera, puede contar con hasta 16 monitores controlados por un único teclado y mouse, sin necesidad de ningún hardware ni software adicional.

Suponga que dispone de cuatro thin clients, cada uno con cuatro monitores configurados con una matriz de 2 x 2 como se muestra a continuación.

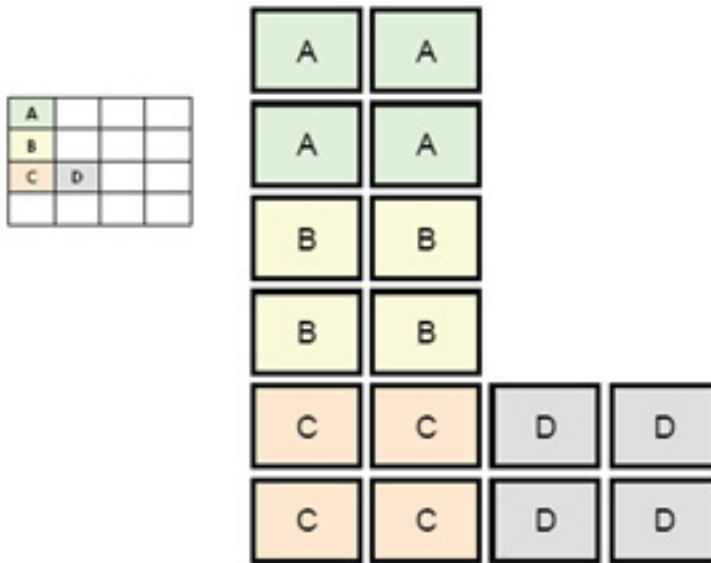


El agrupamiento de clientes le permite organizar los cuatro thin clients en una cuadrícula 4 x 4. En la ilustración siguiente se muestra una posible disposición.



Por ejemplo, al desplazar el puntero del mouse fuera de la parte lateral derecha de los monitores del thin client A, el puntero aparecerá en la parte lateral izquierda de los monitores del thin client C. Del mismo modo, las pulsaciones del teclado se redirigirán del thin client A al thin client C.

La siguiente ilustración muestra otra disposición posible.



En esta configuración, al desplazar el puntero del mouse fuera de la parte lateral derecha de los monitores del thin client A, esta aparecerá en el 1/3 superior de la parte lateral izquierda de los monitores del thin client D. Del mismo modo, al desplazar el puntero del mouse fuera de la parte lateral derecha de los monitores del thin client B, esta aparecerá en el 1/3 central de la parte lateral izquierda de los monitores del thin client D. Y, finalmente, al desplazar el puntero del mouse de la parte lateral derecha de los monitores del thin client C, esta aparecerá en el 1/3 inferior de la parte lateral izquierda de los monitores del thin client D.



NOTA: Las ventanas del escritorio no pueden extenderse ni moverse entre thin clients. Normalmente, cada thin client creará ventanas según su conexión con un equipo remoto asociado y no será necesario desplazarlas entre thin clients.

El thin client conectado físicamente al teclado y al mouse se conoce como servidor de agrupamiento. Los otros thin clients se denominan clientes de agrupamiento. Cuando el puntero del mouse está sobre uno de los clientes de agrupamiento, se codifican las entradas del mouse y del teclado (desde el servidor de agrupamiento) y se envían a través de la red al cliente de agrupamiento. El cliente de agrupamiento descodifica las entradas del mouse y del teclado y pasa la información al escritorio local del cliente de agrupamiento.

El cliente de agrupamiento se basa en un paquete de software de código abierto denominado Synergy, con codificación proporcionada por un paquete denominado stunnel.

Configuración del agrupamiento de cliente

La configuración de agrupamiento de cliente es un proceso que consta de dos pasos:

1. [Configurar los clientes de agrupamiento en la página 46](#)
2. [Configurar el servidor de agrupamiento en la página 47](#)

Configurar los clientes de agrupamiento

Ejecute este procedimiento en cada cliente de agrupamiento:

1. Seleccione **Periféricos > Agrupamiento de cliente** en el Panel de control.
2. Seleccione **Cliente**.
3. Introduzca el nombre de host o la dirección de IP del servidor de agrupamiento en el campo.
4. Seleccione **Aplicar**.

Configurar el servidor de agrupamiento

Para configurar el servidor de agrupamiento:

1. Seleccione **Periféricos > Agrupamiento de cliente** en el Panel de control.
2. Seleccione **Servidor**.
3. El servidor de agrupamiento se muestra en un cuadro azul que contiene su nombre de host. Seleccione y arrastre el servidor de agrupamiento hasta la ubicación deseada en la cuadrícula 4 x 4.
4. Seleccione la ubicación de la cuadrícula 4 x 4 en la que desea colocar el primer cliente de agrupamiento, escriba su nombre de host o dirección IP y luego presione **Intro**. El cliente de agrupamiento se muestra en un cuadro verde.
5. Si lo desea, coloque hasta dos clientes de agrupamiento adicionales en la cuadrícula 4 x 4.

La colocación del servidor de agrupamiento y de los clientes del agrupamiento en la cuadrícula 4 x 4 puede modificarse en cualquier momento haciendo clic y arrastrando la casilla correspondiente a una nueva ubicación.

Una vez que se han configurado los clientes del agrupamiento y el servidor de agrupamiento, tratan automáticamente de establecer las comunicaciones encriptadas entre sí. Seleccione **Estado** para ver el estado de la conexión entre los equipos.

Preferencias de pantalla

HP ThinPro le permite crear perfiles para visualizar preferencias y aplicar diversos perfiles a monitores diferentes. Un perfil incluye resolución, frecuencia de actualización, profundidad de bits y orientación.

Para configurar los perfiles de pantalla:

1. Seleccione **Periféricos > Preferencias de video** en el Panel de control.
2. Configure las opciones según sea necesario y luego seleccione **Aplicar**.



NOTA: Las opciones pueden variar según el modelo del hardware.

Consulte los siguientes consejos sobre cuando es útil personalizar la pantalla de perfiles:

- Algunas aplicaciones podrían requerir una resolución o una profundidad de bits específica para funcionar correctamente.
- Algunas aplicaciones podrían requerir que se gire la pantalla.
- Utilizar una profundidad de color de 16 bits debería optimizar el rendimiento de las conexiones Citrix y RDP porque se deben transmitir menos datos a través de la red o enviar menos datos al chip de gráficos.
- Las plataformas basadas en AMD (t520, t610, t620) ofrecen profundidad de color solo de 32 bits. El t505 y el t510 ofrecen profundidad de color de 16 bits ó 32 bits. En todos los casos, la profundidad de color de 32 bits realmente utiliza 24 bits.
- Es posible que un administrador desee estandarizar un perfil de pantalla, aun cuando existan muchos monitores diferentes en la organización.

Para cambiar rápidamente la configuración de la pantalla cuando se usan monitores externos (solo en thin clients móviles):

- ▲ Presione **Fn + F4**.

Configuración de impresoras

Para configurar una impresora:

1. Seleccione **Periféricos > 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**. Sin un controlador para asignar, cuando se conecta a una sesión remota, es posible que Windows no use el controlador correcto y la impresión podría no funcionar. El controlador también debe estar instalado en el servidor de Windows para que la impresora funcione correctamente.

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.

Redirección de dispositivos USB

Para redirigir los dispositivos USB:

1. Seleccione **Periféricos > Administrador de USB** en el Panel de control.
2. En la página **Protocolo**, seleccione un protocolo remoto.
Si la configuración es **Local**, también puede especificar las opciones **permitir el montaje de dispositivos** y **montar dispositivos solo de 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 finalizado, seleccione **Aceptar**.

Configuración

Opción de menú	Descripción
Administrador de fondos	<p>Le permite configurar el tema de fondo y mostrar de forma dinámica la información del sistema (como el nombre de host del thin client, la dirección de IP, el modelo de hardware y la dirección MAC) en segundo plano.</p> <p>Para obtener más información, consulte el informe técnico sobre HP ThinPro «<i>Login Screen Customization</i>» (disponible solo en inglés).</p>
Fecha y hora	Le permite configurar la zona horaria y las opciones de fecha y hora.
Administrador de firewall	Le permite configurar los ajustes de firewall.
Idioma	Le permite mostrar la interfaz de HP ThinPro en un idioma distinto.
Red	<p>Le permite configurar los ajustes de la red.</p> <p>Para obtener más información, consulte Ajustes de la red en la página 49.</p>
Administrador de energía	Le permite configurar los valores de administración de energía como el protector de pantalla, las configuraciones de la CPU, el momento de apagar la pantalla y de entrar en el modo de suspensión.
Seguridad	Para obtener más información, consulte Configuraciones de seguridad en la página 54 .
Centro de personalización	<p>Le permite realizar una de las siguientes acciones:</p> <ul style="list-style-type: none">• 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 <p>Para obtener más información, consulte Centro de personalización en la página 55.</p>

Ajustes de la red

Los ajustes de la red se pueden configurar utilizando el Administrador de redes. Para abrir el Administrador de redes:

- ▲ Seleccione **Configuración > Red** en el Panel de control.

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

- [Ajustes para la red cableada](#)
- [Ajustes para la red inalámbrica](#)
- [Configuración de DNS](#)
- [Reglas de IPSec](#)
- [Configuración de los ajustes de VPN](#)

- [Configuración de HP Velocity](#)

Ajustes para la red cableada

La siguiente tabla describe las opciones disponibles en la ficha **Con cable** del Administrador de redes.

Opción	Descripción
Habilitar IPv6	Activa IPv6. IPv4 se utiliza de forma predeterminada y no pueden utilizarse al mismo tiempo.
Velocidad Ethernet	Le permite definir la velocidad de Ethernet. Si su interruptor o concentrador no tiene un requisito especial, opte por la configuración predeterminada Automático .
Método de conexión	Le permite elegir entre Automático y Estático . Si su entorno de red usa DHCP, la opción Automático debe funcionar sin que sea necesario establecer otro tipo de configuración. Si se selecciona Estático , 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).
Configuración de seguridad	Le permite definir uno de los siguientes ajustes de autenticación: <ul style="list-style-type: none"> • Ninguno • 802.1X-TTLS • 802.1X-PEAP • 802.1X-TLS Tenga en cuenta lo siguiente sobre TTLS y PEAP: <ul style="list-style-type: none"> • La opción de Autenticación interna debe configurarse de acuerdo con lo que admite el servidor. • 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: <ul style="list-style-type: none"> • 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 del 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.

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).
Habilitar 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	<p>Permite seleccionar entre Automático y Estático. Si su entorno de red usa DHCP, la opción Automático debe funcionar sin otro tipo de configuración.</p> <p>Si se selecciona Estático, aparece el ajuste Configuración de dirección estática. Asegúrese de ingresar estos valores de acuerdo con la opción que está utilizando, IPv4 o IPv6.</p>
Ajustes de seguridad	<p>Le permite definir uno de los siguientes ajustes de autenticación:</p> <ul style="list-style-type: none"> • Ninguno • WEP • WPA/WPA2-PSK • 802.1X-TTLS • 802.1X-PEAP • 802.1X-TLS • EAP-FAST <p>En el caso de WEP y WPA2/WPA-PSK, solo tiene que introducir la clave de red y seleccionar Aceptar.</p> <p>Para EAP-FAST, configure Identidad anónima, Nombre de usuario, Contraseña y Método de aprovisionamiento. No necesita cambiar los ajustes del archivo PAC.</p> <p>Consulte Ajustes para la red cableada en la página 50 para obtener más información sobre TTLS, PEAP y TLS.</p>
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.

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

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

Opción	Descripción
Autenticación	Le permite definir uno de los siguientes ajustes de autenticación: <ul style="list-style-type: none"> • Ninguno • WEP • WPA/WPA2-PSK • WPA/WPA2 Enterprise-TTLS • WPA/WPA2 Enterprise-PEAP • WPA/WPA2 Enterprise-TLS • EAP-FAST <p>En el caso de WEP y WPA2/WPA-PSK, solo tiene que introducir la clave de red y seleccionar Aceptar.</p> <p>Para EAP-FAST, configure Identidad anónima, Nombre de usuario, Contraseña y Método de aprovisionamiento. No necesita cambiar los ajustes del archivo PAC.</p> <p>Consulte Ajustes para la red cableada en la página 50 para obtener más información sobre TTLS, PEAP y TLS.</p>

Configuración de DNS

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

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.
Buscar dominios	Utilice esta casilla para restringir los dominios que se buscan.
Proxy HTTP	Utilice estas casillas para definir la información del servidor proxy usando el formato siguiente:
Proxy FTP	<code>http://<dirección>:<puerto></code>
Proxy HTTPS	HP recomienda utilizar el prefijo <code>http://</code> para los tres ajustes de proxy. De esta forma, logrará una mejor compatibilidad. NOTA: Los ajustes de proxy se predeterminan en las variables del entorno http_proxy , ftp_proxy y https_proxy para el sistema.

Reglas de IPSec

Utilice esta ficha para agregar, editar y eliminar reglas de IPSec. Una regla de 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 **Fase I** y **Fase 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 con relación a creación de una VPN con Cisco:

- La **Puerta de enlace** es la dirección IP del puerta de enlace 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 del 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 con relación a la creación de una VPN con PPTP:

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

Configuración de HP Velocity

Use la ficha **HP Velocity** para establecer los ajustes de HP Velocity. Vaya a <http://www.hp.com/go/velocity> para obtener más información acerca de los modos de HP Velocity.

Configuraciones de seguridad

Los ajustes de seguridad se pueden configurar utilizando el Administrador de seguridad. Para abrir el Administrador de seguridad, seleccione **Configuración > 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 54](#)
- [Encriptación en la página 54](#)
- [Opciones en la página 55](#)

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 está disponible Argon2, 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 computar una tabla arco iris que haga coincidir contraseñas en texto sin formato con valores hash computados 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 descryptación.

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 descryptó supera el tiempo de vida, la coincidencia de hash o la descryptación fallarán.

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.

Centro de personalización

Para abrir el Centro de personalización:

- ▲ Seleccione **Configuración > 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 [Elegir 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**.

Opción	Descripción
Iniciar el Administrador de conexión en el inicio	Cuando está activado, el Administrador de conexión se abre automáticamente al iniciar el sistema.
Activar el menú de clic 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 al host X	Cuando está activada, solo los sistemas enumerados en el área de la Lista de control de acceso de XHost pueden controlar el thin client de forma remota.
Habilitar actualización USB	Permite instalar actualizaciones desde una unidad flash USB. Consulte Actualizaciones desde una unidad USB en la página 79 para obtener más información.
Autenticar actualización 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.


Administración

Opción de menú	Descripción
Active Directory	Para obtener más información, consulte Configuración de Active Directory en la página 58 .
Agente HPDM	Le permite configurar al agente de HP Device Manager (HPDM). Para obtener más información, consulte la <i>Guía del administrador</i> de HPDM.
Actualización automática	Le permite configurar el servidor de Actualización automática manualmente. Para obtener más información, consulte HP Smart Client Services en la página 66 .
Administrador de componentes	Le permite eliminar componentes del sistema. Para obtener más información, consulte Administrador de componentes en la página 56 .
Restablecimiento 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.
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 59 .
Duplicación VNC	Le permite configurar las opciones de duplicación VNC. Para obtener más información, consulte Duplicación VNC en la página 62 .
Estadísticas de conexión inalámbrica	Le permiten ver información sobre los puntos de acceso inalámbrico.

Administrador de componentes

El Administrador de componentes le permite eliminar los componentes del sistema que no se utilizarán en su entorno, lo que puede ser deseable para reducir el tamaño de la imagen. 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.


Para abrir el Administrador de componentes:

- ▲ Seleccione **Administración > 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 **Sí**.

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.

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 pantalla 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

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 arranca 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.

Opción	Descripción
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 de HP ThinPro

Capturar una imagen de HP ThinPro en un servidor FTP


Para capturar una imagen de 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 una descarga simple del disco. 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 de HP ThinPro usando FTP o HTTP

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

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

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

5. Seleccione **Conservar 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 de HP ThinPro en una unidad flash USB

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



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

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 de HP ThinPro con una unidad flash USB

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



IMPORTANTE: Si cancela una implementación, 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 el thin client de destino.
2. Inserte la unidad flash USB.
3. Encienda el thin client.



NOTA: La pantalla permanece en negro de 10 a 15 segundos mientras el thin client detecta la unidad flash USB y se arranca desde allí. Si el thin client no se arranca desde la unidad flash USB, intente desconectar todos los demás 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 y Actualización automática (consulte [Profile Editor en la página 71](#) y [HP Smart Client Services en la página 66](#) 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 **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

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 acceder a la herramienta Duplicación VNC:

- ▲ Seleccione **Administración > 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 Duplicación VNC.

Opción	Descripción
Permitir Duplicación VNC	Activa la Duplicación VNC.
VNC solo de lectura	Hace que la sesión de VNC sea solo de lectura.
Contraseña de Uso VNC	Es obligatorio escribir una contraseña cuando se accede al thin client mediante VNC. Seleccione Defina Contraseña para configurar la contraseña.
Detener la duplicación	Si está activado, aparece un botón Detener la duplicación en la esquina superior izquierda del sistema remoto que detiene la duplicación de VNC cuando se presiona.
VNC Notifique Usuario para Negar	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 x segundos	Cierra el Mensaje de notificación del usuario después de x segundos.
Mensaje de Notificación de Usuario	Le permite mostrar un mensaje en el cuadro de diálogo de notificación para el usuario remoto.

Opción	Descripción
Rechazar conexiones predeterminadas	Si está activado, la conexión VNC será rechazada de forma predeterminada cuando se termine el tiempo.
Restablecer el servidor VNC inmediatamente	Restablece el servidor VNC después de aplicar los nuevos ajustes.

Avanzada

Opción de menú	Descripción
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 63 .
Opciones DHCP	Le permite configurar las opciones de DHCP. Para obtener más información, consulte Opciones DHCP en la página 64 .
Licencia HP	Le permite ver el Contrato de licencia de usuario final (CLUF) de HP.
Administrador de SCEP	Permite la administración de certificados basados en red.
Administrador de serie	Le permite configurar dispositivos en serie.
Atajos del teclado	Le permite crear, modificar y eliminar atajos del teclado.
Herramienta de recorte	Le permite tomar una instantánea de una selección rectangular de la pantalla, una ventana específica o la pantalla completa.
Administrador de tareas	Le permite supervisar el uso de la CPU y el historial de uso de la CPU en el thin client.
Editor de texto	Abre un editor de texto básico para ver y editar archivos de texto.
Terminal X	Le permite ejecutar comandos de Linux.

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 **Avanzado > 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 para adjuntar el certificado a un perfil, tal como se describe en [Agregar certificados a un perfil de cliente en la página 73](#).



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 **Avanzado > 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 ficha **Identificación** 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 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.

Opciones DHCP

Para abrir el Administrador de opción DHCP:

- ▲ Seleccione **Avanzada > Opciones DHCP** en el Panel de control.

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



SUGERENCIA: La lista desplegable en la esquina inferior izquierda del Administrador de opción DHCP le permite filtrar las etiquetas DHCP que se muestran.

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

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

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 con relación a un número de código específico.

Para cambiar un código DHCP:

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



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

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.

8 Información del sistema

Seleccione el botón **Información del sistema** en la barra de tareas para ver la información del software, la red y el sistema. La tabla a continuación describe la información que aparece en cada panel.

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 puerto de enlace y la configuración de DNS.
Herramientas de red	Ofrece las siguientes herramientas para supervisión y solución de problemas: <ul style="list-style-type: none">• 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.• Trazar ruta: use esta herramienta para detectar la ruta que un paquete de red usa de un dispositivo a otro.
Información del software	Muestra una lista de complementos instalados en la ficha Service Packs 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.
Registros del sistema	Muestra los siguientes registros: <ul style="list-style-type: none">• Autorización y seguridad• Administrador de conexión• Arrendamientos de DHCP• Registro general del sistema• Kernel• Administrador de red• Smart Client Services• Servidor X <p>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.</p> <p>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 77.</p>



NOTA: Consulte [SystemInfo en la página 158](#) para obtener información acerca de las claves de registro que pueden utilizarse para ocultar las pantallas de información del sistema.

9 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

Sistemas operativos compatibles

HP Smart Client Services admite los siguientes sistemas operativos:

- Windows 7
- Windows Server® 2008
- Windows Server 2008 R2
- Windows Server 2003
- Windows Vista®
- Windows XP



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>.

Obtención de HP Smart Client Services

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

Visualización del sitio web de Actualización automática

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 > Actualización automática HP > Actualización automática



NOTA: La ubicación física donde se almacenan los archivos de Actualización automática es la siguiente:

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

Creación de un perfil de Actualización automática

Actualización automática usa perfiles para implementar una configuración en thin clients. De forma predeterminada, cuando crea un perfil mediante Profile Editor (consulte [Profile Editor en la página 71](#)), 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.

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 Actualización automática 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 para crear o modificar un perfil de cliente (consulte [Profile Editor en la página 71](#)) hasta que esté listo para guardar el perfil del cliente.
3. En **Profile Editor**, 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.
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 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 76](#).

Uso del método de actualización de la etiqueta DHCP

En los sistemas Windows Server 2003 y Windows Server 2008, 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.

Campo	Entrada
Nombre	Introduzca <code>auto-update</code> .
Tipo de datos	Seleccione String .
Código	Introduzca <code>137</code> .
Descripción	Introduzca <code>HP Automatic Update</code> .

6. Seleccione **Aceptar**.
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, intenta verificar si hay 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 **auto-update** o cree un alias DNS de **auto-update** 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** para modificar estas configuraciones en la root (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

1. Seleccione **Administración > Actualización automática** en el Panel de control.
2. Seleccione **Habilitar la 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 configuración de thin client** si desea conservar todas las configuraciones previas.
7. Seleccione **Aceptar** y luego el thin client realizará las actualizaciones.

10 Profile Editor

HP Smart Client Services contiene Profile Editor, 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

- ▲ 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.

Para cargar un perfil de cliente:

1. En la pantalla inicial de Profile Editor, 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 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, 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, 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, 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 82](#) 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 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 a un perfil de cliente

1. En la pantalla **Files** (Archivos) de Profile Editor, 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 **Export File (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 **root (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 para las siguientes aplicaciones:

- 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, 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 **Path (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

1. En la pantalla **Files** (Archivos) de Profile Editor, seleccione **Add a file** (Agregar un archivo).
2. En la lista desplegable **Type (Tipo)**, seleccione **Link (Enlace)**.
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

1. En **Profile Editor**, 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.

Configuración de impresora en serie o paralela

Puede usar Profile Editor 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 de **Feed (Alimentación)** mientras enciende el dispositivo.
2. Después de unos segundos, suelte el botón de **Feed (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 **Feed (Alimentación)** nuevamente para imprimir la página de diagnóstico.

Configuración de 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 **connections**, seleccione **New connection** (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 **connections**, seleccione **New connection** (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 **Aceptar**.
4. En el directorio nuevo, ajuste los valores de **baudios**, **dataBits**, **flow** y **parity** (baudios, dataBits, flujo y paridad) según los obtenidos en [Cómo obtener los ajustes de la impresora en la página 74](#).

Establezca el valor de **device (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

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 host y de la impresora que desee instalar. Por ejemplo, con un nombre de host como ZTAHENAKOS y una impresora de serie, seleccione el puerto con **(ZTAHENAKOS:COM1)**. Para una impresora paralela, seleccione **(ZTAHENAKOS: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.

11 Solución de problemas

Solución de problemas de conectividad de red

1. Envíe un ping al servidor deseado haciendo lo siguiente:
 - 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 con éxito, el sistema mostrará la siguiente información:

```
PING 10.30.8.52 (10.30.8.52) 56(84) bytes of data.
```

```
64 bytes from 10.30.8.52: icmp_seq=1 ttl=64 time=0.815 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 viceversa.
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 sobre 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 **Nivel de depuración** 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.

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

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 ficheros...**
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

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, introduzca `tar xvfz Diagnostic.tgz`.

Visualización de los archivos de diagnóstico del sistema

Los archivos de diagnóstico del sistema 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**.

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 desde una unidad USB

Cuando las actualizaciones desde una unidad USB están activadas (consulte [Centro de personalización en la página 55](#)), puede usar una unidad flash USB para instalar simultáneamente múltiples complementos y certificados, así como para implementar un perfil.

Para ejecutar actualizaciones USB:

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



NOTA: Los archivos se pueden colocar en el directorio root (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 el 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 copia 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.

Sintaxis	Descripción
<code>hptc-bios-cfg -G <nombre del archivo></code>	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).
<code>hptc-bios-cfg -S <nombre del archivo></code>	Escribe los ajustes del BIOS desde el archivo especificado (CPQSETUP.TXT de forma predeterminada) al BIOS.
<code>hptc-bios-cfg -h</code>	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.

Sintaxis	Descripción
<code>hptc-bios-flash <nombre de la imagen></code>	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 .
<code>hptc-bios-flash -h</code>	Muestra una lista de opciones.

C Cambiar el tamaño de la partición de la unidad flash

 **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.

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.

 **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`

Sintaxis	Descripción
<code>resize-image</code>	Cuando se llama sin parámetros, 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 del 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.
<code>resize-image --size <tamaño en MB></code> Ejemplo: <code>resize-image --size 1024</code>	Con esta sintaxis, puede especificar el tamaño de la partición de destino en megabytes (MB) como un parámetro y luego confirmar el cambio.
<code>resize-image --no-prompt</code> O bien: <code>resize-image --no-prompt --size <tamaño en MB></code> Ejemplo: <code>resize-image --no-prompt --size 1024</code>	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 Claves de registro

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

- Utilice una tarea **_File and Registry** en HPDM
- Utilice el componente Registry Editor (Editor de registros) de Profile Editor y luego implemente el nuevo perfil
- Utilice el Registry Editor (Editor de registros) en la interfaz de usuario de HP ThinPro, que está disponible al escribir `regeditor` en una terminal X.

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

Clave de registro	Descripción
<code>root/Audio/AdjustSoundPath</code>	Establece la ruta completa al sonido reproducido cuando el volumen de reproducción cambia a través de los controles de volumen.
<code>root/Audio/JackRetask</code>	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: <ul style="list-style-type: none">• 0/1: No hay cambios / auriculares• 2: Micrófono Para el puerto posterior del t630: <ul style="list-style-type: none">• 0: No hay cambios / entrada de línea• 1: Auriculares / salida de línea Debe reiniciar el thin client después de cambiar estas configuraciones.
<code>root/Audio/OutputMute</code>	Si se configura en 1, se desactivan el conector de auriculares y el altavoz interno.
<code>root/Audio/OutputScale</code>	Establece la escala de volumen del conector de auriculares y el altavoz interno, de 1 a 400.
<code>root/Audio/OutputScaleAuto</code>	Si se establece en 1, el valor de <code>OutputScale</code> se configurará automáticamente según en el modelo de thin client.
<code>root/Audio/OutputVolume</code>	Establece el volumen del conector de auriculares y el altavoz interno, de 1 a 100.
<code>root/Audio/PlaybackDevice</code>	Establece el dispositivo que se utiliza para la reproducción.
<code>root/Audio/PulseBuffer</code>	El rango recomendado de este valor se ubica entre 1024 y 8192. Un valor demasiado alto podría producir inestabilidad en la

Clave de registro	Descripción
	reproducción, pero 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 <code>freerdp</code> , <code>view</code> y <code>xen</code> .

CertMgr

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

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

Clave de registro	Descripción
root/ConnectionManager/customLogoPath	
root/ConnectionManager/defaultConnection	Para iniciar adecuadamente una conexión al inicio, esta opción debe establecerse en una conexión válida mediante el formato <code><tipo>:<etiqueta></code> , como en el ejemplo siguiente: <code>xen:Default Connection</code>
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 <code>splashLogoPath</code> . De forma predeterminada, esta opción está activada para ThinPro y desactivada para Smart Zero.

ConnectionType

custom

Clave de registro	Descripción
<code>root/ConnectionType/custom/authorizations/user/add</code>	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.
<code>root/ConnectionType/custom/authorizations/user/general</code>	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.
<code>root/ConnectionType/custom/connections/<UUID>/afterStartedCommand</code>	Establece el comando que se debe ejecutar después de que se ha iniciado la conexión.
<code>root/ConnectionType/custom/connections/<UUID>/afterStoppedCommand</code>	Establece el comando que se debe ejecutar después de que se ha detenido la conexión.
<code>root/ConnectionType/custom/connections/<UUID>/authorizations/user/edit</code>	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones para esta conexión.
<code>root/ConnectionType/custom/connections/<UUID>/authorizations/user/execution</code>	Si se establece en 1, un usuario final tiene permiso para ejecutar esta conexión.
<code>root/ConnectionType/custom/connections/<UUID>/autoReconnect</code>	Si se establece en 1, la conexión se reiniciará cuando se cierre o desconecte.
<code>root/ConnectionType/custom/connections/<UUID>/autoReconnectDelay</code>	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 <code>autoReconnect</code> se establece en 1.
<code>root/ConnectionType/custom/connections/<UUID>/autostart</code>	Si se establece en un valor de 1 a 5, la conexión se iniciará automáticamente después de que inicie el sistema, con el valor de 1 con la prioridad más alta.
<code>root/ConnectionType/custom/connections/<UUID>/autostartDelay</code>	Establece la cantidad de tiempo en segundos que se deben esperar antes de que la conexión se inicie después de que inicie el sistema. El valor predeterminado 0 hará que la conexión se inicie inmediatamente. Esta configuración solo surte efecto cuando <code>autostart</code> se establece en 1.
<code>root/ConnectionType/custom/connections/<UUID>/beforeStartingCommand</code>	Establece que se ejecute el comando antes de que empiece la conexión.
<code>root/ConnectionType/custom/connections/<UUID>/command</code>	Establece que se ejecute el comando principal de la conexión personalizada.
<code>root/ConnectionType/custom/connections/<UUID>/connectionEndAction</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/custom/connections/<UUID>/coord</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/custom/connections/<UUID>/dependConnectionId</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/custom/connections/<UUID>/extraEnvValues/<UUID>/key</code>	Establece el nombre de una variable de entorno adicional para su uso con la conexión.

Clave de registro	Descripción
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 de seguridad 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>/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 establece en el valor predeterminado focus y la conexión ya se ha iniciado, la conexión se concentrará. De lo contrario, se muestra 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.
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 arranca 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 arranca el Administrador de conexión General para este tipo de conexión. No debería ser necesario modificar esta clave.
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/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 conexión 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 conexión. 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.

Clave de registro	Descripción
<code>root/ConnectionType/custom/coreSettings/stopProcess</code>	Establece el comportamiento que debería ocurrir cuando se llama <code>connection-mgr stop</code> en esta conexión. De forma predeterminada, esta opción es <code>close</code> , lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como <code>kill</code> , el proceso especificado por <code>appName</code> se interrumpirá de forma forzada. Cuando se establece como <code>custom</code> se ejecutará una línea de comandos de ejecución personalizada especificada por <code>wrapperScript</code> con el argumento <code>stop</code> para finalizar el proceso correctamente.
<code>root/ConnectionType/custom/coreSettings/watchPid</code>	Si se establece en 1, la conexión se supervisa bajo el nombre especificado por <code>appName</code> . No debería ser necesario modificar esta clave.
<code>root/ConnectionType/custom/coreSettings/wrapperScript</code>	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Esta es la línea de comandos principal que maneja todas las configuraciones de la conexión y los argumentos de la línea de comandos para la conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/custom/gui/CustomManager/name</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/custom/gui/CustomManager/status</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/custom/gui/CustomManager/title</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/custom/gui/CustomManager/widgets/autoReconnect</code>	Controla el estado del widget Reconexión automática en el Administrador de conexión Custom. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/custom/gui/CustomManager/widgets/autostart</code>	Controla el estado del widget Prioridad de inicio automático en el Administrador de conexión Custom. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/custom/gui/CustomManager/widgets/command</code>	Controla el estado del widget Ingresa el comando a ejecutar en el Administrador de conexión Custom. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/custom/gui/CustomManager/widgets/fallBackConnection</code>	Controla el estado del widget Conexión de seguridad en el Administrador de conexión Custom. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/custom/gui/CustomManager/widgets/hasDesktopIcon</code>	Controla el estado del widget Mostrar icono en escritorio en el Administrador de conexión Custom. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como

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

firefox

Clave de registro	Descripción
<code>root/ConnectionType/firefox/authorizations/user/add</code>	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.
<code>root/ConnectionType/firefox/authorizations/user/general</code>	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.
<code>root/ConnectionType/firefox/connections/<UUID>/address</code>	Establece la dirección URL o IP a la cual conectarse.
<code>root/ConnectionType/firefox/connections/<UUID>/afterStartedCommand</code>	Establece el comando que se debe ejecutar después de que se ha iniciado la conexión.
<code>root/ConnectionType/firefox/connections/<UUID>/afterStoppedCommand</code>	Establece el comando que se debe ejecutar después de que se ha detenido la conexión.
<code>root/ConnectionType/firefox/connections/<UUID>/authorizations/user/edit</code>	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones para esta conexión.
<code>root/ConnectionType/firefox/connections/<UUID>/authorizations/user/execution</code>	Si se establece en 1, un usuario final tiene permiso para ejecutar esta conexión.
<code>root/ConnectionType/firefox/connections/<UUID>/autoReconnect</code>	Si se establece en 1, la conexión se reiniciará cuando se cierre o desconecte.
<code>root/ConnectionType/firefox/connections/<UUID>/autoReconnectDelay</code>	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 <code>autoReconnect</code> se establece en 1.
<code>root/ConnectionType/firefox/connections/<UUID>/autostart</code>	Si se establece en un valor de 1 a 5, la conexión se iniciará automáticamente después de que inicie el sistema, con el valor de 1 con la prioridad más alta.
<code>root/ConnectionType/firefox/connections/<UUID>/autostartDelay</code>	Establece la cantidad de tiempo en segundos que se deben esperar antes de la conexión se inicie después de que inicie el sistema. El valor predeterminado 0 hará que la conexión se inicie

Clave de registro	Descripción
	inmediatamente. Esta configuración solo surte efecto cuando <code>autostart</code> se establece en 1.
<code>root/ConnectionType/firefox/connections/<UUID>/beforeStartingCommand</code>	Establece que se ejecute el comando antes de que empiece la conexión.
<code>root/ConnectionType/firefox/connections/<UUID>/connectionEndAction</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/firefox/connections/<UUID>/coord</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/firefox/connections/<UUID>/dependConnectionId</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/firefox/connections/<UUID>/enablePrintDialog</code>	Si se establece en 1, puede usarse el cuadro de diálogo de impresión en el explorador web.
<code>root/ConnectionType/firefox/connections/<UUID>/enableSmartCard</code>	Si se establece en 1, se habilita el inicio de sesión con smart card en las conexiones Citrix creadas mediante el navegador web.
<code>root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/key</code>	Establece el nombre de una variable de entorno adicional para su uso con la conexión.
<code>root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/value</code>	Establece el valor de una variable de entorno adicional para su uso con la conexión.
<code>root/ConnectionType/firefox/connections/<UUID>/fallBackConnection</code>	Establece la conexión de seguridad a través de su UUID.
<code>root/ConnectionType/firefox/connections/<UUID>/forbiddenFiles</code>	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: <code>*.rdf,cookies.sqlite</code>
<code>root/ConnectionType/firefox/connections/<UUID>/fullscreen</code>	Si se establece en 1, el explorador web se iniciará en modo de pantalla completa. Si <code>kioskMode</code> está desactivado, se puede acceder a la UI del navegador en modo de pantalla completa.
<code>root/ConnectionType/firefox/connections/<UUID>/hasDesktopIcon</code>	Si se establece en 1, se activa el icono del escritorio para esta conexión. Esta tecla no tiene efecto en Smart Zero.
<code>root/ConnectionType/firefox/connections/<UUID>/intendedUse</code>	Establece el uso previsto de esta conexión Web Browser en Citrix, RDPo Internet.
<code>root/ConnectionType/firefox/connections/<UUID>/kioskMode</code>	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 <code>fullscreen</code> está establecido en 0) y no se puede acceder a la UI del navegador.
<code>root/ConnectionType/firefox/connections/<UUID>/label</code>	Establece el nombre de conexión que se muestra en la interfaz de usuario. En Smart Zero, por lo general esta opción se establece en <code>Default Connection</code> y no aparece en la interfaz de usuario.
<code>root/ConnectionType/firefox/connections/<UUID>/showBackForwardButton</code>	Si se establece en 1, los botones Atrás y Adelante del navegador web se muestra cuando está habilitado el modo quiosco.
<code>root/ConnectionType/firefox/connections/<UUID>/showHomeButton</code>	Si se establece en 1, el botón Inicio del navegador web se muestra cuando está habilitado el modo quiosco.

Clave de registro	Descripción
<code>root/ConnectionType/firefox/connections/<UUID>/showSearchBar</code>	Si se establece en 1, la barra de búsqueda del navegador web se muestra cuando está habilitado el modo quiosco.
<code>root/ConnectionType/firefox/connections/<UUID>/showTabsBar</code>	Si se establece en 1, las fichas del navegador web se muestra cuando está habilitado el modo quiosco.
<code>root/ConnectionType/firefox/connections/<UUID>/showTaskBar</code>	Si se establece en 1, la barra de tareas del navegador web se muestra cuando está habilitado el modo quiosco.
<code>root/ConnectionType/firefox/connections/<UUID>/showUrlBarRefreshButton</code>	Si se establece en 1, el botón Actualizar y la barra de URL del navegador web se muestra cuando está habilitado el modo quiosco.
<code>root/ConnectionType/firefox/connections/<UUID>/startMode</code>	Si se establece en el valor predeterminado <code>focus</code> y la conexión ya se ha iniciado, la conexión se concentrará. De lo contrario, se muestra un error que indica que la conexión ya se ha iniciado.
<code>root/ConnectionType/firefox/connections/<UUID>/waitForNetwork</code>	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.
<code>root/ConnectionType/firefox/coreSettings/USBrelevant</code>	Especifica si este tipo de conexión es relevante para el USB. Si es así, puede tener un complemento USB para redirigir dispositivos USB.
<code>root/ConnectionType/firefox/coreSettings/appName</code>	Establece el nombre de la aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/firefox/coreSettings/className</code>	Establece el nombre de la clase de aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/firefox/coreSettings/editor</code>	Establece el nombre de la aplicación interna que se utiliza cuando se arranca el Administrador de conexión para este tipo de conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/firefox/coreSettings/generalSettingsEditor</code>	Establece el nombre de la aplicación interna que se utiliza cuando se arranca el Administrador de conexión General para este tipo de conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/firefox/coreSettings/icon16Path</code>	Establece la ruta al icono de 16 x 16 píxeles para esta aplicación.
<code>root/ConnectionType/firefox/coreSettings/icon32Path</code>	Establece la ruta al icono de 32 x 32 píxeles para esta aplicación.
<code>root/ConnectionType/firefox/coreSettings/icon48Path</code>	Establece la ruta al icono de 48 x 48 píxeles para esta aplicación.
<code>root/ConnectionType/firefox/coreSettings/label</code>	Establece el nombre que se va a mostrar para este tipo de conexión en la interfaz de usuario.
<code>root/ConnectionType/firefox/coreSettings/priorityInConnectionLists</code>	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.

Clave de registro	Descripción
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 <code>unused</code> , <code>optional</code> o <code>required</code> para este tipo de conexión.
root/ConnectionType/firefox/coreSettings/stopProcess	Establece el comportamiento que debería ocurrir cuando se llama <code>connection-mgr stop</code> en esta conexión. De forma predeterminada, esta opción es <code>close</code> , lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como <code>kill</code> , el proceso especificado por <code>appName</code> se interrumpirá de forma forzada. Cuando se establece como <code>custom</code> se ejecutará una línea de comandos de ejecución personalizada especificada por <code>wrapperScript</code> con el argumento <code>stop</code> para finalizar el proceso correctamente.
root/ConnectionType/firefox/coreSettings/wrapperScript	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Esta es la línea de comandos principal que maneja todas las configuraciones de la conexión y los argumentos de la 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.

Clave de registro	Descripción
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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , 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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , el widget puede verse en el modo de solo lectura.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/kioskMode	Controla el estado del widget Habilitar modo quiosco en el Administrador de conexión Web Browser. Si se establece como <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , 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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , 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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , 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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , 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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , el widget puede verse en el modo de solo lectura.
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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , 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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , el widget puede verse en el modo de solo lectura.

Clave de registro	Descripción
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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.

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/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/freerdp/connections/<UUID>/ExtraArgs	Especifica los argumentos adicionales para el cliente xfreerdp. Ejecute <code>xfreerdp --help</code> desde una terminal X para ver todos los argumentos disponibles.
root/ConnectionType/freerdp/connections/<UUID>/SingleSignOn	
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: <code>servername:3389</code>
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.

Clave de registro	Descripción
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 inicie el sistema, con el valor de 1 con la prioridad más alta.
root/ConnectionType/freerdp/connections/<UUID>/autostartDelay	Establece la cantidad de tiempo en segundos que se deben esperar antes de la conexión se inicie después de que inicie el sistema. El valor predeterminado 0 hará que la conexión se inicie inmediatamente. Esta configuración solo surte efecto cuando autostart se establece en 1.
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.
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>/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 de seguridad a través de su UUID.

Clave de registro	Descripción
<code>root/ConnectionType/freerdp/connections/<UUID>/frameAcknowledgeCount</code>	Establece el número de fotogramas de video que el servidor puede forzar sin tener que esperar el reconocimiento desde el cliente. Los números inferiores dan por resultado un escritorio con mayor capacidad de respuesta pero con menos fotogramas por segundo. Si se establece en 0, no se utiliza el reconocimiento de fotogramas en las interacciones del cliente y el servidor.
<code>root/ConnectionType/freerdp/connections/<UUID>/gatewayAddress</code>	Establece el nombre del servidor o la dirección RD Gateway.
<code>root/ConnectionType/freerdp/connections/<UUID>/gatewayCredentialsType</code>	Especifica el tipo de credencial entre la opción de que las credenciales las suministre <code>sso</code> (inicio de sesión único), <code>startup</code> (las credenciales se solicitan en el inicio) o <code>password</code> (contraseña/dominio/usuario preconfigurados).
<code>root/ConnectionType/freerdp/connections/<UUID>/gatewayDomain</code>	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 <code>gatewayUsesSameCredentials</code> en 1, este valor se desactiva.
<code>root/ConnectionType/freerdp/connections/<UUID>/gatewayEnabled</code>	Si se establece en 1, es de esperar que se use RD Gateway.
<code>root/ConnectionType/freerdp/connections/<UUID>/gatewayPassword</code>	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 <code>gatewayUsesSameCredentials</code> en 1, este valor se desactiva.
<code>root/ConnectionType/freerdp/connections/<UUID>/gatewayPort</code>	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.
<code>root/ConnectionType/freerdp/connections/<UUID>/gatewayUser</code>	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 <code>gatewayUsesSameCredentials</code> en 1, este valor se desactiva.
<code>root/ConnectionType/freerdp/connections/<UUID>/gatewayUsesSameCredentials</code>	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.
<code>root/ConnectionType/freerdp/connections/<UUID>/hasDesktopIcon</code>	Si se establece en 1, se activa el icono del escritorio para esta conexión. Esta tecla no tiene efecto en Smart Zero.
<code>root/ConnectionType/freerdp/connections/<UUID>/label</code>	Establece el nombre de conexión que se muestra en la interfaz de usuario. En Smart Zero, por lo general esta opción se establece en <code>Default Connection</code> y no aparece en la interfaz de usuario.
<code>root/ConnectionType/freerdp/connections/<UUID>/loadBalanceInfo</code>	Este valor es la cookie de equilibrio de carga enviado al servidor para fines de intermediación tras la conexión y corresponde al campo <code>loadbalanceinfo</code> en el archivo <code>.rdp</code> . De forma predeterminada, el valor está vacío.
<code>root/ConnectionType/freerdp/connections/<UUID>/localPartitionRedirection</code>	Si se establece en 1, las particiones de almacenamiento local no USB se redirigen al host remoto mediante la extensión <code>Storage</code> . Si se establece en 0, la extensión se desactiva para las particiones de almacenamiento no USB y que HP ThinPro no utiliza.

Clave de registro	Descripción
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 se muestra pero desactivada. Si se establece en 0, la casilla de verificación está oculta.
root/ConnectionType/freerdp/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 desactivado. Si se establece en 0, el botón queda oculto.
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 se muestra pero desactivada. 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.

Clave de registro	Descripción
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 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 Ports. 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

Clave de registro	Descripción
	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 <code>verifyPublisherSignature</code> 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 <code>.rdp</code> 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 <code>trustedPublisherSha1Thumbprints</code> .
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 solo 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 <code>thin client</code> 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 solo 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 <code>auto</code> 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 <code>remote computer</code> , se realiza una conexión RDP directa a un equipo remoto. Si se establece en <code>RD Web Access</code> , 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

Clave de registro	Descripción
	en una versión futura de HP ThinPro. Este ajuste debe desactivarse solo 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>/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.
root/ConnectionType/freerdp/connections/<UUID>/seamlessWindow	Si se establece en 1, se desactivan 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 <code>root/ConnectionType/freerdp/general/sendHostname</code> se debe establecer en <code>hostname</code> 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 arranca 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 arranca 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 <code>Audio</code> . 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 <code>Multimedia Redirection</code>) coincida con la configuración de audio local.
root/ConnectionType/freerdp/connections/<UUID>/startMode	Si se establece en el valor predeterminado <code>focus</code> y la conexión ya se ha iniciado, la conexión se concentrará. De lo contrario, se muestra 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.

Clave de registro	Descripción
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.
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 <code>auto</code> . 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 <code>sound</code> , <code>printerMapping</code> , <code>portMapping</code> , <code>usbStorageRedirection</code> y <code>localPartitionRedirection</code> . 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 <code>Storage</code> . 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 <code>Remote Application</code> , RDP se ejecutará en el modo Aplicación remota integrada localmente (RAIL). Esto requiere que el servidor de <code>RemoteApp</code> 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 <code>remoteApp</code> . Si se establece en <code>Alternate Shell</code> , se invoca un shell no estándar. Consulte también las claves de registro <code>application</code> y <code>directory</code> .
root/ConnectionType/freerdp/connections/<UUID>/windowSizeHeight	

Clave de registro	Descripción
root/ConnectionType/freerdp/connections/<UUID>/windowSizePercentage	
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: <code>xfreerdp --kbd-list</code> .
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 arranca el Administrador de conexión para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/freerdp/coreSettings/generalSettingsEditor	Establece el nombre de la aplicación interna que se utiliza cuando se arranca el Administrador de conexión General para este tipo de conexión. No debería ser necesario modificar esta clave.
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.

Clave de registro	Descripción
<code>root/ConnectionType/freerdp/coreSettings/initialConnectionTimeout</code>	Establece el número de segundos de espera de una respuesta inicial del servidor RDP antes de desistir.
<code>root/ConnectionType/freerdp/coreSettings/label</code>	Establece el nombre que se va a mostrar para este tipo de conexión en la interfaz de usuario.
<code>root/ConnectionType/freerdp/coreSettings/priorityInConnectionLists</code>	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.
<code>root/ConnectionType/freerdp/coreSettings/stopProcess</code>	Establece el comportamiento que debería ocurrir cuando se llama <code>connection-mgr stop</code> en esta conexión. De forma predeterminada, esta opción es <code>close</code> , lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como <code>kill</code> , el proceso especificado por <code>appName</code> se interrumpirá de forma forzada. Cuando se establece como <code>custom</code> se ejecutará una línea de comandos de ejecución personalizada especificada por <code>wrapperScript</code> con el argumento <code>stop</code> para finalizar el proceso correctamente.
<code>root/ConnectionType/freerdp/coreSettings/watchPid</code>	Si se establece en 1, la conexión se supervisa bajo el nombre especificado por <code>appName</code> . No debería ser necesario modificar esta clave.
<code>root/ConnectionType/freerdp/coreSettings/wrapperScript</code>	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Esta es la línea de comandos principal que maneja todas las configuraciones de la conexión y los argumentos de la línea de comandos para la conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/freerdp/coreSettings/wrapperScriptGeneration</code>	Permite que el Administrador de conexión sepa qué tipo de parámetros aprueban el script.
<code>root/ConnectionType/freerdp/general/autoReconnectDialogTimeout</code>	Si <code>autoReconnect</code> 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.
<code>root/ConnectionType/freerdp/general/disablePasswordChange</code>	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.
<code>root/ConnectionType/freerdp/general/enableMMR</code>	Si se establece en 1, se activa el complemento <code>Multimedia Redirection</code> . Esto hace que los códecs compatibles que se reproducen a través de Windows Media Player se redirijan al cliente. De esta forma la reproducción de video de alta definición y a pantalla completa mejorará notablemente para códecs como WMV9, VC1 y MPEG4.
<code>root/ConnectionType/freerdp/general/preferredAudio</code>	Establece el backend del audio predeterminado para la redirección de audio de alto nivel (tanto de entrada como de salida).
<code>root/ConnectionType/freerdp/general/rdWebFeedUrlPattern</code>	Establece el patrón utilizado para crear la URL de RD Web Access. El host de la URL, por ej. <code>Myserver.com</code> , se sustituye por el valor del campo Dirección de la conexión. Este patrón no se utiliza cuando la dirección ya es una URL.

Clave de registro	Descripción
root/ConnectionType/freerdp/general/sendHostname	Si se establece en <code>hostname</code> , 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 <code>sendHostname</code> en la configuración específica para la conexión. Si se establece en <code>mac</code> , en vez del nombre de host, se envía la dirección MAC del primer adaptador de red disponible.
root/ConnectionType/freerdp/general/serialPortsDriver	Esta configuración garantiza una mejor compatibilidad con el controlador subyacente esperado de Windows: <code>SerCx2.sys</code> , <code>SerCx.sys</code> o <code>Serial.sys</code> .
root/ConnectionType/freerdp/general/serialPortsPermissive	Si se establece en 1, se ignorarán los errores de recursos no compatibles.

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 <code>autoReconnect</code> 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 inicie el sistema, con el valor de 1 con la prioridad más alta.
root/ConnectionType/ssh/connections/<UUID>/autostartDelay	Establece la cantidad de tiempo en segundos que se deben esperar antes de la conexión se inicie después de que inicie el

Clave de registro	Descripción
	sistema. El valor predeterminado 0 hará que la conexión se inicie inmediatamente. Esta configuración solo surte efecto cuando <code>autostart</code> se establece en 1.
<code>root/ConnectionType/ssh/connections/<UUID>/backgroundColor</code>	Establece el color de fondo de la conexión.
<code>root/ConnectionType/ssh/connections/<UUID>/beforeStartingCommand</code>	Establece que se ejecute el comando antes de que empiece la conexión.
<code>root/ConnectionType/ssh/connections/<UUID>/compression</code>	Activa la compresión para una conexión SSH.
<code>root/ConnectionType/ssh/connections/<UUID>/connectionEndAction</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/ssh/connections/<UUID>/coord</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/ssh/connections/<UUID>/dependConnectionId</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/ssh/connections/<UUID>/extraEnvValues/<UUID>/key</code>	Establece el nombre de una variable de entorno adicional para su uso con la conexión.
<code>root/ConnectionType/ssh/connections/<UUID>/extraEnvValues/<UUID>/value</code>	Establece el valor de una variable de entorno adicional para su uso con la conexión.
<code>root/ConnectionType/ssh/connections/<UUID>/fallBackConnection</code>	Establece la conexión de seguridad a través de su UUID.
<code>root/ConnectionType/ssh/connections/<UUID>/font</code>	Establece el tamaño de la letra de la conexión.
<code>root/ConnectionType/ssh/connections/<UUID>/foregroundColor</code>	Establece el color de primer plano de la conexión.
<code>root/ConnectionType/ssh/connections/<UUID>/fork</code>	Si se establece en 1, se activa la opción Bifurque en segundo plano de la conexión.
<code>root/ConnectionType/ssh/connections/<UUID>/hasDesktopIcon</code>	Si se establece en 1, se activa el icono del escritorio para esta conexión. Esta tecla no tiene efecto en Smart Zero.
<code>root/ConnectionType/ssh/connections/<UUID>/isInMenu</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/ssh/connections/<UUID>/label</code>	Establece el nombre de conexión que se muestra en la interfaz de usuario. En Smart Zero, por lo general esta opción se establece en <code>Default Connection</code> y no aparece en la interfaz de usuario.
<code>root/ConnectionType/ssh/connections/<UUID>/port</code>	Establece el número de puerto que se utiliza cuando se comunica con el servidor SSH. De forma predeterminada es 22.
<code>root/ConnectionType/ssh/connections/<UUID>/startMode</code>	Si se establece en el valor predeterminado <code>focus</code> y la conexión ya se ha iniciado, la conexión se concentrará. De lo contrario, se muestra un error que indica que la conexión ya se ha iniciado.
<code>root/ConnectionType/ssh/connections/<UUID>/tty</code>	Si se establece en 1, la opción Forzar asignación TTY para la conexión.
<code>root/ConnectionType/ssh/connections/<UUID>/username</code>	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.

Clave de registro	Descripción
<code>root/ConnectionType/ssh/connections/<UUID>/waitForNetwork</code>	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.
<code>root/ConnectionType/ssh/connections/<UUID>/x11</code>	Si se establece en 1, se activa la opción Envío de conexión X11 para la conexión.
<code>root/ConnectionType/ssh/coreSettings/USBrelevant</code>	Especifica si este tipo de conexión es relevante para el USB. Si es así, puede tener un complemento USB para redirigir dispositivos USB.
<code>root/ConnectionType/ssh/coreSettings/appName</code>	Establece el nombre de la aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/ssh/coreSettings/className</code>	Establece el nombre de la clase de aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/ssh/coreSettings/editor</code>	Establece el nombre de la aplicación interna que se utiliza cuando se arranca el Administrador de conexión para este tipo de conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/ssh/coreSettings/icon16Path</code>	Establece la ruta al icono de 16 x 16 píxeles para esta aplicación.
<code>root/ConnectionType/ssh/coreSettings/icon32Path</code>	Establece la ruta al icono de 32 x 32 píxeles para esta aplicación.
<code>root/ConnectionType/ssh/coreSettings/icon48Path</code>	Establece la ruta al icono de 48 x 48 píxeles para esta aplicación.
<code>root/ConnectionType/ssh/coreSettings/label</code>	Establece el nombre que se va a mostrar para este tipo de conexión en la interfaz de usuario.
<code>root/ConnectionType/ssh/coreSettings/priorityInConnectionLists</code>	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.
<code>root/ConnectionType/ssh/coreSettings/serverRequired</code>	Establece si un nombre o dirección de servidor es <code>unused</code> , <code>optional</code> o <code>required</code> para este tipo de conexión.
<code>root/ConnectionType/ssh/coreSettings/stopProcess</code>	Establece el comportamiento que debería ocurrir cuando se llama <code>connection-mgr stop</code> en esta conexión. De forma predeterminada, esta opción es <code>close</code> , lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como <code>kill</code> , el proceso especificado por <code>appName</code> se interrumpirá de forma forzada. Cuando se establece como <code>custom</code> se ejecutará una línea de comandos de ejecución personalizada especificada por <code>wrapperScript</code> con el argumento <code>stop</code> para finalizar el proceso correctamente.
<code>root/ConnectionType/ssh/coreSettings/watchPid</code>	Si se establece en 1, la conexión se supervisa bajo el nombre especificado por <code>appName</code> . No debería ser necesario modificar esta clave.
<code>root/ConnectionType/ssh/coreSettings/wrapperScript</code>	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Esta es la línea de comandos

Clave de registro	Descripción
	principal que maneja todos los ajustes de la conexión y los argumentos de la 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.

Clave de registro	Descripción
root/ConnectionType/ssh/gui/SshManager/widgets/font	Controla el estado del widget Fuente en el Administrador de conexión Secure Shell. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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.
root/ConnectionType/ssh/gui/SshManager/widgets/label	Controla el estado del widget Nombre en el Administrador de conexión Secure Shell. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
root/ConnectionType/ssh/gui/SshManager/widgets/tty	Controla el estado del widget Forzar asignación TTY en el Administrador de conexión Secure Shell. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de

Clave de registro	Descripción
	usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/x11</code>	Controla el estado del widget Envío de conexión X11 en el Administrador de conexión Secure Shell. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.

teemtalk

Clave de registro	Descripción
<code>root/ConnectionType/teemtalk/authorizations/user/add</code>	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.
<code>root/ConnectionType/teemtalk/authorizations/user/general</code>	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.
<code>root/ConnectionType/teemtalk/connections/<UUID>/afterStartedCommand</code>	Establece el comando que se debe ejecutar después de que se ha iniciado la conexión.
<code>root/ConnectionType/teemtalk/connections/<UUID>/afterStoppedCommand</code>	Establece el comando que se debe ejecutar después de que se ha detenido la conexión.
<code>root/ConnectionType/teemtalk/connections/<UUID>/authorizations/user/edit</code>	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones para esta conexión.
<code>root/ConnectionType/teemtalk/connections/<UUID>/authorizations/user/execution</code>	Si se establece en 1, un usuario final tiene permiso para ejecutar esta conexión.
<code>root/ConnectionType/teemtalk/connections/<UUID>/autoReconnect</code>	Si se establece en 1, la conexión se reiniciará cuando se cierre o desconecte.
<code>root/ConnectionType/teemtalk/connections/<UUID>/autoStart</code>	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.
<code>root/ConnectionType/teemtalk/connections/<UUID>/beforeStartingCommand</code>	Establece que se ejecute el comando antes de que empiece la conexión.
<code>root/ConnectionType/teemtalk/connections/<UUID>/connectionEndAction</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/teemtalk/connections/<UUID>/coord</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/teemtalk/connections/<UUID>/dependConnectionId</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/teemtalk/connections/<UUID>/extraEnvValues/<UUID>/key</code>	Establece el nombre de una variable de entorno adicional para su uso con la conexión.
<code>root/ConnectionType/teemtalk/connections/<UUID>/extraEnvValues/<UUID>/value</code>	Establece el valor de una variable de entorno adicional para su uso con la conexión.

Clave de registro	Descripción
root/ConnectionType/teemtalk/connections/<UUID>/fallBackConnection	Establece la conexión de seguridad a través de su UUID.
root/ConnectionType/teemtalk/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/teemtalk/connections/<UUID>/isInMenu	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/teemtalk/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/teemtalk/connections/<UUID>/startMode	Si se establece en el valor predeterminado focus y la conexión ya se ha iniciado, la conexión se concentrará. De lo contrario, se muestra un error que indica que la conexión ya se ha iniciado.
root/ConnectionType/teemtalk/connections/<UUID>/systembeep	Si se establece en 1, se activa el sonido del sistema para la conexión.
root/ConnectionType/teemtalk/connections/<UUID>/ttsName	Establece el nombre de perfil de TeemTalk.
root/ConnectionType/teemtalk/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/teemtalk/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/teemtalk/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/teemtalk/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/teemtalk/coreSettings/editor	Establece el nombre de la aplicación interna que se utiliza cuando se arranca el Administrador de conexión para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/teemtalk/coreSettings/generalSettingsEditor	Establece el nombre de la aplicación interna que se utiliza cuando se arranca el Administrador de conexión General para este tipo de conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/teemtalk/coreSettings/icon16Path	Establece la ruta al icono de 16 x 16 píxeles para esta aplicación.
root/ConnectionType/teemtalk/coreSettings/icon32Path	Establece la ruta al icono de 32 x 32 píxeles para esta aplicación.
root/ConnectionType/teemtalk/coreSettings/icon48Path	Establece la ruta al icono de 48 x 48 píxeles para esta aplicación.
root/ConnectionType/teemtalk/coreSettings/label	Establece el nombre que se va a mostrar para este tipo de conexión en la interfaz de usuario.
root/ConnectionType/teemtalk/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

Clave de registro	Descripción
	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/teemtalk/coreSettings/serverRequired	Establece si un nombre o dirección de servidor es <code>unused</code> , <code>optional</code> o <code>required</code> para este tipo de conexión.
root/ConnectionType/teemtalk/coreSettings/stopProcess	Establece el comportamiento que debería ocurrir cuando se llama <code>connection-mgr stop</code> en esta conexión. De forma predeterminada, esta opción es <code>close</code> , lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como <code>kill</code> , el proceso especificado por <code>appName</code> se interrumpirá de forma forzada. Cuando se establece como <code>custom</code> se ejecutará una línea de comandos de ejecución personalizada especificada por <code>wrapperScript</code> con el argumento <code>stop</code> para finalizar el proceso correctamente.
root/ConnectionType/teemtalk/coreSettings/wrapperScript	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Esta es la línea de comandos principal que maneja todas las configuraciones de la conexión y los argumentos de la línea de comandos para la conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/teemtalk/gui/TeemtalkManager/name	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/teemtalk/gui/TeemtalkManager/status	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/teemtalk/gui/TeemtalkManager/title	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/autoReconnect	Controla el estado del widget Reconexión automática en el Administrador de conexión TeemTalk. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/autostart	Controla el estado del widget Prioridad de inicio automático en el Administrador de conexión TeemTalk. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/hasDesktopIcon	Controla el estado del widget Mostrar icono en escritorio en el Administrador de conexión TeemTalk. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/isInMenu	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/label	Controla el estado del widget Nombre en el Administrador de conexión TeemTalk. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget

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

telnet

Clave de registro	Descripción
<code>root/ConnectionType/telnet/authorizations/user/add</code>	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.
<code>root/ConnectionType/telnet/authorizations/user/general</code>	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.
<code>root/ConnectionType/telnet/connections/<UUID>/address</code>	Establece el nombre de host o la dirección IP a la cual conectarse.
<code>root/ConnectionType/telnet/connections/<UUID>/afterStartedCommand</code>	Establece el comando que se debe ejecutar después de que se ha iniciado la conexión.
<code>root/ConnectionType/telnet/connections/<UUID>/afterStoppedCommand</code>	Establece el comando que se debe ejecutar después de que se ha detenido la conexión.
<code>root/ConnectionType/telnet/connections/<UUID>/authorizations/user/edit</code>	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones para esta conexión.
<code>root/ConnectionType/telnet/connections/<UUID>/authorizations/user/execution</code>	Si se establece en 1, un usuario final tiene permiso para ejecutar esta conexión.
<code>root/ConnectionType/telnet/connections/<UUID>/autoReconnect</code>	Si se establece en 1, la conexión se reiniciará cuando se cierre o desconecte.
<code>root/ConnectionType/telnet/connections/<UUID>/autostart</code>	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.
<code>root/ConnectionType/telnet/connections/<UUID>/backgroundColor</code>	Establece el color de fondo de la conexión.
<code>root/ConnectionType/telnet/connections/<UUID>/beforeStartingCommand</code>	Establece que se ejecute el comando antes de que empiece la conexión.
<code>root/ConnectionType/telnet/connections/<UUID>/connectionEndAction</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/telnet/connections/<UUID>/coord</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/telnet/connections/<UUID>/dependConnectionId</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/telnet/connections/<UUID>/extraEnvValues/<UUID>/key</code>	Establece el nombre de una variable de entorno adicional para su uso con la conexión.

Clave de registro	Descripción
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 de seguridad 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.
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 <code>Default Connection</code> 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>/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 establece en el valor predeterminado <code>focus</code> y la conexión ya se ha iniciado, la conexión se concentrará. De lo contrario, se muestra 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 arranca 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 arranca el el Administrador de conexión General para este tipo de conexión. No debería ser necesario modificar esta clave.
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.
root/ConnectionType/telnet/coreSettings/label	Establece el nombre que se va a mostrar para este tipo de conexión en la interfaz de usuario.

Clave de registro	Descripción
<code>root/ConnectionType/telnet/coreSettings/priorityInConnectionLists</code>	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.
<code>root/ConnectionType/telnet/coreSettings/serverRequired</code>	Establece si un nombre o dirección de servidor es <code>unused</code> , <code>optional</code> o <code>required</code> para este tipo de conexión.
<code>root/ConnectionType/telnet/coreSettings/stopProcess</code>	Establece el comportamiento que debería ocurrir cuando se llama <code>connection-mgr stop</code> en esta conexión. De forma predeterminada, esta opción es <code>close</code> , lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como <code>kill</code> , el proceso especificado por <code>appName</code> se interrumpirá de forma forzada. Cuando se establece como <code>custom</code> se ejecutará una línea de comandos de ejecución personalizada especificada por <code>wrapperScript</code> con el argumento <code>stop</code> para finalizar el proceso correctamente.
<code>root/ConnectionType/telnet/coreSettings/wrapperScript</code>	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Esta es la línea de comandos principal que maneja todas las configuraciones de la conexión y los argumentos de la línea de comandos para la conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/telnet/gui/TelnetManager/name</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/telnet/gui/TelnetManager/status</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/telnet/gui/TelnetManager/title</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/address</code>	Controla el estado del widget Dirección en el Administrador de conexión Telnet. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/autoReconnect</code>	Controla el estado del widget Reconexión automática en el Administrador de conexión Telnet. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/autostart</code>	Controla el estado del widget Prioridad de inicio automático en el Administrador de conexión Telnet. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/backgroundColor</code>	Controla el estado del widget Color de segundo plano en el Administrador de conexión Telnet. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget

Clave de registro	Descripción
	queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/fallBackConnection</code>	Controla el estado del widget Conexión de seguridad en el Administrador de conexión Telnet. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/foregroundColor</code>	Controla el estado del widget Color de primer plano en el Administrador de conexión Telnet. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/hasDesktopIcon</code>	Controla el estado del widget Mostrar ícono en escritorio en el Administrador de conexión Telnet. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/label</code>	Controla el estado del widget Nombre en el Administrador de conexión Telnet. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/port</code>	Controla el estado del widget Puerto en el Administrador de conexión Telnet. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/waitForNetwork</code>	Controla el estado del widget Esperando por red antes de conectar en el Administrador de conexión Telnet. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.

view

Clave de registro	Descripción
<code>root/ConnectionType/view/authorizations/user/add</code>	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.
<code>root/ConnectionType/view/authorizations/user/commandLineBox</code>	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.

Clave de registro	Descripción
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 <code>view_client --help 0 vmware-view --help</code> 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>/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>/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 inmediatamente. Esta configuración solo surte efecto cuando <code>autoReconnect</code> 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	Establece la cantidad de tiempo en segundos que se deben esperar antes de la conexión se inicie después de que arranque el sistema. El valor predeterminado 0 hará que la conexión se inicie inmediatamente. Esta configuración solo surte efecto cuando <code>autostart</code> se establece en 1.
root/ConnectionType/view/connections/<UUID>/beforeStartingCommand	Establece que se ejecute el comando antes de que empiece la conexión.

Clave de registro	Descripción
<code>root/ConnectionType/view/connections/<UUID>/closeAfterDisconnect</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/closeAfterRoaming</code>	Si se establece en 1, la conexión VMware se desconectará si se lleva a otro lugar.
<code>root/ConnectionType/view/connections/<UUID>/coord</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/view/connections/<UUID>/credentialsType</code>	Especifica el tipo de credencial entre <code>anonymous</code> (acceso no autenticado), <code>sso</code> (inicio de sesión único), <code>startup</code> (las credenciales se solicitan en el inicio), <code>password</code> (contraseña/dominio/usuario preconfigurados) o <code>smartcard</code> (smart card preconfigurada).
<code>root/ConnectionType/view/connections/<UUID>/dependConnectionId</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/view/connections/<UUID>/desktop</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/desktopSize</code>	Establece el tamaño en el que el cliente de VMware Horizon View iniciará el escritorio.
<code>root/ConnectionType/view/connections/<UUID>/directory</code>	
<code>root/ConnectionType/view/connections/<UUID>/disableMaximizedApp</code>	Si se establece en 1, se desactiva la configuración de tamaño de ventana para aplicaciones maximizadas.
<code>root/ConnectionType/view/connections/<UUID>/domain</code>	Establece el dominio que se proporciona al View Connection Server. Si no hay ningún dominio especificado, se utiliza el dominio predeterminado para el servidor.
<code>root/ConnectionType/view/connections/<UUID>/enableMMR</code>	Si se establece en 1, se activa el complemento <code>Multimedia Redirection</code> . 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.
<code>root/ConnectionType/view/connections/<UUID>/enableSingleMode</code>	
<code>root/ConnectionType/view/connections/<UUID>/extraEnvValues/<UUID>/key</code>	Establece el nombre de una variable de entorno adicional para su uso con la conexión.
<code>root/ConnectionType/view/connections/<UUID>/extraEnvValues/<UUID>/value</code>	Establece el valor de una variable de entorno adicional para su uso con la conexión.
<code>root/ConnectionType/view/connections/<UUID>/fallBackConnection</code>	Establece la conexión de seguridad a través de su UUID.
<code>root/ConnectionType/view/connections/<UUID>/fullscreen</code>	Si se establece en 1, el cliente de VMware Horizon View abre en modo de pantalla completa cuando inicia.
<code>root/ConnectionType/view/connections/<UUID>/hasDesktopIcon</code>	Si se establece en 1, se activa el icono del escritorio para esta conexión. Esta tecla no tiene efecto en Smart Zero.

Clave de registro	Descripción
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>/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 <code>Default Connection</code> 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.
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 se muestra pero desactivada. Si se establece en 0, la casilla de verificación está oculta.
root/ConnectionType/view/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 desactivado. Si se establece en 0, el botón queda oculto.
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 se muestra pero desactivada. 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>/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	

Clave de registro	Descripción
<code>root/ConnectionType/view/connections/<UUID>/server</code>	Establece la dirección del host remoto al cual conectarse. Normalmente es una URL como <code>http://server.domain.com</code> .
<code>root/ConnectionType/view/connections/<UUID>/sessionEndAction</code>	
<code>root/ConnectionType/view/connections/<UUID>/singleDesktop</code>	
<code>root/ConnectionType/view/connections/<UUID>/smartcard</code>	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 solo permite el inicio de sesión de la smart card en el host remoto, no en View Connection Server.
<code>root/ConnectionType/view/connections/<UUID>/startMode</code>	Si se establece en el valor predeterminado <code>focus</code> y la conexión ya se ha iniciado, la conexión se concentrará. De lo contrario, se muestra un error que indica que la conexión ya se ha iniciado.
<code>root/ConnectionType/view/connections/<UUID>/username</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/viewSecurityLevel</code>	Si se establece como <code>Refuse insecure connections</code> 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 <code>Warn</code> , 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 <code>Allow all connections</code> , el certificado del servidor no se verificará y se permitirán las conexiones a cualquier servidor.
<code>root/ConnectionType/view/connections/<UUID>/waitForNetwork</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/attachToConsole</code>	
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/audioLatency</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/clipboardExtension</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/colorDepth</code>	No se recomienda este ajuste. 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 color a un nivel no admitido por el controlador de video puede causar daños en la pantalla o generar fallos.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/compression</code>	Si se establece en 1, se activa la compresión de datos RDP entre el cliente y el servidor.

Clave de registro	Descripción
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/disableMMRwithRFX</code>	Si se establece en 1, se desactiva la redirección de contenido multimedia en caso de que se establezca una sesión RemoteFX válida.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/frameAcknowledgeCount</code>	Establece el número de fotogramas de video que el servidor puede forzar sin tener que esperar el reconocimiento desde el cliente. Los números inferiores dan por resultado un escritorio con mayor capacidad de respuesta 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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/general/sendHostname</code>	Si se establece en <code>hostname</code> , 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 <code>sendHostname</code> en la configuración específica para la conexión. Si se establece en <code>mac</code> , en vez del nombre de host, se envía la dirección MAC del primer adaptador de red disponible.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/loadBalanceInfo</code>	Este valor es la cookie de equilibrio de carga enviado al servidor para fines de intermediación tras la conexión y corresponde al campo <code>loadbalanceinfo</code> en el archivo <code>.rdp</code> . De forma predeterminada, el valor está vacío.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/mouseMotionEvents</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/offScreenBitmaps</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagDesktopComposition</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagFontSmoothing</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoCursorSettings</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoCursorShadow</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoMenuAnimations</code>	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.

Clave de registro	Descripción
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoTheming</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoWallpaper</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoWindowDrag</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/portMapping</code>	Si se establece en 1, los siguientes puertos seriales y paralelos se redirigen al host remoto: ttyS0, ttyS1, ttyS2, ttyS3, ttyUSB0, lp0.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/printerMapping</code>	Si se establece en 1, todas las impresoras definidas localmente a través de CUPS se redirigen al host remoto.
<code>root/ConnectionType/freerdp/connections/<UUID>/rdp6Buffering</code>	Si se establece en 1, aumenta el rendimiento de gráficos que no son RemoteFX aunque las actualizaciones serán menos frecuentes.
<code>root/ConnectionType/freerdp/connections/<UUID>/rdp8Codecs</code>	Si se establece en 1, se utilizan códecs RDP 8 si están disponibles. Este ajuste debe desactivarse solo en el caso de un defecto específico de los códecs RDP 8. Al desactivar este ajuste también podrían desactivarse códecs más avanzados.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/rdpEncryption</code>	Si se establece en 1, la encriptación RDP estándar se utiliza para encriptar todos los datos entre el cliente y el servidor.
<code>root/ConnectionType/freerdp/connections/<UUID>/rdpH264Codec</code>	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.
<code>root/ConnectionType/freerdp/connections/<UUID>/rdpProgressiveCodec</code>	Si se establece en 1, se utilizan códecs progresivos RDP 8 si están disponibles. Este ajuste debe desactivarse solo en el caso de un defecto específico en los códecs progresivos RDP 8. Al desactivar este ajuste también podrían desactivarse códecs más avanzados.
<code>root/ConnectionType/freerdp/connections/<UUID>/redirectPreference</code>	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 <code>auto</code> fuerza el orden original.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/remoteFx</code>	Si se establece en 1, se utiliza RemoteFX en caso de que esté disponible.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/sendHostname</code>	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 <code>root/ConnectionType/view/connections/<UUID>/</code>

Clave de registro	Descripción
	<code>xfreerdpOptions/general/sendHostname</code> en <code>hostname</code> para que se use esta clave.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/sound</code>	Si se establece en <code>Bring to this computer</code> el sonido se redirigirá desde el host remoto al cliente mediante un canal virtual estándar. Si se establece en <code>Leave at remote computer</code> , 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 <code>Bring to this computer</code> 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 <code>Multimedia Redirection</code>) coincida con la configuración de audio local.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutError</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutRecovery</code>	Establece el número de milisegundos de espera después de perder la conexión para que la red se recupere sin tratar de forzar una reconexión.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutWarning</code>	Establece el número de milisegundos de espera después de perder la conexión antes de advertirle al usuario que la conexión se ha perdido.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutWarningDialog</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutsEnabled</code>	Si se establece en 1, se realizan las verificaciones de estado de la conexión de extremo a extremo.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/tlsVersion</code>	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.
<code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/xkbLayoutId</code>	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: <code>xfreerdp --kbd-list</code> .
<code>root/ConnectionType/view/coreSettings/USBrelevant</code>	Indica si este tipo de conexión es relevante para el USB. Si es así, puede tener un complemento USB para redirigir dispositivos USB.
<code>root/ConnectionType/view/coreSettings/appName</code>	Establece el nombre de la aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/view/coreSettings/className</code>	Establece el nombre de la clase de aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/view/coreSettings/editor</code>	Establece el nombre de la aplicación interna que se utiliza cuando se arranca el Administrador de conexión para este tipo de conexión. No debería ser necesario modificar esta clave.

Clave de registro	Descripción
<code>root/ConnectionType/view/coreSettings/icon16Path</code>	Establece la ruta al icono de 16 x 16 píxeles para esta aplicación.
<code>root/ConnectionType/view/coreSettings/icon32Path</code>	Establece la ruta al icono de 32 x 32 píxeles para esta aplicación.
<code>root/ConnectionType/view/coreSettings/icon48Path</code>	Establece la ruta al icono de 48 x 48 píxeles para esta aplicación.
<code>root/ConnectionType/view/coreSettings/label</code>	Establece el nombre que se va a mostrar para este tipo de conexión en la interfaz de usuario.
<code>root/ConnectionType/view/coreSettings/priorityInConnectionLists</code>	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.
<code>root/ConnectionType/view/coreSettings/serverRequired</code>	Establece si un nombre o dirección de servidor es <code>unused</code> , <code>optional</code> o <code>required</code> para este tipo de conexión.
<code>root/ConnectionType/view/coreSettings/stopProcess</code>	Establece el comportamiento que debería ocurrir cuando se llama <code>connection-mgr stop</code> en esta conexión. De forma predeterminada, esta opción es <code>close</code> , lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como <code>kill</code> , el proceso especificado por <code>appName</code> se interrumpirá de forma forzada. Cuando se establece como <code>custom</code> se ejecutará una línea de comandos de ejecución personalizada especificada por <code>wrapperScript</code> con el argumento <code>stop</code> para finalizar el proceso correctamente.
<code>root/ConnectionType/view/coreSettings/watchPid</code>	Si se establece en 1, la conexión se supervisa bajo el nombre especificado por <code>appName</code> . No debería ser necesario modificar esta clave.
<code>root/ConnectionType/view/coreSettings/wrapperScript</code>	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Esta es la línea de comandos principal que maneja todas las configuraciones de la conexión y los argumentos de la línea de comandos para la conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/view/coreSettings/wrapperScriptGeneration</code>	Permite que el Administrador de conexión sepa qué tipo de parámetros aprueban el script.
<code>root/ConnectionType/view/general/rdpOptions</code>	Las opciones que se especifican aquí se enviarán directamente al cliente RDP si RDP se utiliza como protocolo de visualización para la conexión VMware Horizon View. Para ver una lista completa de opciones, introduzca el siguiente comando en un terminal X: <code>rdesktop --help</code>
<code>root/ConnectionType/view/gui/viewManager/name</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/view/gui/viewManager/status</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/view/gui/viewManager/title</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/view/gui/viewManager/widgets/autostart</code>	Controla el estado del widget Prioridad de inicio automático en el Administrador de conexión VMware Horizon View. Si se

Clave de registro	Descripción
	establece como <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/view/gui/viewManager/widgets/fallBackConnection</code>	Controla el estado del widget Conexión de seguridad en el Administrador de conexión VMware Horizon View. Si se establece como <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/view/gui/viewManager/widgets/label</code>	Controla el estado del widget Nombre en el Administrador de conexión VMware Horizon View. Si se establece como <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , el widget puede verse en el modo de solo lectura.

xdmcp

Clave de registro	Descripción
<code>root/ConnectionType/xdmcp/authorizations/user/add</code>	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.
<code>root/ConnectionType/xdmcp/authorizations/user/general</code>	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.
<code>root/ConnectionType/xdmcp/connections/<UUID>/address</code>	Establece el nombre de host o la dirección IP a la cual conectarse.
<code>root/ConnectionType/xdmcp/connections/<UUID>/afterStartedCommand</code>	Establece el comando que se debe ejecutar después de que se ha iniciado la conexión.
<code>root/ConnectionType/xdmcp/connections/<UUID>/afterStoppedCommand</code>	Establece el comando que se debe ejecutar después de que se ha detenido la conexión.
<code>root/ConnectionType/xdmcp/connections/<UUID>/authorizations/user/edit</code>	Si se establece en 1, un usuario final tiene permiso para modificar las configuraciones para esta conexión.
<code>root/ConnectionType/xdmcp/connections/<UUID>/authorizations/user/execution</code>	Si se establece en 1, un usuario final tiene permiso para ejecutar esta conexión.
<code>root/ConnectionType/xdmcp/connections/<UUID>/autoReconnect</code>	Si se establece en 1, la conexión se reiniciará cuando se cierre o desconecte.
<code>root/ConnectionType/xdmcp/connections/<UUID>/autostart</code>	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.
<code>root/ConnectionType/xdmcp/connections/<UUID>/beforeStartingCommand</code>	Establece que se ejecute el comando antes de que empiece la conexión.
<code>root/ConnectionType/xdmcp/connections/<UUID>/color</code>	Establece la profundidad de color de la pantalla de la conexión.

Clave de registro	Descripción
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 de seguridad 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 <code>useFontServer</code> 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>/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 <code>Default Connection</code> y no aparece en la interfaz de usuario.
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 establece en el valor predeterminado <code>focus</code> y la conexión ya se ha iniciado, la conexión se concentrará. De lo contrario, se muestra 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 <code>chooser</code> , todos los hosts se enumeran y el usuario puede seleccionar el host al cual desea conectarse. Si se configura en <code>query</code> , se envía una solicitud XDMCP directamente al host especificado. Si se configura en <code>broadcast</code> , 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.

Clave de registro	Descripción
<code>root/ConnectionType/xdmcp/coreSettings/audio</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/xdmcp/coreSettings/className</code>	Establece el nombre de la clase de aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/xdmcp/coreSettings/desktopButton</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/xdmcp/coreSettings/editor</code>	Establece el nombre de la aplicación interna que se utiliza cuando se arranca el Administrador de conexión para este tipo de conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/xdmcp/coreSettings/generalSettingsEditor</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/xdmcp/coreSettings/icon16Path</code>	Establece la ruta al icono de 16 x 16 píxeles para esta aplicación.
<code>root/ConnectionType/xdmcp/coreSettings/icon32Path</code>	Establece la ruta al icono de 32 x 32 píxeles para esta aplicación.
<code>root/ConnectionType/xdmcp/coreSettings/icon48Path</code>	Establece la ruta al icono de 48 x 48 píxeles para esta aplicación.
<code>root/ConnectionType/xdmcp/coreSettings/label</code>	Establece el nombre que se va a mostrar para este tipo de conexión en la interfaz de usuario.
<code>root/ConnectionType/xdmcp/coreSettings/priorityInConnectionLists</code>	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.
<code>root/ConnectionType/xdmcp/coreSettings/serverRequired</code>	Establece si un nombre o dirección de servidor es <code>unused</code> , <code>optional</code> o <code>required</code> para este tipo de conexión.
<code>root/ConnectionType/xdmcp/coreSettings/stopProcess</code>	Establece el comportamiento que debería ocurrir cuando se llama <code>connection_mgr stop</code> en esta conexión. De forma predeterminada, esta opción es <code>close</code> , lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como <code>kill</code> , el proceso especificado por <code>appName</code> se interrumpirá de forma forzada. Cuando se establece como <code>custom</code> se ejecutará una línea de comandos de ejecución personalizada especificada por <code>wrapperScript</code> con el argumento <code>stop</code> para finalizar el proceso correctamente.
<code>root/ConnectionType/xdmcp/coreSettings/watchPid</code>	Si se establece en 1, la conexión se supervisa bajo el nombre especificado por <code>appName</code> . No debería ser necesario modificar esta clave.
<code>root/ConnectionType/xdmcp/coreSettings/wrapperScript</code>	Establece la línea de comandos o código binario a ejecutar al iniciar este tipo de conexión. Esta es la línea de comandos principal que maneja todos los ajustes de la conexión y los argumentos de la línea de comandos para la conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/xdmcp/gui/XdmcpManager/name</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.

Clave de registro	Descripción
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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , el widget puede verse en el modo de solo lectura.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/autoReconnect	Controla el estado del widget Reconexión automática en el Administrador de conexión XDMCP. Si se establece como <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , 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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , 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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , 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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , 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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , 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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , el widget puede verse en el modo de solo lectura.

Clave de registro	Descripción
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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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

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 <code>http://server.domain.com</code> .
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>/appInMenu	Si se establece en 1, todas las aplicaciones de la conexión se mostrarán en el menú de la barra de tareas.
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.
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 solo devuelve una única aplicación publicada o un solo escritorio, ese recurso se iniciará automáticamente.

Clave de registro	Descripción
<code>root/ConnectionType/xen/connections/<UUID>/autoReconnect</code>	Si se establece en 1, la conexión se reiniciará cuando se cierre o desconecte.
<code>root/ConnectionType/xen/connections/<UUID>/autoReconnectAppsOnLogin</code>	Si se establece en 1, el sistema intentará reconectar cualquier sesión Citrix activa o desconectada después del inicio de sesión original.
<code>root/ConnectionType/xen/connections/<UUID>/autoReconnectDelay</code>	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 <code>autoReconnect</code> se establece en 1.
<code>root/ConnectionType/xen/connections/<UUID>/autoRefreshInterval</code>	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.
<code>root/ConnectionType/xen/connections/<UUID>/autoStartDesktop</code>	Si se establece en 1 y <code>autoStartResource</code> está vacío, se iniciará automáticamente el primer escritorio que esté disponible cuando se arranca la conexión.
<code>root/ConnectionType/xen/connections/<UUID>/autoStartResource</code>	Establece el nombre del escritorio o la aplicación que se iniciará automáticamente cuando se arranca la conexión.
<code>root/ConnectionType/xen/connections/<UUID>/autostart</code>	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.
<code>root/ConnectionType/xen/connections/<UUID>/autostartDelay</code>	Establece la cantidad de tiempo en segundos que se deben esperar antes de la conexión se inicie después de que arranque el sistema. El valor predeterminado 0 hará que la conexión se inicie inmediatamente. Esta configuración solo surte efecto cuando <code>autostart</code> se establece en 1.
<code>root/ConnectionType/xen/connections/<UUID>/beforeStartingCommand</code>	Establece que se ejecute el comando antes de que empiece la conexión.
<code>root/ConnectionType/xen/connections/<UUID>/connectionMode</code>	Establece el modo de conexión Citrix para la conexión.
<code>root/ConnectionType/xen/connections/<UUID>/connectionStopAction</code>	Define la acción que se realizará cuando termine la conexión del Administrador de conexiones disponibles son <code>disconnect</code> y <code>logoff</code> .
<code>root/ConnectionType/xen/connections/<UUID>/coord</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/xen/connections/<UUID>/credentialsType</code>	Especifica el tipo de credencial entre <code>anonymous</code> (acceso no autenticado), <code>sso</code> (inicio de sesión único), <code>startup</code> (las credenciales se solicitan en el inicio), <code>password</code> (contraseña/dominio/usuario preconfigurados) o <code>smartcard</code> (smart card preconfigurada).
<code>root/ConnectionType/xen/connections/<UUID>/dependConnectionId</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/ConnectionType/xen/connections/<UUID>/domain</code>	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.
<code>root/ConnectionType/xen/connections/<UUID>/enableRSAToken</code>	PRECAUCIÓN: Esta funcionalidad no es compatible.

Clave de registro	Descripción
	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 de seguridad 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 arranca.
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>/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 Conexión predeterminada 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.
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 se muestra pero desactivada. Si se establece en 0, la casilla de verificación está oculta.
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 desactivado. 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 se muestra pero desactivada. 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.

Clave de registro	Descripción
<code>root/ConnectionType/xen/connections/<UUID>/loginfields/username</code>	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.
<code>root/ConnectionType/xen/connections/<UUID>/password</code>	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.
<code>root/ConnectionType/xen/connections/<UUID>/resListRequest</code>	Si se establece en 1, una conexión solo enumera los recursos sin iniciarlos o descargar los iconos.
<code>root/ConnectionType/xen/connections/<UUID>/saveNewUrl</code>	Este es un valor interno. Si se establece en <code>ToBeAsked</code> , el script hace la solicitud al usuario. Si se establece en <code>Auto</code> , el script no hace la solicitud al usuario y la URL se guarda según el caso. Si se establece en <code>Yes</code> , se pide al usuario que guarde la nueva URL. Si se establece en <code>No</code> , se pide al usuario que no guarde la nueva URL.
<code>root/ConnectionType/xen/connections/<UUID>/savePassword</code>	
<code>root/ConnectionType/xen/connections/<UUID>/smartCardModuleKey</code>	Especifica el módulo de seguridad que se va a utilizar para una conexión de smart card.
<code>root/ConnectionType/xen/connections/<UUID>/startMode</code>	Si se establece en el valor predeterminado <code>focus</code> y la conexión ya se ha iniciado, la conexión se concentrará. De lo contrario, se muestra un error que indica que la conexión ya se ha iniciado.
<code>root/ConnectionType/xen/connections/<UUID>/subscribedOnly</code>	Si se establece en 1, solo se muestran los recursos suscritos para la conexión.
<code>root/ConnectionType/xen/connections/<UUID>/unplugSmartCardAction</code>	Establece la acción que se realizará cuando una smart card se desconecta durante la conexión. <code>disconnect</code> desconectará la sesión actual. <code>close</code> cerrará todos los recursos abiertos. <code>noaction</code> no hará nada.
<code>root/ConnectionType/xen/connections/<UUID>/username</code>	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.
<code>root/ConnectionType/xen/connections/<UUID>/waitForNetwork</code>	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.
<code>root/ConnectionType/xen/coreSettings/USBrelevant</code>	Especifica si este tipo de conexión es relevante para el USB. Si es así, puede tener un complemento USB para redirigir dispositivos USB.
<code>root/ConnectionType/xen/coreSettings/appName</code>	Establece el nombre de la aplicación interna que se utiliza para este tipo de conexión. No debería ser necesario modificar esta clave.
<code>root/ConnectionType/xen/coreSettings/autoLogoutDelayAfterLaunch</code>	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

Clave de registro	Descripción
	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 arranca 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/editor	Establece el nombre de la aplicación interna que se utiliza cuando se arranca 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 arranca el el Administrador de conexión General para este tipo de conexión. No debería ser necesario modificar esta clave.
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/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 <code>unused</code> , <code>optional</code> o <code>required</code> para este tipo de conexión.
root/ConnectionType/xen/coreSettings/ stopProcess	Establece el comportamiento que debería ocurrir cuando se llama <code>connection-mgr stop</code> en esta conexión. De forma predeterminada, esta opción es <code>close</code> , lo que enviará una señal estándar de interrupción del proceso. Cuando se establece como <code>kill</code> , el proceso especificado por <code>appName</code> se interrumpirá de forma forzada. Cuando se establece como <code>custom</code> se ejecutará una línea de comandos de ejecución personalizada especificada por <code>wrapperScript</code> con el argumento <code>stop</code> para finalizar el proceso correctamente.

Clave de registro	Descripción
root/ConnectionType/xen/coreSettings/watchPid	Si se establece en 1, la conexión se supervisa bajo el nombre especificado por <code>appName</code> . 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. Esta es la línea de comandos principal que maneja todas las configuraciones de la conexión y los argumentos de la línea de comandos para la conexión. No debería ser necesario modificar esta clave.
root/ConnectionType/xen/coreSettings/wrapperScriptGeneration	Permite que el Administrador de conexión sepa qué tipo de parámetros aprueban el script.
root/ConnectionType/xen/general/CGPAddress	<p>Especifica la dirección de CGP mediante la sintaxis <code>hostname:port</code>.</p> <p>Como opción, en vez de especificar el nombre de host, puede escribir un asterisco (*). Esto usará el valor de la clave de registro <code>address</code> de la conexión como host. Por ejemplo: <code>*:2598</code></p> <p>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.</p>
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 <code>.ini</code> de Citrix <code>TWIMode</code> .
root/ConnectionType/xen/general/TWIModeResizeType	Esta configuración se asigna directamente a la configuración del archivo <code>.ini</code> de Citrix <code>TWIMoveResizeType</code> .
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 <code>.ini</code> de Citrix <code>CommPollSize</code> .
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 <code>autoReconnect</code> específica de la conexión. Ocurre internamente en el cliente Citrix sin reiniciar la conexión. Esta configuración se asigna directamente a la configuración del archivo <code>.ini</code> de Citrix <code>TransportReconnectEnabled</code> .
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 <code>.ini</code> de Citrix <code>PersistentCacheMinBitmap</code> .
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 <code>Shared - Approximate Colors</code> , se usan colores aproximados del mapa de colores predeterminado.

Clave de registro	Descripción
	Si se establece en <code>Private - Exact Colors</code> , se utilizan colores precisos. Esta configuración se asigna directamente a la configuración del archivo <code>.ini</code> de Citrix <code>ApproximateColors</code> .
<code>root/ConnectionType/xen/general/contentRedirection</code>	Si se establece en 1, se envían enlaces del contenido web del servidor al cliente para que éste pueda tratar de abrirlos localmente.
<code>root/ConnectionType/xen/general/defaultBrowserProtocol</code>	Controla el protocolo utilizado para ubicar el host de la conexión. Si se especifica, se usa el valor predeterminado de la sección <code>[WFClient]</code> de <code>wfclient.ini</code> . Esta configuración se asigna directamente a la configuración del archivo <code>.ini</code> de Citrix <code>BrowserProtocol</code> .
<code>root/ConnectionType/xen/general/drivePathMappedOnA ... drivePathMappedOnZ</code>	Establece el directorio filesystem local que se asigna al host remoto. Normalmente, se establece como <code>/media</code> para permitir que todas las unidades USB conectadas se asocien al host remoto a través de una sola letra de unidad.
<code>root/ConnectionType/xen/general/enableAlertSound</code>	Si se establece en 1, se activan sonidos de alerta de Windows. Esta configuración se asigna indirectamente a la configuración de archivo <code>.ini</code> de Citrix <code>DisableSound</code> .
<code>root/ConnectionType/xen/general/enableClipboard</code>	Si se establece en 1, se activa la redirección del portapapeles.
<code>root/ConnectionType/xen/general/enableConnectionBar</code>	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.
<code>root/ConnectionType/xen/general/enableCursorColors</code>	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.
<code>root/ConnectionType/xen/general/enableDataCompression</code>	Si se establece en 1, se activa la compresión de datos. Esta configuración se asigna directamente a la configuración del archivo <code>.ini</code> de Citrix <code>Compress</code> .
<code>root/ConnectionType/xen/general/enableDriveMapAndRedirect</code>	Si se establece en 1, se activan la asignación y la redirección de dispositivos de almacenamiento USB.
<code>root/ConnectionType/xen/general/enableDriveMapping</code>	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, <code>/media</code> se asigna a <code>Z</code> 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 asignarse correctamente al host remoto en este modo, el dispositivo USB debe utilizar uno de los siguientes sistemas de archivos: FAT32, NTFS, ext2, ext3.
<code>root/ConnectionType/xen/general/enableDynamicDriveMapping</code>	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.
<code>root/ConnectionType/xen/general/enableH264Compression</code>	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.

Clave de registro	Descripción
root/ConnectionType/xen/general/enableHDXFlashRedirection	<p>NOTA: Este recurso solo se admite en la versión de 32 bits de HP ThinPro.</p> <p>Controla el comportamiento de Redirección de HDX Flash. Si se establece en <i>Always</i>, se usa Redirección de HDX Flash si es posible y no se avisa nada al usuario. Si se establece en <i>Ask</i>, se avisa al usuario. Si se establece en <i>Never</i>, se desactiva el recurso.</p>
root/ConnectionType/xen/general/enableHDXFlashServerContentFetch	<p>NOTA: Este recurso solo se admite en la versión de 32 bits de HP ThinPro.</p> <p>Controla el comportamiento de Recoger el contenido del lado del servidor HDX Flash. Si está desactivado, el cliente buscará el contenido.</p>
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 <code>enableH264Compression</code> , 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 <code>drivePathMappedOn</code> 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 <code>X PixMap</code> 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 <code>EnableOSS</code> .
root/ConnectionType/xen/general/enableSessionReliability	Si se establece en 1, se activa Confiabilidad de la sesión de Citrix. 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 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 <code>enableTextTracking</code> 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/enableTextTracking	Si se establece en 1, se activan superposiciones optimizadas sin pérdidas para H.264.
root/ConnectionType/xen/general/enableUSBRedirection	Si se establece en 1, se redirigirán los dispositivos de almacenamiento USB.

Clave de registro	Descripción
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/lastComPortNum	Establece el número de puertos seriales asignados. Si se establece en 0, se desactiva 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, solo 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 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

Clave de registro	Descripción
	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/serverCheckTimeout	
root/ConnectionType/xen/general/sessionReliabilityTTL	Especifica el tiempo de espera de confiabilidad de la sesión en segundos. Esto configura el Confiabilidad de la sesión Time To Live (TTL).
root/ConnectionType/xen/general/sessionSharingClient	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/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 principal para mostrar el escritorio virtual. Si se establece en 0, el monitor no se usará para mostrar el escritorio virtual.

Clave de registro	Descripción
root/ConnectionType/xen/general/transparentKeyPassthrough	Controla cómo se administran ciertas combinaciones de teclas de Windows. Si se establece en <code>Translated</code> , las combinaciones de teclas se aplican al escritorio local. Si se establece <code>Direct in full screen desktops only</code> , las combinaciones de teclas se aplican a la sesión remota solo cuando está en modo de pantalla completa. Si se establece en <code>Direct</code> , 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 <code>.ini</code> de Citrix <code>TransparentKeyPassthrough</code> .
root/ConnectionType/xen/general/twRedundantImageItems	Controla el número de áreas de la pantalla que se siguen en <code>ThinWire</code> 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 <code>.ini</code> de Citrix <code>UseAlternateAddress</code> .
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 se asigna directamente a la configuración del archivo <code>.ini</code> de Citrix <code>PersistentCacheEnabled</code> .
root/ConnectionType/xen/general/useEUKS	Controla el uso de <code>Extended Unicode Keyboard Support (EUKS)</code> 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 <code>.ini</code> de Citrix <code>useLocalIME</code> .
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 <code>HDXWebCamFramesPerSec</code> en el archivo <code>All_Regions.ini</code> .
root/ConnectionType/xen/general/webcamSupport	Si se establece en 0, la cámara web y el audio de la cámara web se desactivan. Si se establece en 1, la cámara web y el audio de la cámara web se activan, con compresión. Si se establece en 2, se activa la redirección USB de la cámara web y el audio de la cámara web.
root/ConnectionType/xen/general/windowHeight	Establece la altura de la ventana en píxeles si <code>windowSize</code> se establece en <code>Fixed Size</code> .

Clave de registro	Descripción
root/ConnectionType/xen/general/windowPercent	Establece el tamaño de la ventana como un porcentaje si <code>windowSize</code> se establece en <code>Percentage of Screen Size</code> .
root/ConnectionType/xen/general/windowSize	Si se establece en <code>Default</code> , se utilizan las configuraciones del lado del servidor. Si se establece en <code>Full Screen</code> , la ventana se maximiza sin bordes en todas las pantallas disponibles. Si se establece en <code>Fixed Size</code> , se pueden utilizar las claves de registro <code>windowWidth</code> y <code>windowHeight</code> para especificar el tamaño de la ventana en píxeles. Si se establece en <code>Percentage of Screen Size</code> , puede utilizarse la clave <code>windowPercent</code> para especificar el tamaño de la ventana como un porcentaje. Para que <code>Percentage of Screen Size</code> entre en efecto, se deben establecer <code>enableForceDirectConnect</code> en 1 y <code>TWIMode</code> en 0. Esta configuración solo funciona con <code>XenApp</code> y solo en caso de que el servidor permita conexiones directas. Esta configuración no funciona con <code>XenDesktop</code> .
root/ConnectionType/xen/general/windowWidth	Establece el ancho de la ventana en píxeles si <code>windowSize</code> se establece en <code>Fixed Size</code> .
root/ConnectionType/xen/gui/XenDesktopPanel/disabled	Si se establece en 1, el panel de <code>Xen Desktop</code> y su barra de tareas se desactivan. Esto suele utilizarse cuando <code>autoStartResource</code> o <code>autoStartDesktop</code> 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget

Clave de registro	Descripción
	queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/xen/gui/XenManager/widgets/autoStartDesktop</code>	Controla el estado del widget Iniciar automáticamente el escritorio en el Administrador de conexión Citrix. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/xen/gui/XenManager/widgets/autoStartResource</code>	Controla el estado del widget Iniciar recurso automáticamente en el Administrador de conexión Citrix. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/xen/gui/XenManager/widgets/autostart</code>	Controla el estado del widget Prioridad de inicio automático en el Administrador de conexión Citrix. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/xen/gui/XenManager/widgets/domain</code>	Controla el estado del widget Dominio en el Administrador de conexión Citrix. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/xen/gui/XenManager/widgets/fallBackConnection</code>	Controla el estado del widget Conexión de seguridad en el Administrador de conexión Citrix. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/xen/gui/XenManager/widgets/folder</code>	
<code>root/ConnectionType/xen/gui/XenManager/widgets/hasDesktopIcon</code>	Controla el estado del widget Mostrar icono en escritorio en el Administrador de conexión Citrix. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/xen/gui/XenManager/widgets/label</code>	Controla el estado del widget Nombre en el Administrador de conexión Citrix. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/xen/gui/XenManager/widgets/password</code>	Controla el estado del widget Contraseña en el Administrador de conexión Citrix. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.

Clave de registro	Descripción
<code>root/ConnectionType/xen/gui/XenManager/widgets/username</code>	Controla el estado del widget Nombre de usuario en el Administrador de conexión Citrix. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/xen/gui/XenManager/widgets/waitForNetwork</code>	Controla el estado del widget Esperando por red antes de conectar en el Administrador de conexión Citrix. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/ConnectionType/xen/gui/fbpanel/autohide</code>	Si se establece como <code>true</code> , la barra de tareas se oculta automáticamente.
<code>root/ConnectionType/xen/gui/fbpanel/edge</code>	Establece la posición predeterminada de la barra de tareas cuando más de un escritorio o una aplicación publicados se encuentran disponibles.
<code>root/ConnectionType/xen/gui/fbpanel/hidden</code>	Si se establece en 1, la barra de tareas queda completamente oculta, pero solo si <code>autoStartResource</code> o <code>autoStartDesktop</code> 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

 **NOTA:** El panel es lo mismo que la barra de tareas.

Clave de registro	Descripción
<code>root/Dashboard/GUI/Clock</code>	Si se establece en 1, el reloj se muestra en la barra de tareas.
<code>root/Dashboard/GUI/ConnectionManager</code>	Si se establece en 1, el Administrador de conexión se muestra en la barra de tareas.
<code>root/Dashboard/GUI/ControlPanel</code>	Si se establece en 1, el botón Panel de control se muestra en la barra de tareas.
<code>root/Dashboard/GUI/DomainUser</code>	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.
<code>root/Dashboard/GUI/PowerButton</code>	Si se establece en 1, el botón de inicio/apagado se muestra en la barra de tareas.
<code>root/Dashboard/GUI/PowerButtonPosition</code>	Si se establece en 1, el botón de inicio/apagado se muestra a la derecha de la barra de tareas (en caso de una barra de tareas horizontal) o en la parte inferior (en el caso de una barra de tareas vertical). Si se establece en 0, el botón de inicio/apagado se muestra a la izquierda de la barra de tareas (en caso de una barra de tareas horizontal) o en la parte superior (en el caso de una barra de tareas vertical).

Clave de registro	Descripción
root/Dashboard/GUI/Search	Si se establece en 1, el botón de Búsqueda se muestra en la barra de tareas.
root/Dashboard/GUI/SystemInformation	Si se establece en 1, el botón Información del sistema 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/AlwaysOnTop	Si se establece en 1, la barra de tareas estará siempre en la parte superior.
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 <code>AutoHide</code> está activado.
root/Dashboard/General/IconSize	Establece el tamaño de los iconos 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.
root/Dashboard/General/PanelDockSide	Establece el lado de la pantalla al que se acopla la barra de tareas.
root/Dashboard/General/RemainPixel	Establece el número de píxeles que quedan visibles cuando se oculta 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 <code>AutoHide</code> está activado.
root/Dashboard/General/Width	Establece el ancho de la barra de tareas.

Display

Clave de registro	Descripción
root/Display/Configuration/Hotplug/newMonitorPosition	En las plataformas compatibles, establece dónde deben colocarse los nuevos monitores (a la izquierda o la derecha de los monitores acoplados actualmente) cuando están conectados en caliente.
root/Display/Configuration/displaymode	Establece el modo de visualización. Si se establece en 0, se usa el modo estándar (una configuración de 1-4 monitores). Si se establece en 1, se puede usar una configuración de 6 monitores, pero solo en plataformas compatibles con la tarjeta adicional adecuada.
root/Display/Configuration/hexlayout	Establece la visualización en el modo de seis monitores.
root/Display/Configuration/hexprofile	Establece el perfil que se utiliza en el modo de seis monitores.
root/Display/Configuration/primaryprofile	Establece el perfil que se utiliza para el monitor principal mediante el nombre del perfil. En el caso de Smart Zero, esta opción siempre debe establecerse en <code>default</code> .

Clave de registro	Descripción
<code>root/Display/Configuration/quaternarymode</code>	Establece la posición del cuarto monitor con relación al monitor indicado en <code>quaternaryrelative</code> . Esto depende del hardware y no es compatible con todos los modelos. Los valores se definen de la siguiente forma: 0 = Igual que; 1 = Superior; 2 = A la derecha de; 3 = A la izquierda de; 4 = Inferior.
<code>root/Display/Configuration/quaternaryprofile</code>	Establece el perfil que se utiliza para el cuarto monitor mediante el nombre del perfil.
<code>root/Display/Configuration/quaternaryrelative</code>	Establece cuál monitor se usa como referencia para definir la posición del cuarto monitor.
<code>root/Display/Configuration/secondaryConnector</code>	Establece el conector secundario.
<code>root/Display/Configuration/secondarymode</code>	Establece la posición del monitor secundario con relación al monitor principal. Esto depende del hardware y no es compatible con todos los modelos. Los valores se definen de la siguiente forma: 0 = Igual que; 1 = Superior; 2 = A la derecha de; 3 = A la izquierda de; 4 = Inferior.
<code>root/Display/Configuration/secondaryorientation</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/Display/Configuration/secondaryprofile</code>	Establece el perfil que se utiliza para el monitor secundario mediante el nombre del perfil.
<code>root/Display/Configuration/swapstate</code>	Especifica cuál conector está conectado al monitor principal. Esto depende del hardware y no es compatible con todos los modelos. Por lo general, 0 significa que el monitor principal está en el conector VGA y 1 hace referencia al otro conector. En el caso de t510, 0 significa que el monitor principal está en el conector DVI-I y 1 que el monitor principal está en el conector DVI-D. En el caso de las plataformas con una tarjeta de video adicional, 0 significa que el monitor principal se encuentra en la tarjeta de video incorporada y 1 significa que el monitor principal está en la tarjeta de video adicional.
<code>root/Display/Configuration/tertiarymode</code>	Establece la posición del tercer monitor con relación al monitor indicado en <code>tertiaryrelative</code> . Esto depende del hardware y no es compatible con todos los modelos. Los valores se definen de la siguiente forma: 0 = Igual que; 1 = Superior; 2 = A la derecha de; 3 = A la izquierda de; 4 = Inferior.
<code>root/Display/Configuration/tertiaryprofile</code>	Establece el perfil que se utiliza para el tercer monitor mediante el nombre del perfil.
<code>root/Display/Configuration/tertiaryrelative</code>	Establece cuál monitor se usa como referencia para definir la posición del tercer monitor.
<code>root/Display/Profiles/<UUID>/colorScaling</code>	Establece la temperatura de color o la escalabilidad directa de RGB para thin clients con monitores incorporados. La entrada es un valor hexadecimal de 6 dígitos (RRGGBB), en el que <code>ffffff</code> podría indicar una escala completa (100%) en los tres canales de color.
<code>root/Display/Profiles/<UUID>/depth</code>	Establece la profundidad de color de la pantalla en bits por píxel. Una mayor profundidad de color significa mejor calidad pero menor rendimiento.
<code>root/Display/Profiles/<UUID>/height</code>	Establece la altura de resolución del monitor. Si se establece en 0, la resolución se detecta automáticamente.
<code>root/Display/Profiles/<UUID>/label</code>	Establece el nombre del perfil de pantalla. En el caso de Smart Zero, esta opción siempre debe establecerse en <code>default</code> .

Clave de registro	Descripción
root/Display/Profiles/<UUID>/orientation	Establece la orientación del monitor de la siguiente manera: 0 = Normal; 1 = Girar a la izquierda; 2 = Girar a la derecha; 3 = Invertir.
root/Display/Profiles/<UUID>/refresh	Establece la frecuencia de actualización deseada del monitor. No todas las frecuencias de actualización son compatibles con todas las resoluciones. Si se establece en 0, la frecuencia de actualización se detecta automáticamente. Los valores admitidos dependen del monitor. Si se establece una frecuencia de actualización que no es compatible con el monitor conectado, la pantalla se pondrá en negro. HP recomienda dejar este valor en 0.
root/Display/Profiles/<UUID>/width	Establece el ancho de resolución del monitor. Si se establece en 0, la resolución se detecta automáticamente.
root/Display/userLock	Si se establece en 1 y el usuario ha modificado los ajustes de la pantalla, éstos se conservan al importar un perfil de cliente.
root/Display/userLockEngaged	Esta clave de registro se establece automáticamente en 1 después de que el usuario ha modificado los ajustes de la pantalla. Normalmente no necesita modificar esta configuración.

Domain

Clave de registro	Descripción
root/domain/OU	Especifica la unidad organizacional asociada con la membresía de dominio del thin client.
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 <code>enableDomainAdmin</code> , 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 <code>enableDomainUsers</code> , 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 <code>domainAdminGroup</code> 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.

Clave de registro	Descripción
<code>root/domain/enableDomainUsers</code>	Si se establece en 1, los inicios de sesión del dominio se limitan a los miembros del grupo enumerados en <code>domainUserGroup</code> . Si se establece en 0, se permite cualquier credencial de dominio válida para iniciar sesión en el thin client.
<code>root/domain/enablePasswordChange</code>	Si se establece en 1, el usuario puede cambiar su contraseña de dominio directamente desde el thin client.
<code>root/domain/enableSSO</code>	Si se habilita, las credenciales actuales encriptadas se almacenan en caché en la memoria y se pueden volver a utilizar al iniciar conexiones remotas.
<code>root/domain/loginAtStart</code>	Si se establece en 1, y el thin client se ha agregado a un dominio, aparece una pantalla de inicio de sesión cuando se arranca el thin client. De lo contrario, aparece en el inicio el escritorio compartido de ThinPro heredado.
<code>root/domain/retainUserRegistry</code>	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.
<code>root/domain/workgroup</code>	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.

Network

Clave de registro	Descripción
<code>root/Network/ActiveDirectory/Domain</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/Network/ActiveDirectory/DynamicDNS</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/Network/ActiveDirectory/Enabled</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/Network/ActiveDirectory/Method</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/Network/ActiveDirectory/Password</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/Network/ActiveDirectory/Username</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/Network/DNSServers</code>	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.
<code>root/Network/DefaultHostnamePattern</code>	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 <code>Hostname</code> y <code>/etc/hostname</code> están vacías. El patrón del nombre de host usa <code>%</code> como un delimitador. En el ejemplo <code>HPTC%MAC:%1-6</code> , <code>HPTC</code> sería el prefijo y luego

Clave de registro	Descripción
	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.
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.

Clave de registro	Descripción
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.
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 redes 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 arranca automáticamente cuando se arranca el sistema.
root/Network/VPN/PPTP/Domain	Establece el dominio de PPTP.
root/Network/VPN/PPTP/Gateway	Establece la puerta de enlace 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: endian grande; 1: endian pequeño. 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.

Clave de registro	Descripción
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 puerta de enlace 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 (NATMode) es cisco-udp.
root/Network/VPN/VPNC/NATMode	Establece el modo transversal VPNC NAT.
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/Wired/DefaultGateway	Establece la puerta de enlace 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/Wired/EnableDefGatewayAsDNS	Si se establece en 1, la puerta de enlace 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.

Clave de registro	Descripción
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. <code>Automatic</code> 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 (<code>Full</code> o <code>Half</code>) 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 <code>Method</code> se establece en <code>Static</code> .
root/Network/Wired/Profiles/<UUID>/IPv4/DefaultGateway	Establece la puerta de enlace predeterminada que usa el dispositivo para comunicarse con Internet. Normalmente, esta es la dirección IP del enrutador. Esta configuración solo surte efecto si <code>Method</code> se establece en <code>Static</code> .
root/Network/Wired/Profiles/<UUID>/IPv4/Enabled	Si se establece en 1, IPv4 se habilita para este perfil.
root/Network/Wired/Profiles/<UUID>/IPv4/Method	Si se establece en <code>Automatic</code> , el cliente usa DHCP para intentar recuperar la configuración de red. Si se establece en <code>Static</code> , se utilizan los valores de las claves de registro de <code>Address</code> , <code>SubnetMask</code> y <code>DefaultGateway</code> . HP no recomienda el uso de <code>Static</code> 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 <code>Method</code> se establece en <code>Static</code> .
root/Network/Wired/Profiles/<UUID>/IPv6/Address	Establece la dirección IPv6 del cliente. Esta configuración solo surte efecto si <code>Method</code> se establece en <code>Static</code> .
root/Network/Wired/Profiles/<UUID>/IPv6/DefaultGateway	Establece la puerta de enlace predeterminada que usa el dispositivo para comunicarse con Internet. Normalmente, esta es la dirección IP del enrutador. Esta configuración solo surte efecto si <code>Method</code> se establece en <code>Static</code> .
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 <code>Automatic</code> , el cliente usa DHCP para intentar recuperar la configuración de red. Si se establece en <code>Static</code> , se utilizan los valores de las claves de registro de <code>Address</code> , <code>SubnetMask</code> y <code>DefaultGateway</code> . HP no recomienda el uso de <code>Static</code> 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 por lo general es la longitud del prefijo de IPv6. Esta configuración solo surte efecto si <code>Method</code> se establece en <code>Static</code> .
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.

Clave de registro	Descripción
root/Network/Wired/Profiles/<UUID>/EAPPEAP/CACert	Establece la ruta al archivo de certificado CA para la autenticación PEAP.
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.
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.

Clave de registro	Descripción
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 solo 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 solo 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 <code>Method</code> se establece en <code>Static</code> .
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/Wired/WirelessSwitch	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 enlace 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 <code>Method</code> se establece en <code>Static</code> .
root/Network/Wireless/EnableDefGatewayAsDNS	Si se establece en 1, la puerta de enlace 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 <code>Method</code> se establece en <code>Static</code> .
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 <code>Automatic</code> , el thin client usará DHCP para intentar recuperar la configuración de red. Si se establece en <code>Static</code> , se utilizan los valores de las claves de registro de <code>IPAddress</code> , <code>SubnetMask</code> y <code>DefaultGateway</code> . HP no recomienda el uso de <code>Static</code> 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.

Clave de registro	Descripción
root/Network/Wireless/Profiles/<UUID>/IPv4/Address	Establece la dirección IPv4 del cliente. Esta configuración solo surte efecto si <i>Method</i> se establece en <i>Static</i> .
root/Network/Wireless/Profiles/<UUID>/IPv4/DefaultGateway	Establece la puerta de enlace predeterminada que usa el dispositivo para comunicarse con Internet. Normalmente, esta es la dirección IP del enrutador. Esta configuración solo surte efecto si <i>Method</i> se establece en <i>Static</i> .
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 <i>Automatic</i> , el cliente usa DHCP para recuperar la configuración de red. Si se establece en <i>Static</i> , se utilizan los valores de las claves de registro de <i>Address</i> , <i>SubnetMask</i> y <i>DefaultGateway</i> . HP no recomienda el uso de <i>Static</i> 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 <i>Method</i> se establece en <i>Static</i> .
root/Network/Wireless/Profiles/<UUID>/IPv6/Address	Establece la dirección IPv6 del cliente. Esta configuración solo surte efecto si <i>Method</i> se establece en <i>Static</i> .
root/Network/Wireless/Profiles/<UUID>/IPv6/DefaultGateway	Establece la puerta de enlace predeterminada que usa el dispositivo para comunicarse con Internet. Normalmente, esta es la dirección IP del enrutador. Esta configuración solo surte efecto si <i>Method</i> se establece en <i>Static</i> .
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 <i>Automatic</i> , el cliente usa DHCP para intentar recuperar la configuración de red. Si se establece en <i>Static</i> , se utilizan los valores de las claves de registro de <i>Address</i> , <i>SubnetMask</i> y <i>DefaultGateway</i> . HP no recomienda el uso de <i>Static</i> 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 <i>Method</i> se establece en <i>Static</i> .
root/Network/Wireless/Profiles/<UUID>/PowerEnable	Si se establece en 1, se activa la administración de energía de la tarjeta de red inalámbrica.
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.

Clave de registro	Descripción
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.
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/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.

Clave de registro	Descripción
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 canales de 2,4 GHz; seleccione 5GHz para buscar solo 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/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, solo 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 solo 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 solo 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 WEP.

Clave de registro	Descripción
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 <code>Method</code> se establece en <code>Static</code> .
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. 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 <code>Auto</code> para buscar todos los canales inalámbricos; seleccione <code>2.4GHz</code> para buscar solo los canales de 2,4 GHz; seleccione <code>5GHz</code> para buscar solo los canales de 5 GHz.
root/Network/Wireless/WpaDriver	Especifica el controlador utilizado por <code>wpa_supplicant</code> (<code>wext</code> de forma predeterminada). <code>n180211</code> 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 <code>bcmwl</code> acepta la opción <code>wl_country</code> , 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/iPeak/ShowStatus	Si se establece en 1, se muestra el estado de HP Velocity como parte del icono de bandeja del sistema. HP Velocity no es compatible con HP t420.
root/Network/iPeak/SingleSidedAccelerate	Si se establece en 1, se habilita el recurso de aceleración en un solo lado de HP Velocity. Si se establece en 0, se desactiva este recurso. HP Velocity no es compatible con HP t420 o HP mt20.

Clave de registro	Descripción
root/Network/iPeak/Status	Si se establece en 1, se activa HP Velocity. Si se establece en 2, se activa HP Velocity en el modo de Monitor. Si se establece en 0, se activa HP Velocity. HP Velocity no es compatible con HP t420.
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.

Power

Clave de registro	Descripción
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/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, este valor se establece en la opción de 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 el modo de suspensión mientras el equipo está conectado a la alimentación de CA. De forma predeterminada, se establece en 30. Si se establece en 0, el equipo nunca entra en el modo 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 forma predeterminada, se establece en 15. Si se establece en 0, el equipo nunca entra en el modo de suspensión.
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 <code>criticalBatteryLevel</code> .

Clave de registro	Descripción
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.
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, este valor se establece en la opción de 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 el modo de suspensión mientras el equipo no está conectado a la alimentación de CA. De forma predeterminada, se establece en 30. Si se establece en 0, el equipo nunca entra en el modo 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 forma predeterminada, 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.

SCIM

Clave de registro	Descripción
root/SCIM/ScimEnabled	Si se establece en 1, se activa SCIM para la entrada en chino, japonés y coreano.

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.

Clave de registro	Descripción
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 FQDN de forma predeterminada.
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>/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.

Search

Clave de registro	Descripción
root/Search/Category/Applications/ConnectionManager/checked	
root/Search/Category/Applications/ConnectionManager/enabled	
root/Search/Category/Applications/Connections/checked	
root/Search/Category/Applications/Connections/enabled	
root/Search/Category/Applications/ControlPanel/checked	

Clave de registro	Descripción
root/Search/Category/Applications/ControlPanel/enabled	
root/Search/Category/Applications/Desktop/checked	
root/Search/Category/Applications/Desktop/enabled	
root/Search/Category/Applications/icon	
root/Search/Category/Applications/name	
root/Search/Category/FileSystem/caseSensitive	
root/Search/Category/FileSystem/enabled	
root/Search/Category/FileSystem/folderFilter	Especifica las carpetas en el sistema de archivos en las que se permitirá que el usuario haga búsquedas. Utilice un punto y coma para separar las carpetas. Por ejemplo: /home/user;/usr/bin
root/Search/Category/FileSystem/location	
root/Search/Category/FileSystem/subFolder	
root/Search/Category/Miscellaneous/CheckForUpdate	
root/Search/Category/Miscellaneous/Logout	
root/Search/Category/Miscellaneous/Reboot	
root/Search/Category/Miscellaneous/ShutDown	
root/Search/Category/Miscellaneous/Sleep	
root/Search/Category/Miscellaneous/SwitchToAdmin	
root/Search/Category/Regeditor/byDir	
root/Search/Category/Regeditor/byKey	
root/Search/Category/Regeditor/byValue	
root/Search/Category/Regeditor/byWhole	
root/Search/GUI/showCategory	

Serial

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 carácter.
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.

Clave de registro	Descripción
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 <code>none</code> , no hay detección de paridad.

SystemInfo

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/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	Descripción
root/TaskMgr/General/AlwaysOnTop	Si se establece en 1, la ventana del Administrador de tareas siempre está en la parte superior.

USB

Clave de registro	Descripción
root/USB/Classes/<class type>/ClassID	Establece el número de ID de clase USB.
root/USB/Classes/<class type>/DisplayName	Establece el nombre de clase USB.
root/USB/Classes/<class type>/State	Establece si la clase está asignada al host remoto.

Clave de registro	Descripción
<code>root/USB/Classes/<class type>/Visible</code>	Establece si la clase se muestra en la interfaz de usuario o no, o si está desactivada.
<code>root/USB/Devices/<UUID>/DisplayName</code>	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.
<code>root/USB/Devices/<UUID>/ProductID</code>	Establece la ID de producto del dispositivo.
<code>root/USB/Devices/<UUID>/State</code>	Establece si este dispositivo está asignado al host remoto de la siguiente forma: 0 = No redirigir; 1 = Usar valores predeterminados. 2 = Redirigir.
<code>root/USB/Devices/<UUID>/VendorID</code>	Establece el ID del proveedor del dispositivo.
<code>root/USB/root/autoSwitchProtocol</code>	Si se establece en 1, el protocolo USB remoto cambiará automáticamente según el protocolo elegido.
<code>root/USB/root/mass-storage/allowed</code>	Si se establece en 1, los dispositivos de almacenamiento masivo se montarán automáticamente cuando el protocolo sea <code>local</code> .
<code>root/USB/root/mass-storage/read-only</code>	Si se establece en 1, cuando los dispositivos de almacenamiento masivo se monten de forma automática, se montarán solo para lectura.
<code>root/USB/root/protocol</code>	Establece qué protocolo posee el USB remoto. Los valores válidos dependen de los protocolos que están instalados en el sistema, pero pueden incluir <code>local</code> , <code>xen</code> , <code>freerdp</code> y <code>view</code> .
<code>root/USB/root/showClasses</code>	Si se establece en 1, la sección Clases aparece en el Administrador de USB.

auto-update

Clave de registro	Descripción
<code>root/auto-update/DNSAliasDir</code>	Establece el directorio root (raíz) predeterminado para el modo de alias DNS en servidor que aloja HP Smart Client Services.
<code>root/auto-update/LockScreenTimeout</code>	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.
<code>root/auto-update/ManualUpdate</code>	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 <code>password</code> , <code>path</code> , <code>protocol</code> , <code>user</code> y <code>ServerURL</code> deben configurarse para asegurarse de que se conoce el servidor de actualización.
<code>root/auto-update/ScheduledScan/Enabled</code>	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 solo buscará actualizaciones al iniciar el sistema.
<code>root/auto-update/ScheduledScan/Interval</code>	Establece la cantidad de tiempo de espera entre las detecciones de actualizaciones programadas. Esto se debe especificar en el formato <code>HH:MM</code> . Se pueden especificar intervalos de más de 24 horas. Por ejemplo, para que ocurran las detecciones cada 48 horas, establezca esta opción en <code>48:00</code> .

Clave de registro	Descripción
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 período 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/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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , 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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , 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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , 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 <i>active</i> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <i>inactive</i> , el widget queda oculto. Si se establece como <i>read-only</i> , 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 <i>active</i> , el

Clave de registro	Descripción
	widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/auto-update/gui/auto-update/protocol</code>	Controla el estado del widget Protocolo en la herramienta Actualización automática. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/auto-update/gui/auto-update/tag</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/auto-update/gui/auto-update/user</code>	Controla el estado del widget Nombre de usuario en la herramienta Actualización automática. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/auto-update/password</code>	Establece la contraseña utilizada cuando está activada <code>ManualUpdate</code> . Esto solo se usa cuando se establece <code>protocol</code> en <code>ftp</code> . Este valor se encriptará.
<code>root/auto-update/path</code>	Establece la ruta relativa desde la URL del servidor predeterminado cuando se activa <code>ManualUpdate</code> . Normalmente, está vacía o configurada en <code>auto-update</code> .
<code>root/auto-update/preserveConfig</code>	Si se establece en 1, se conservará la configuración actual del thin client cuando ocurra una actualización de imagen a través de Actualización automática.
<code>root/auto-update/protocol</code>	Establece el protocolo que se utiliza cuando se activa <code>ManualUpdate</code>
<code>root/auto-update/tag</code>	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 <code>auto-update</code> .
<code>root/auto-update/user</code>	Establece el nombre de usuario utilizado cuando se activa <code>ManualUpdate</code> . Esto solo se usa cuando se establece el 'protocol' en 'ftp'.

background

Clave de registro	Descripción
<code>root/background/bginfo/alignment</code>	Establece la alineación del texto de Información del sistema en segundo plano.
<code>root/background/bginfo/enabled</code>	Si se establece en 1, la información del sistema aparece en el fondo del escritorio (Información del sistema en segundo plano).
<code>root/background/bginfo/horizontalLocation</code>	Establece la ubicación de Información del sistema en segundo plano en el eje X en un porcentaje.
<code>root/background/bginfo/interval</code>	Establece el intervalo de actualización del texto de Información del sistema en segundo plano en segundos.

Clave de registro	Descripción
root/background/bginfo/preset	Establece el archivo predefinido de Información del sistema en segundo plano en <code>use</code> . Si se establece en <code>none</code> , 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 « <i>Login Screen Customization</i> » (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	Si se establece <code>theme</code> en <code>none</code> , esta clave almacena el color utilizado por el tema definido por el usuario.
root/background/desktop/imagePath	Si se establece <code>theme</code> en <code>none</code> , 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 <code>theme</code> en <code>none</code> , esta clave almacena el último directorio utilizado.
root/background/desktop/style	Si se establece el <code>theme</code> en <code>none</code> , esta clave almacena la forma en que se coloca la imagen de fondo en el escritorio (por ejemplo <code>center</code> , <code>tile</code> , <code>stretch</code> , <code>fit</code> y <code>fill</code>).
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 en <code>none</code> para permitir que el usuario defina el tema, en <code>auto</code> para que el sistema establezca de forma automática el tema del protocolo adecuado para Smart Zero, o en <code>default</code> para usar el tema predeterminado para ThinPro.

config-wizard

Clave de registro	Descripción
root/config-wizard/FirmwareUpdate/ firmwareUpdateTimeout	Establece el período de tiempo de espera en segundos cuando se verifica si hay actualizaciones. Si se establece en 1, no hay tiempo de espera.
root/config-wizard/FirmwareUpdate/ firmwareUpdateURL	Establece la URL del FTP para actualizaciones de imágenes.
root/config-wizard/FirmwareUpdate/ preserveConfig	Si se establece en 1, se conservará la configuración actual del thin client cuando ocurra una actualización de imagen mediante el asistente de configuración inicial.

Clave de registro	Descripción
root/config-wizard/SelfUpdate/selfUpdateTimeout	Establece el periodo de espera en segundos para buscar actualizaciones automáticas. Si se establece en 1, no hay tiempo de espera.
root/config-wizard/SelfUpdate/selfUpdateURL	Establece la URL de FTP del asistente de configuración.
root/config-wizard/disableAllChecksAtStartup	Si se establece en 1, se desactivan todas verificaciones en el inicio. Si se establece en 0, puede activar/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.
root/config-wizard/enableNetworkCheck	Si se establece en 1, se activa la verificación de la red al iniciar el sistema.
root/config-wizard/enableUpdateCheck	Si se establece en 1, se activa la verificación de actualizaciones al iniciar el sistema.
root/config-wizard/enableUpdateCheckGui	Si se establece en 1, se activa la GUI de verificación de actualizaciones 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

Clave de registro	Descripción
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.

entries

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	

keyboard

Clave de registro	Descripción
<code>root/keyboard/DrawLocaleLetter</code>	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.
<code>root/keyboard/SystrayMenu/keyboardLayout</code>	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.
<code>root/keyboard/SystrayMenu/languages</code>	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.
<code>root/keyboard/SystrayMenu/virtualKeyboard</code>	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.
<code>root/keyboard/VisibleInSystray</code>	Si se establece en 1, se muestra el icono de la bandeja del sistema del teclado e indica la disposición actual del teclado.
<code>root/keyboard/XkbLayout</code>	Esta es una clave interna utilizada para asignarse a una disposición de teclado XKB. No debería ser necesario modificar esta clave.
<code>root/keyboard/XkbModel</code>	Esta es una clave interna utilizada para asignarse a un modelo de teclado XKB. No debería ser necesario modificar esta clave.
<code>root/keyboard/XkbOptions</code>	Esta es una clave interna utilizada para asignarse a opciones de teclado XKB. No debería ser necesario modificar esta clave.
<code>root/keyboard/XkbVariant</code>	Esta es una clave interna utilizada para asignarse a una variante de teclado XKB. No debería ser necesario modificar esta clave.
<code>root/keyboard/enable2</code>	Si se establece en 1, puede cambiarse la disposición del teclado secundario mediante el acceso directo del teclado, definido por <code>switch</code> .
<code>root/keyboard/layout</code>	Establece la disposición del teclado principal.
<code>root/keyboard/layout2</code>	Establece la disposición del teclado secundario.
<code>root/keyboard/model</code>	Establece el modelo de teclado principal.
<code>root/keyboard/model2</code>	Establece el modelo de teclado secundario.
<code>root/keyboard/numlock</code>	Si se establece en 1, se activa la función Bloq Num al iniciar el sistema. Esta clave de registro se ignora intencionalmente en los <code>thin clients</code> móviles.
<code>root/keyboard/rdp_kb</code>	Esta es una clave interna utilizada para asignarse a un mapa de teclado RDP. No debería ser necesario modificar esta clave.
<code>root/keyboard/switch</code>	Establece el acceso directo para alternar entre la disposición del teclado principal y secundario (<code>enable2</code> también se debe establecer en 1). Los valores válidos son los siguientes: <code>grp:ctrl_shift_toggle,grp:ctrl_alt_toggle,grp:alt_shift_toggle</code> .
<code>root/keyboard/variant</code>	Establece la variante de teclado principal.
<code>root/keyboard/variant2</code>	Establece la variante de teclado secundario.

logging

Clave de registro	Descripción
<code>root/logging/general/debug</code>	Si se establece en 1, se activa la depuración para todos los subsistemas compatibles con la depuración. Esto se suele utilizar en combinación con <code>generateDiagnostic.sh 0</code> la herramienta Diagnóstico de información del sistema para generar un paquete de diagnóstico que incluya registros de depuración del sistema.
<code>root/logging/general/debugLevel</code>	Establece el nivel de depuración. Este valor será aprovechado por otros módulos para generar los registros correspondientes.
<code>root/logging/general/showDebugLevelBox</code>	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 solo para administradores.

login

Clave de registro	Descripción
<code>root/login/buttons/configure/authorized</code>	Si se establece en 1, el botón Configuración está disponible en la pantalla de inicio de sesión.
<code>root/login/buttons/info/authorized</code>	Si se establece en 1, el botón Información del sistema está disponible en la pantalla de inicio de sesión.
<code>root/login/keyboard/authorized</code>	Si se establece en 1, los ajustes de disposición del teclado se pueden configurar en la pantalla de inicio de sesión.
<code>root/login/locale/authorized</code>	Si se establece en 1, los ajustes de idioma se pueden configurar en la pantalla de inicio de sesión.
<code>root/login/mouse/authorized</code>	Si se establece en 1, los ajustes del mouse se pueden configurar en la pantalla de inicio de sesión.
<code>root/login/onscreenKeyboard/authorized</code>	Si se establece en 1, el teclado en la pantalla está disponible en la pantalla de inicio de sesión.
<code>root/login/power/authorized</code>	Si se establece en 1, el botón de inicio/apagado está disponible en la pantalla de inicio de sesión.
<code>root/login/poweroff/authorized</code>	Si se establece en 1, la función de apagado está disponible en la pantalla de inicio de sesión.
<code>root/login/reboot/authorized</code>	Si se establece en 1, la función de reinicio está disponible en la pantalla de inicio de sesión.
<code>root/login/show/authorized</code>	Si se establece en 1, la lista con opciones adicionales del botón está disponible en la pantalla de inicio de sesión.
<code>root/login/sleep/authorized</code>	Si se establece en 1, la función de suspensión está disponible en la pantalla de inicio de sesión.
<code>root/login/touchscreen/authorized</code>	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 <code>root/touchscreen/enabled</code> también debe activarse.

mouse

Clave de registro	Descripción
<code>root/mouse/MouseHandedness</code>	Si se establece en 0, el mouse es para diestros. Si se establece en 1, el mouse es para zurdos.
<code>root/mouse/MouseSpeed</code>	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.
<code>root/mouse/MouseThreshold</code>	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.
<code>root/mouse/disableTrackpadWhileTyping</code>	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.
<code>root/mouse/enableTrackpad</code>	Si se establece en 1, se activa el trackpad. Si se establece en 0, se desactiva el trackpad.

restore-points

Clave de registro	Descripción
<code>root/restore-points/factory</code>	Especifica cuál instantánea se va a utilizar para un restablecimiento de fábrica.

screensaver

Clave de registro	Descripción
<code>root/screensaver/SlideShowAllMonitors</code>	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.
<code>root/screensaver/SlideShowInterval</code>	Establece el intervalo en segundos para el cambio de imágenes en la presentación del protector de pantalla.
<code>root/screensaver/SlideShowPath</code>	Especifica el directorio que contiene las imágenes para la presentación del protector de pantalla.
<code>root/screensaver/buttons/configure/authorized</code>	Si se establece en 1, el botón Configuración está disponible cuando la pantalla está bloqueada.
<code>root/screensaver/buttons/info/authorized</code>	Si se establece en 1, el botón Información del sistema está disponible cuando la pantalla está bloqueada.
<code>root/screensaver/buttons/keyboard/authorized</code>	Si se establece en 1, los ajustes de disposición del teclado se pueden configurar cuando la pantalla está bloqueada.
<code>root/screensaver/buttons/locale/authorized</code>	Si se establece en 1, los ajustes de idioma se pueden configurar cuando la pantalla está bloqueada.
<code>root/screensaver/buttons/mouse/authorized</code>	Si se establece en 1, los ajustes del mouse se pueden configurar cuando la pantalla está bloqueada.

Clave de registro	Descripción
<code>root/screensaver/buttons/onscreenKeyboard/authorized</code>	Si se establece en 1, el teclado de la pantalla está disponible cuando la pantalla está bloqueada.
<code>root/screensaver/buttons/power/authorized</code>	Si se establece en 1, el botón de inicio/apagado está disponible cuando la pantalla está bloqueada.
<code>root/screensaver/buttons/poweroff/authorized</code>	Si se establece en 1, la función de apagado está disponible cuando la pantalla está bloqueada.
<code>root/screensaver/buttons/reboot/authorized</code>	Si se establece en 1, la función de reinicio está disponible cuando la pantalla está bloqueada.
<code>root/screensaver/buttons/show/authorized</code>	Si se establece en 1, la lista con opciones adicionales del botón está disponible cuando la pantalla está bloqueada.
<code>root/screensaver/buttons/sleep/authorized</code>	Si se establece en 1, la función de suspensión está disponible cuando la pantalla está bloqueada.
<code>root/screensaver/buttons/touchscreen/authorized</code>	Si se establece en 1, los ajustes de la pantalla táctil se pueden configurar cuando la pantalla está bloqueada. La clave de registro <code>root/touchscreen/enabled</code> también debe activarse.
<code>root/screensaver/enableCustomLogo</code>	Si se establece en 1, se usa la imagen personalizada definida en <code>logoPath</code> para el protector de pantalla.
<code>root/screensaver/enableDPMS</code>	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.
<code>root/screensaver/enableScreensaver</code>	Si se establece en 1, se activa el protector de pantalla.
<code>root/screensaver/enableSleep</code>	Si se establece en 1, se activa la suspensión.
<code>root/screensaver/lockScreen</code>	Si se establece en 1, se requiere una contraseña para volver al escritorio desde el protector de pantalla.
<code>root/screensaver/logoPath</code>	Establece la ruta a una imagen personalizada que se utiliza para el protector de pantalla.
<code>root/screensaver/mode</code>	Establece el modo de renderización para la imagen del protector de pantalla (como <code>Center</code> , <code>Tile</code> y <code>Stretch</code>). Si se establece en <code>Default</code> , la imagen se muestra sin ningún procesamiento. Si se establece en <code>SlideShow</code> , el protector de pantalla circulará imágenes del directorio especificado por <code>SlideShowPath</code> .
<code>root/screensaver/off</code>	Establece el intervalo de espera en minutos antes de que se apague el monitor.
<code>root/screensaver/origImageCopyPath</code>	Esta es la ruta donde se guarda la imagen personalizada cuando el <code>mode</code> se establece en <code>Default</code> .
<code>root/screensaver/standby</code>	Establece el intervalo de espera en minutos antes de que el monitor entre en modo de espera.
<code>root/screensaver/suspend</code>	Establece el intervalo de espera en minutos antes de que el monitor entre en modo de suspensión.
<code>root/screensaver/timeoutScreensaver</code>	Establece el intervalo de espera en minutos antes de que se inicie el protector de pantalla.
<code>root/screensaver/timeoutSleep</code>	Establece el intervalo de espera en minutos antes de que el <code>thin client</code> entre en modo de suspensión.

security

Clave de registro	Descripción
<code>root/security/authenticationFailDelay</code>	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.
<code>root/security/domainEntryMode</code>	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 .
<code>root/security/enableLockOverride</code>	Si se establece en 1, los administradores pueden anular el bloqueo de la pantalla de un escritorio local.
<code>root/security/enableSecretPeek</code>	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.
<code>root/security/encryption/identity/encryptedSecretCipher</code>	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.
<code>root/security/encryption/identity/encryptedSecretTTL</code>	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.
<code>root/security/encryption/identity/secretHashAlgorithm</code>	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 computar 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).
<code>root/security/encryption/identity/secretHashTTL</code>	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.
<code>root/security/mustLogin</code>	Si se establece en 1, se obliga a todos los usuarios a iniciar sesión antes de acceder al escritorio.

shutdown

Clave de registro	Descripción
<code>root/shutdown/enableAutomaticShutdownTimeout</code>	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.
<code>root/shutdown/timeOfAutomaticShutdownTimeout</code>	Establece el tiempo de espera del apagado automático.

sshd

Clave de registro	Descripción
<code>root/sshd/disableWeakCipher</code>	Si se establece en 1, se desactiva el cifrado del modo CBC, así como otros cifrados débiles conocidos, como 3DES, arcfour, etc.
<code>root/sshd/disableWeakHmac</code>	Si se establece en 1, se desactiva hmac de 96 bits, así como cualquier hmac basado en sha1 y en md5.
<code>root/sshd/disableWeakKex</code>	Si se establece en 1, se desactivan los algoritmos de intercambio de clave que tienen DH con SHA1.
<code>root/sshd/enabled</code>	Si se establece en 1, se activa el daemon SSH y se puede acceder al thin client a través de SSH.
<code>root/sshd/userAccess</code>	Si se establece en 1, los usuarios finales pueden conectarse al thin client a través de SSH.

time

Clave de registro	Descripción
<code>root/time/NTPServers</code>	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 <code>pool.ntp.org</code> 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.
<code>root/time/dateFormatLong</code>	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 <code>QDate::toString</code> . Si se deja en blanco, por lo general se usa una cadena específica del lugar.
<code>root/time/dateFormatShort</code>	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 <code>QDate::toString</code> . Si se deja en blanco, por lo general se usa una cadena específica del lugar.
<code>root/time/dateTimeFormatLong</code>	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 <code>QDate::toString</code> . Si se deja en blanco, por lo general se usa una cadena específica del lugar.
<code>root/time/dateTimeFormatShort</code>	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 <code>QDate::toString</code> . Si se deja en blanco, por lo general se usa una cadena específica del lugar.
<code>root/time/hideCountries</code>	Es una lista separada por puntos y comas de los países que quiere ocultar en la GUI de selección de zona horaria.
<code>root/time/hideWinZones</code>	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.

Clave de registro	Descripción
<code>root/time/hideZones</code>	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.
<code>root/time/timeFormatLong</code>	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 <code>QDate::toString</code> . Si se deja en blanco, por lo general se usa una cadena específica del lugar.
<code>root/time/timeFormatShort</code>	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 <code>QDate::toString</code> . Si se deja en blanco, por lo general se usa una cadena específica del lugar.
<code>root/time/timezone</code>	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: <code><región>/<subregión></code> .
<code>root/time/use24HourFormat</code>	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.
<code>root/time/useADNSTimeServers</code>	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: <code>_ldap._tcp.dc._msdcs.domain.</code>
<code>root/time/useDHCPTimezone</code>	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 <code>tc_code</code> (que suele ser la etiqueta 101, aunque la 100 y la 2 también pueden funcionar).
<code>root/time/useNTPServers</code>	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 <code>NTPServers</code> .

touchscreen

Clave de registro	Descripción
<code>root/touchscreen/beep</code>	Define si el thin client produce un bip cuando se usa la pantalla táctil.
<code>root/touchscreen/calibrated</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
<code>root/touchscreen/enabled</code>	Si se establece en 1, se activa la entrada táctil.
<code>root/touchscreen/maxx</code>	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.

Clave de registro	Descripción
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.
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

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 <code>en_US</code> (inglés), <code>de_DE</code> (alemán), <code>es_ES</code> (español), <code>fr_FR</code> (francés), <code>ru_RU</code> (ruso), <code>ja_JP</code> (japonés), <code>ko_KR</code> (coreano), <code>zh_CN</code> (chino simplificado) y <code>zh_TW</code> (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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.

usb-update

Clave de registro	Descripción
root/usb-update/authentication	Si se establece en 1, se requiere una contraseña de administrador para las actualizaciones USB.

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 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

Clave de registro	Descripción
root/users/gui/hptc-user-rights/name	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/users/gui/hptc-user-rights/status	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
root/users/gui/hptc-user-rights/title	Esta clave de registro se utiliza internamente o se reserva para el uso futuro. El valor no debe modificarse.
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, solo se permite el control remoto del thin client a los sistemas enumerados en <code>root/users/usuario/xhosts</code> .
root/users/user/apps/hptc-ad-dns-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento Administrador de AD/DDNS 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.
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.

Clave de registro	Descripción
root/users/user/apps/hptc-clientaggregation-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento Agrupamiento de cliente en el 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 Administrador de opción 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 Preferencias de video 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-energy-star/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento Energy Star en el Panel de control.
root/users/user/apps/hptc-il8n-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-keyboard-layout/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento Formato de teclado en el Panel de control.
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.
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-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-screenlock/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-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-shortcut-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento Administrador de método abreviado del teclado 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-task-mgr/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento Administrador de tareas en el Panel de control.
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 Panel de control.
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.

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 Duplicación VNC en el Panel de control.
root/users/user/apps/hptc-xterm/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento Terminal X en el Panel de control. PRECAUCIÓN: La activación 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 activarse si se utiliza en la depuración de un entorno protegido y no de producción.
root/users/user/apps/scim-setup/authorized	Si se establece en 1, los usuarios finales pueden acceder al elemento Configuración de método de entrada SCIM en el Panel de control.
root/users/user/enablePassword	Si está activado, 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/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 activado XHostCheck .

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.

Clave de registro	Descripción
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 <code>vncUsePassword</code> .
root/vncserver/coreSettings/vncReadOnly	Si se establece en 1, la duplicación de VNC funcionará en modo de solo 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/vncUsePassword	Si se establece en 1, la contraseña especificada en <code>vncPassword</code> es necesario para la duplicación de 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 Duplicación VNC en la herramienta Duplicación VNC. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 Duplicación VNC. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , 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 <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.

Clave de registro	Descripción
<code>root/vncserver/gui/VNCShadowManager/widgets/vncNotifyShowTimeout</code>	Controla el estado del widget VNC Mostrar tiempo de espera para notificación en la herramienta Duplicación VNC. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncNotifyTimeout</code>	Controla el estado del widget numérico en la herramienta Duplicación VNC. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncNotifyUser</code>	Controla el estado del widget VNC Notifique Usuario para Negar en la herramienta Duplicación VNC. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncPassword</code>	Controla el estado del widget Defina Contraseña en la herramienta Duplicación VNC. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncReadOnly</code>	Controla el estado del widget VNC solo de lectura en la herramienta Duplicación VNC. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncRefuseInDefault</code>	Controla el estado del widget Rechazar conexiones predeterminadas en la herramienta Duplicación VNC. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/vncserver/gui/vncStopButton</code>	Controla el estado del botón Detener duplicación de VNC en la utilidad Duplicación VNC. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncTakeEffectRightNow</code>	Controla el estado del widget Restablecer el servidor VNC inmediatamente en la herramienta Duplicación VNC. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncUsePassword</code>	Controla el estado del widget Contraseña de Uso VNC en la herramienta Duplicación VNC. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget

Clave de registro	Descripción
	queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncUseSSL</code>	Controla el estado del widget SSL de uso VNC en la herramienta Duplicación VNC. Si se establece como <code>active</code> , el widget puede verse en la interfaz de usuario y el usuario puede interactuar con él. Si se establece como <code>inactive</code> , el widget queda oculto. Si se establece como <code>read-only</code> , el widget puede verse en el modo de solo lectura.

Índice

A

Active Directory 56
actualizaciones de imágenes 1
actualizar thin clients
 actualización manual 69
 Actualización mediante alias de DNS 69
 Actualización mediante etiquetado de DHCP 68
 actualización por transmisión 68
Administrador de certificados 63
Administrador de componentes 56
Administrador de energía 49
Administrador de imagen de fondo 49
Administrador de SCEP 63, 64
Administrador de serie 63
Administrador de tareas 63
Administrador SSHD 56
Agente HPDM 56
agrupamiento de client 45
agrupamiento de cliente
 configuración de cliente 46
 configuración del servidor 47
ajustes de fecha y hora 49
ajustes de idioma 49
ajustes de la pantalla táctil 44
ajustes de la red
 acceso 49
 cableada 50
 conexiones inalámbricas 50
 DNS 52
 HP Velocity 53
 IPSec 53
 VPN 53
ajustes del mouse 44
ajustes de protector de pantalla 49
ajustes de seguridad 49
ajustes de sonido 44
atajos del teclado 63

C

certificados
 instalación 63
 VMware Horizon View 32
Citrix
 ajustes, generales 10
 ajustes, por conexión 14
 HP True Graphics 39
claves de registro 82
complementos 1
conexiones
 configuración 8
 configuración avanzada 8
 ocultar 49
conexiones custom 37
configuración de administración de energía 49
configuración de impresora 74
configuración de impresora en serie 74
configuración de impresora paralela 74
Configuración de SO, elección 1
contraseñas, cambio 49
D
diagnóstico del sistema 77
Duplicación VNC 62
E
estadísticas de conexión inalámbrica 56
G
GUI
 Administrador de conexión (solo en ThinPro) 7
 barra de tareas 5
 descripción general 4
 escritorio 4
H
Herramienta de recorte 63
HP Device Manager. *Consulte* Agente HPDM

Consulte también servicio de administración remota

HP Smart Client Services
 descripción general 66
 instalación 66
Profile Editor. *Consulte* Profile Editor
sistemas operativos compatibles 66
Consulte también servicio de administración remota
HP TeemTalk. *Consulte* TeemTalk
HP True Graphics 39
HP Velocity 53

I

imágenes. *Consulte* HP ThinState
impresoras 48
instantáneas 56

M

MMR. *Consulte* redirección de multimedia
modo de administrador 3
modo de suspensión 49
modo de usuario 3
modo quiosco 9

O

obtener más información 1
Opciones DHCP 64

P

Panel de control
 Active Directory 56
 Administrador de componentes 56
 Administrador de energía 49
 Administrador de imagen de fondo 49
 Administrador de opción DHCP 64
 Administrador de SCEP 63
 Administrador de serie 63
 Administrador de tareas 63

- Administrador SSHD 56
 - Agrupamiento de cliente 45
 - Atajos del teclado 63
 - Centro de personalización 49
 - Configuración de método de entrada SCIM 44
 - descripción general 44
 - Duplicación VNC 62
 - Editor de texto 63
 - Estadísticas de conexión
 - inalámbrica 56
 - Fecha y hora 49
 - Herramienta de recorte 63
 - Idioma 49
 - Instantáneas 56
 - Mouse 44
 - Pantalla táctil 44
 - Preferencias de pantalla 47
 - Red 49
 - Restablecimiento de los valores de fábrica 56
 - Seguridad 49
 - Sonido 44
 - Terminal X 63
 - ThinState. *Consulte* HP ThinState utilidades, ocultar 49
 - pasos iniciales 1
 - perfil de cliente
 - agregar archivos 72
 - agregar enlace simbólico 73
 - carga 71
 - certificados 72
 - configuraciones de registro 72
 - guardar 74
 - personalización 71
 - perfiles de pantalla 47
 - preferencias de pantalla 47
 - Profile Editor 71
- R**
- RDP
 - ajustes, generales 15
 - ajustes, por conexión 16
 - redirección de almacenamiento masivo 22
 - redirección de audio 23
 - redirección de dispositivo 22
 - redirección de impresora 23
 - redirección de multimedia 21
 - redirección de smart card 25
 - redirección de USB 22
 - RemoteFX 20
 - sesiones con varios monitores 21
 - redirección de almacenamiento masivo
 - RDP 22
 - VMware Horizon View 30
 - redirección de audio
 - RDP 23
 - VMware Horizon View 30
 - redirección de cámara web
 - VMware Horizon View 31
 - redirección de dispositivo
 - RDP 22
 - VMware Horizon View 29
 - redirección de impresora
 - RDP 23
 - VMware Horizon View 30
 - redirección de multimedia
 - RDP 21
 - VMware Horizon View 29
 - redirección de smart card
 - RDP 25
 - VMware Horizon View 31
 - redirección de USB
 - RDP 22
 - VMware Horizon View 29
 - Redirección de USB
 - Administrador de USB 48
 - RemoteFX 20
 - restablecimiento de los valores de fábrica 56
- S**
- SCIM 44
 - servicio de administración remota, elección 3
 - sitios web
 - Soporte de Citrix 1
 - Soporte de HP 1
 - Soporte de Microsoft 1
 - Soporte de VMware 1
 - Smart Zero. *Consulte* Configuración de SO
 - solución de problemas 76
 - conectividad de red 76
 - uso de diagnóstico del sistema 77
 - SSH 36
- T**
- TeemTalk 34
 - Telnet 37
 - Terminal X 63
 - text editor 63
 - thin clients
 - actualización. *Consulte* actualizar thin clients
 - ThinPro. *Consulte* Configuración de SO
 - ThinState. *Consulte* HP ThinState
- V**
- VMware Horizon View
 - accesos directos del teclado 29
 - ajustes, por conexión 25
 - cambio de protocolos 31
 - certificados 32
 - redirección de almacenamiento masivo 30
 - redirección de audio 30
 - redirección de cámara web 31
 - redirección de dispositivo 29
 - redirección de impresora 30
 - redirección de multimedia 29
 - redirección de smart card 31
 - redirección de USB 29
 - sesiones con varios monitores 29
- W**
- Web Browser
 - ajustes, generales 33
 - ajustes, por conexión 33
- X**
- XDMCP 36