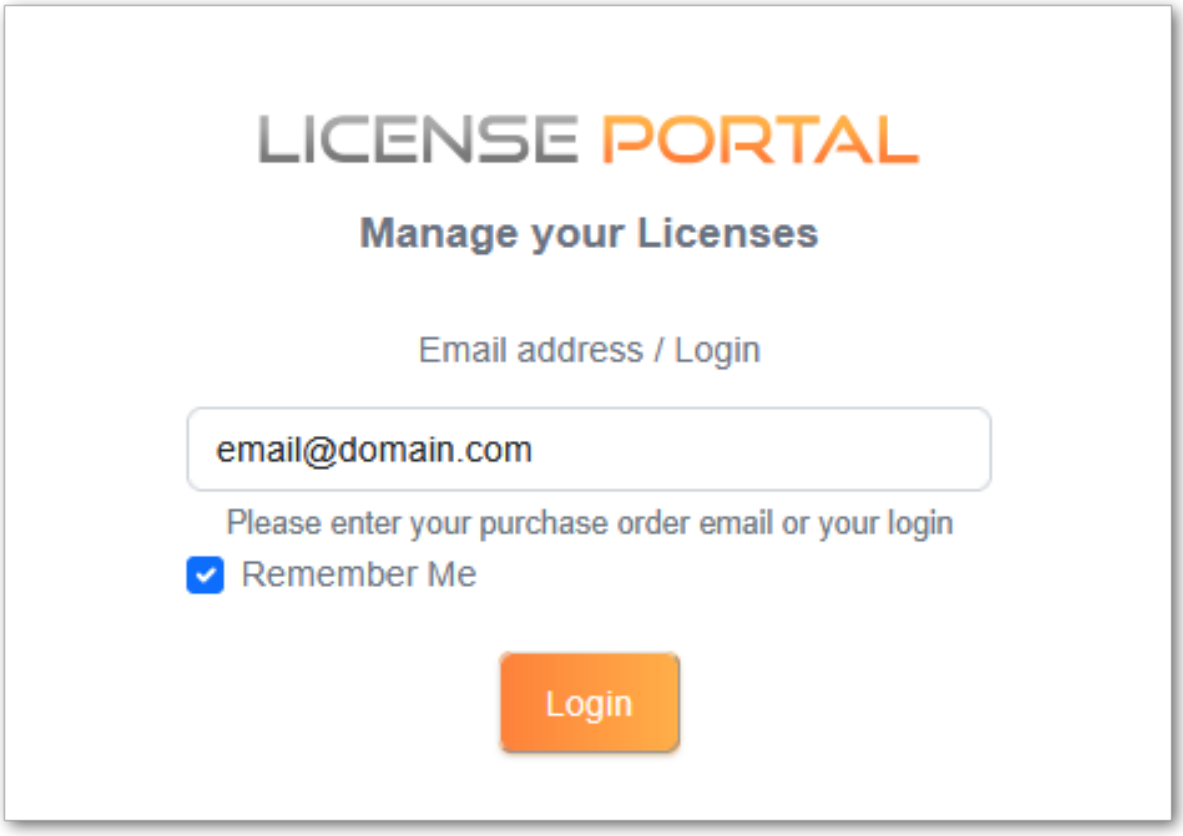
Activando su licencia permanente de TSplus (sin conexión)

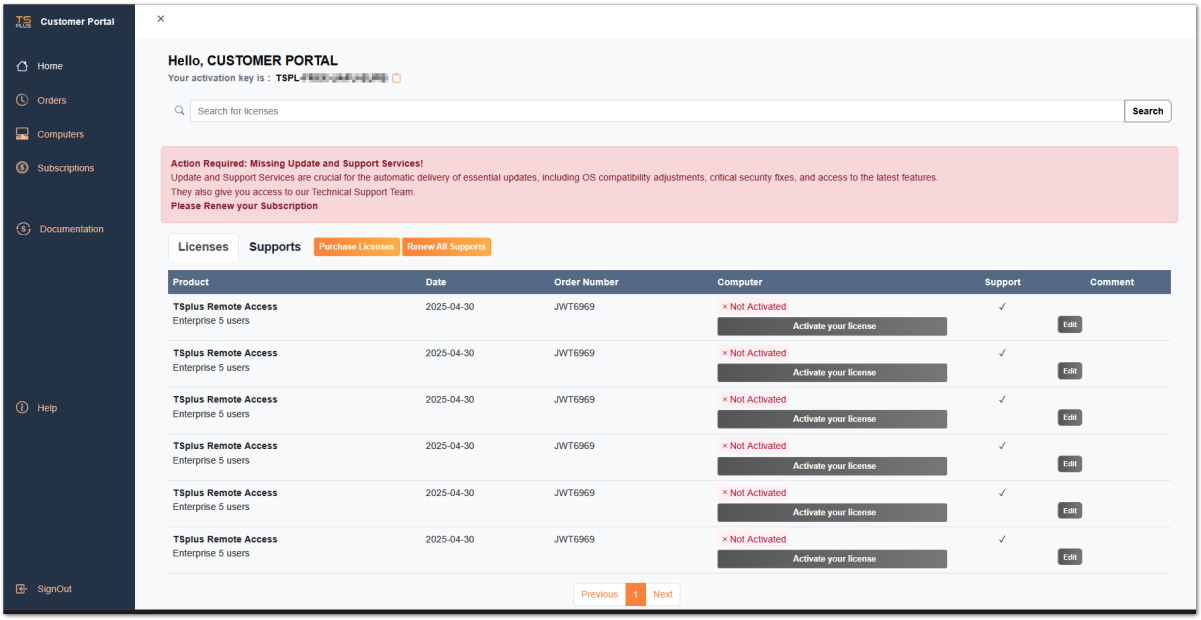
Recupera tu clave de activación

Cuando pida una licencia, conéctese a nuestro Portal de Licencias y ingrese su dirección de correo electrónico y su número de pedido.

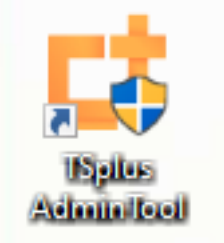


Descargar la Guía del Usuario del Portal del Cliente para más información sobre cómo usarlo.

Su clave de activación se mostrará en la parte superior del panel de control:



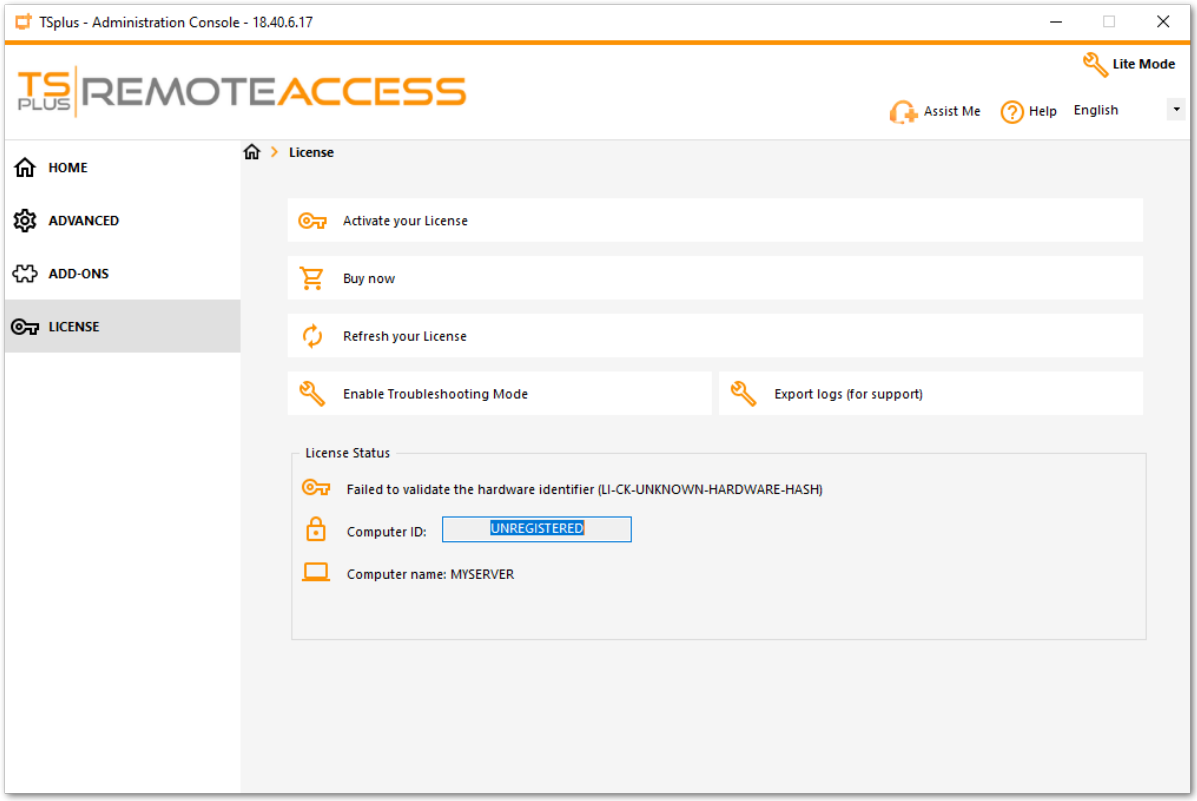
Localiza la herramienta de administrador en tu escritorio



Si no puedes encontrar el acceso directo de la herramienta de administración, debería estar ubicado en la carpeta de escritorio de la cuenta de administrador utilizada para descargar TSplus. También puedes encontrar la carpeta de TSplus en esta ruta: ‘C:\Program Files (x86)\TSplus\UserDesktop\files’.

Haga doble clic en él, luego haga clic en la pestaña de licencia.

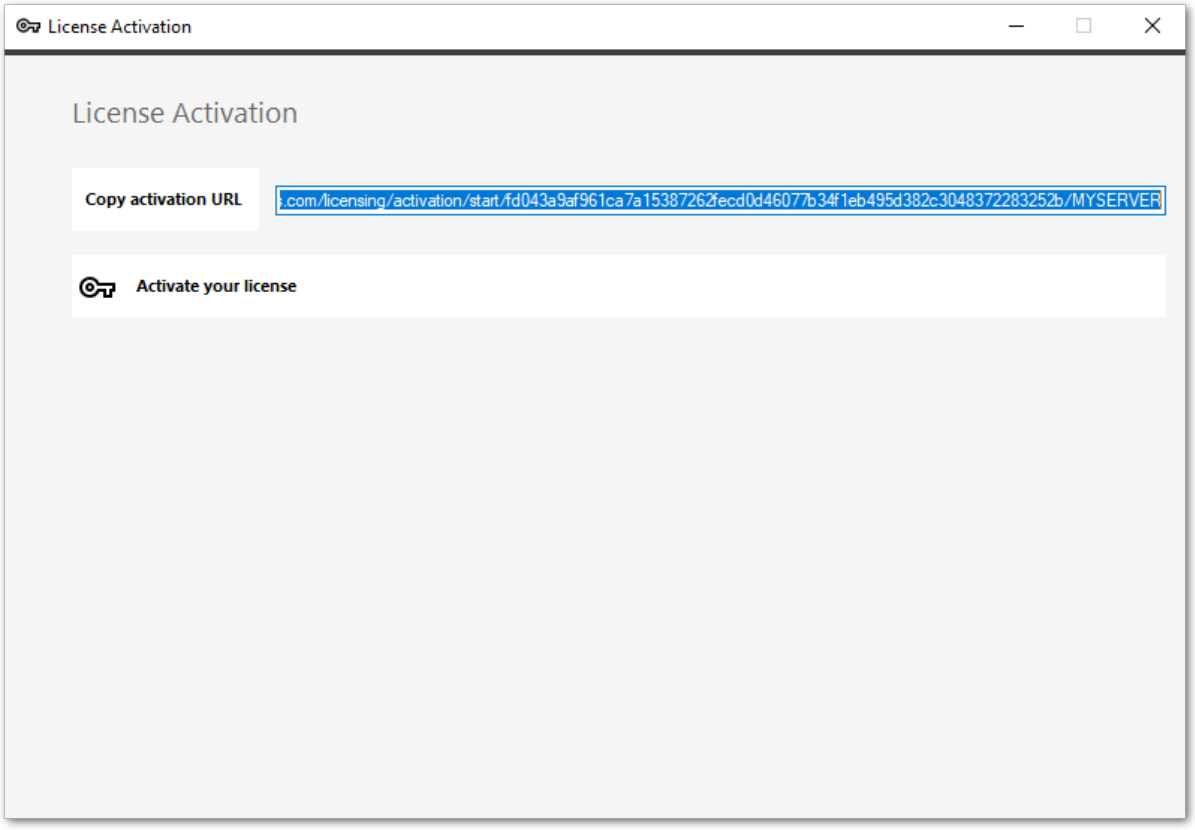
Aquí puedes ver el estado de tu licencia de TSplus, así como tu ID de computadora y el nombre de la computadora "NO REGISTRADO".



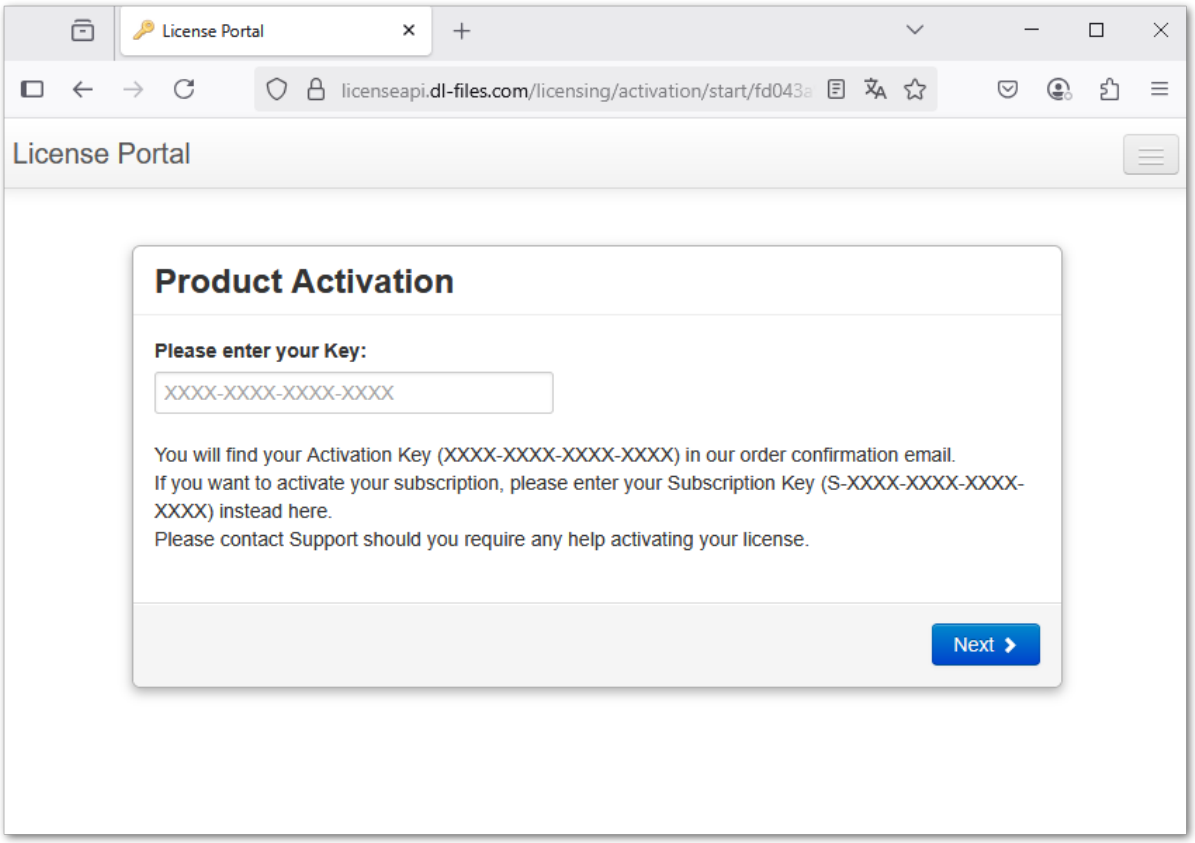
Activa tus licencias en un servidor TSplus sin conexión

Haga clic en el botón "Activar su licencia". Aparece una ventana emergente que muestra una dirección URL bastante larga.

Copia esta URL en el navegador de un ordenador conectado a Internet y accede a ella para recuperar un archivo de licencia:

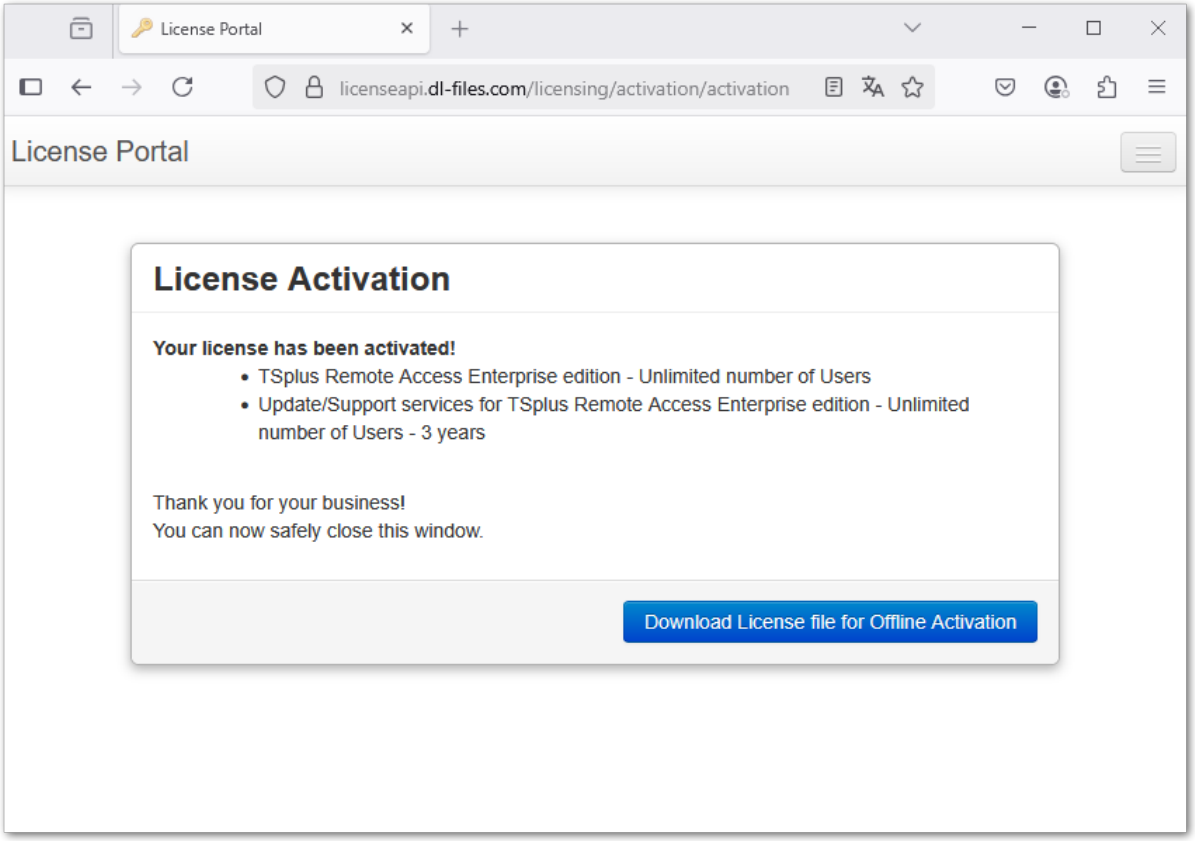


Ingrese su clave de activación:

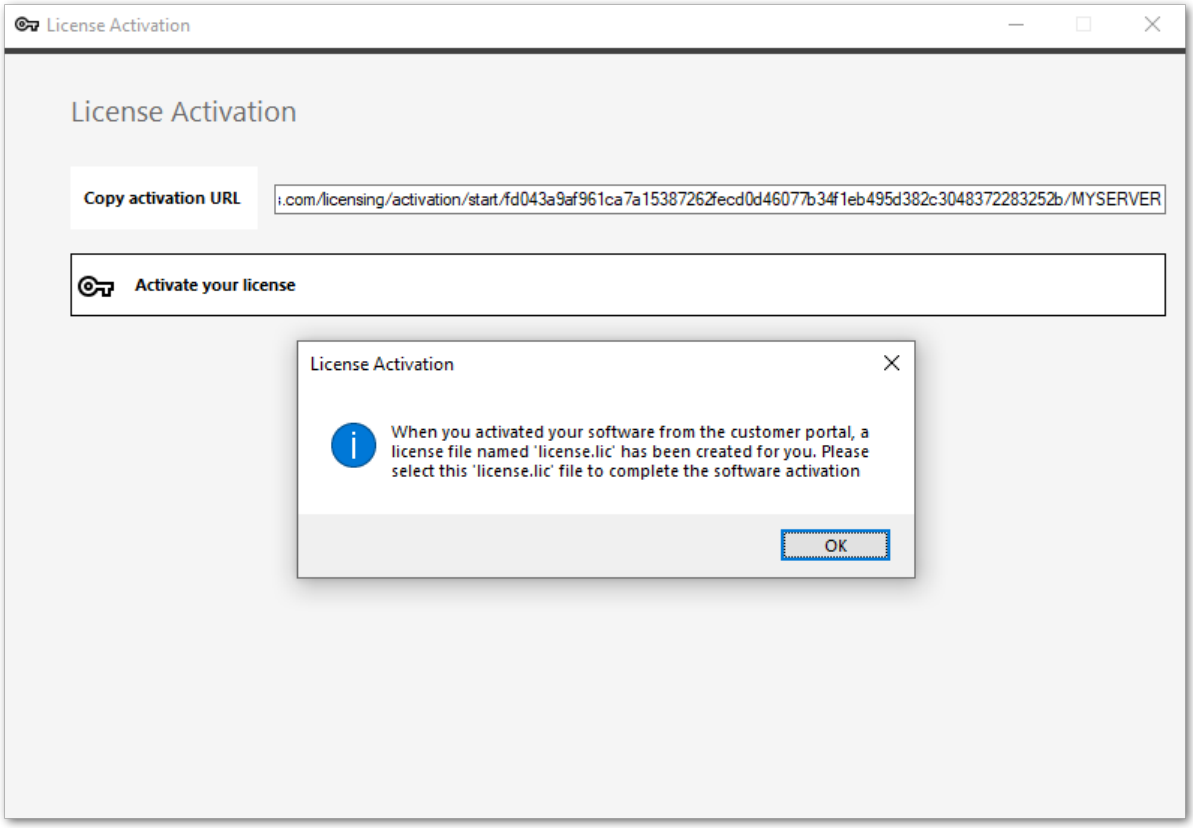


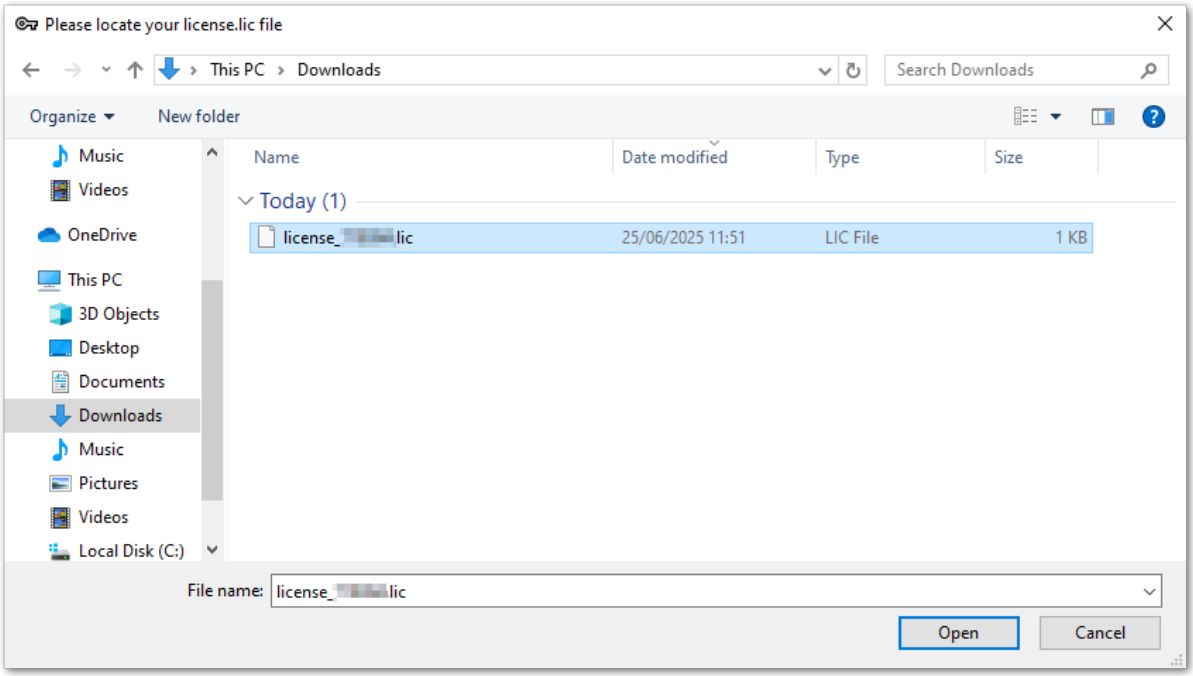
Su licencia se valida entonces. Descargue el archivo de licencia haciendo clic en el botón

correspondiente:

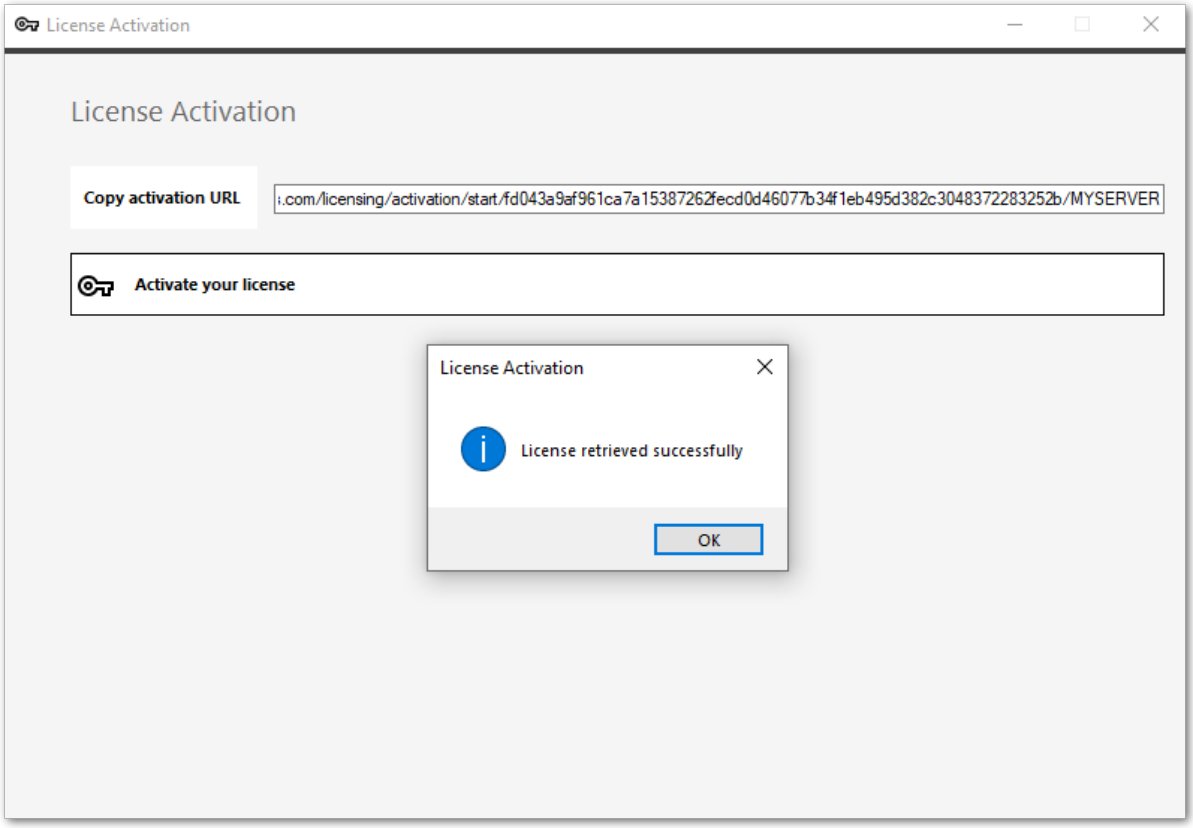


Este archivo de licencia debe ser copiado de nuevo al servidor para completar el proceso de activación sin conexión:





Un mensaje confirmará que su licencia fue recuperada con éxito:

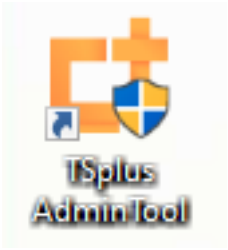


Luego tendrás que seleccionar las licencias / soporte correspondientes para activar y un mensaje confirmando que todos tus productos / soporte están ahora activados.

N.B Aún puedes descargar archivos license.lic en el Portal de Licencias para las Versiones Legadas de TSplus. Descargar la Guía del Usuario del Portal del Cliente .

Activando su licencia de TSplus (en línea) permanente o de suscripción.

Localiza la herramienta de administrador en tu escritorio:

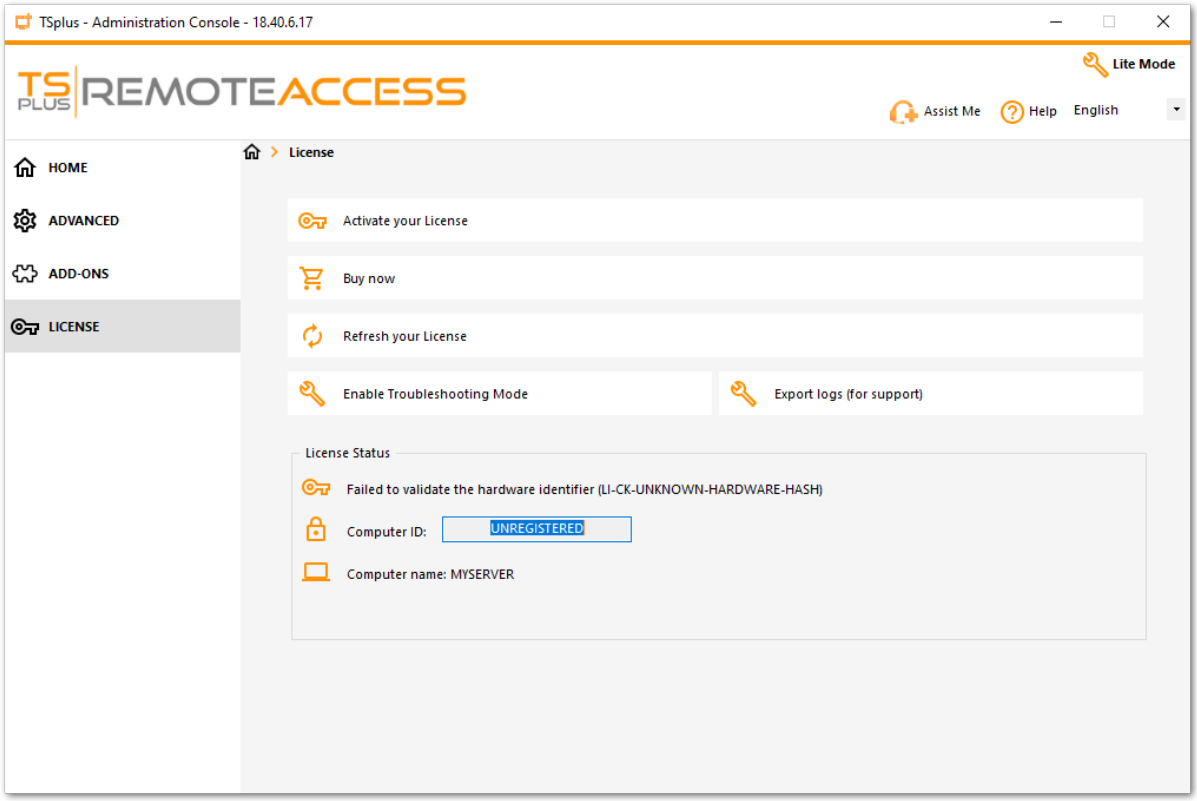


- Si no puedes encontrar el acceso directo de la herramienta de administración, debería estar ubicado en la carpeta de escritorio de la cuenta de administrador utilizada para descargar TSplus. También puedes encontrar la carpeta de TSplus en esta ruta: ‘C:\Program Files (x86)\TSplus\UserDesktop\files’.

Haga doble clic en él, luego haga clic en la pestaña de licencia.

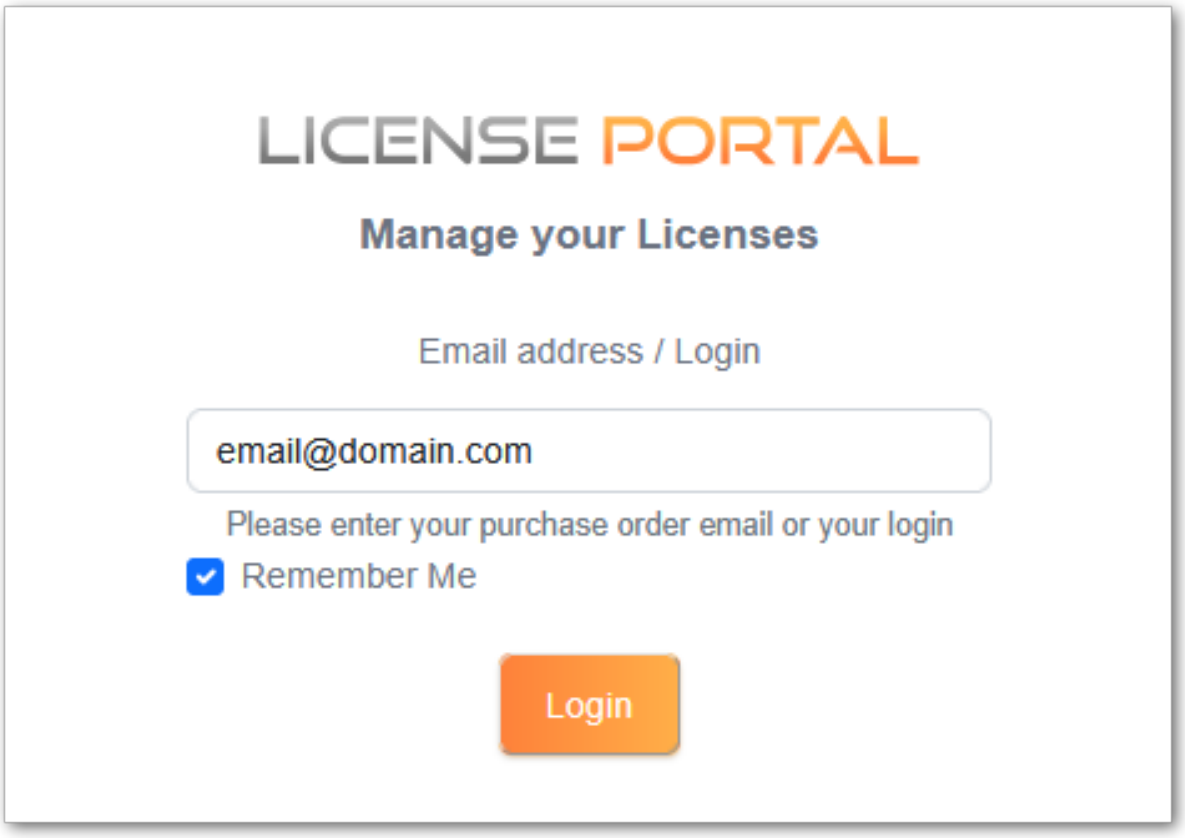
Aquí puedes ver el estado de tu licencia de TSplus, así como tu ID de computadora y nombre de computadora:

si se muestra "NO REGISTRADO" significa que su servidor no está conectado a Internet y necesita verificar el acceso web de su servidor antes de continuar.



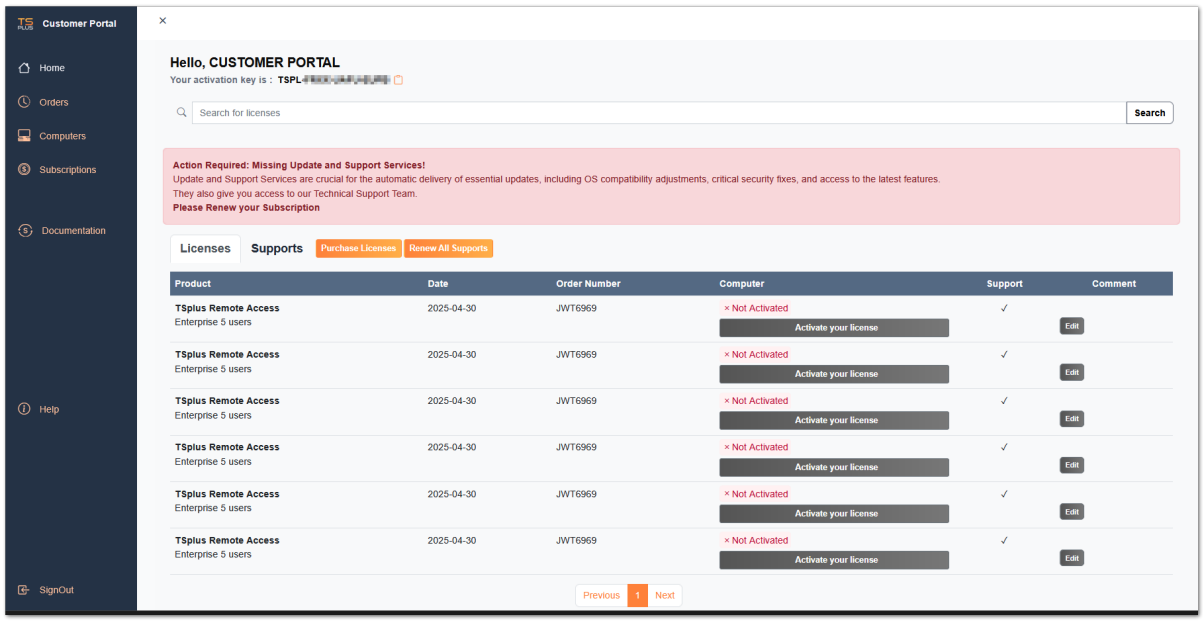
Activa tus licencias en un servidor TSplus en línea

Cuando pida una licencia, conéctese a nuestro Portal de Licencias y ingrese su dirección de correo electrónico y su número de pedido:



Descargar la Guía del Usuario del Portal del Cliente para más información sobre cómo usarlo.

Su clave de activación se mostrará en la parte superior del panel de control:

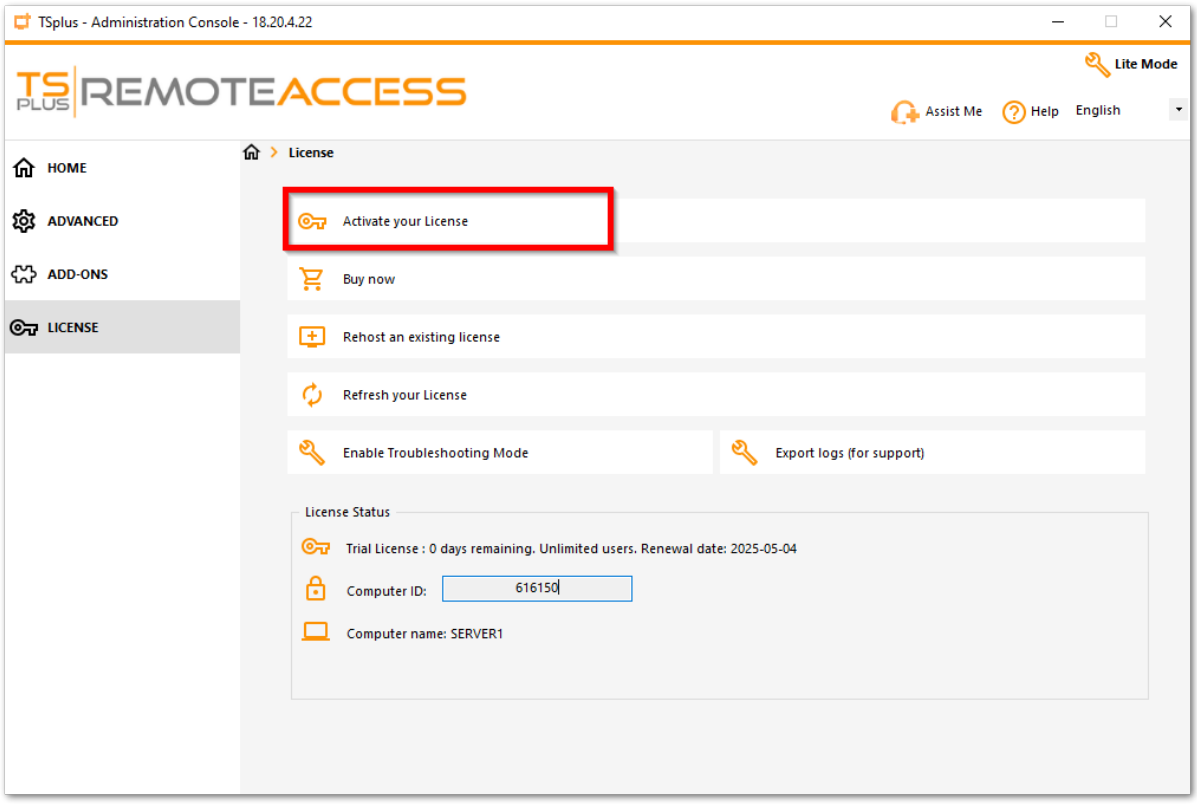


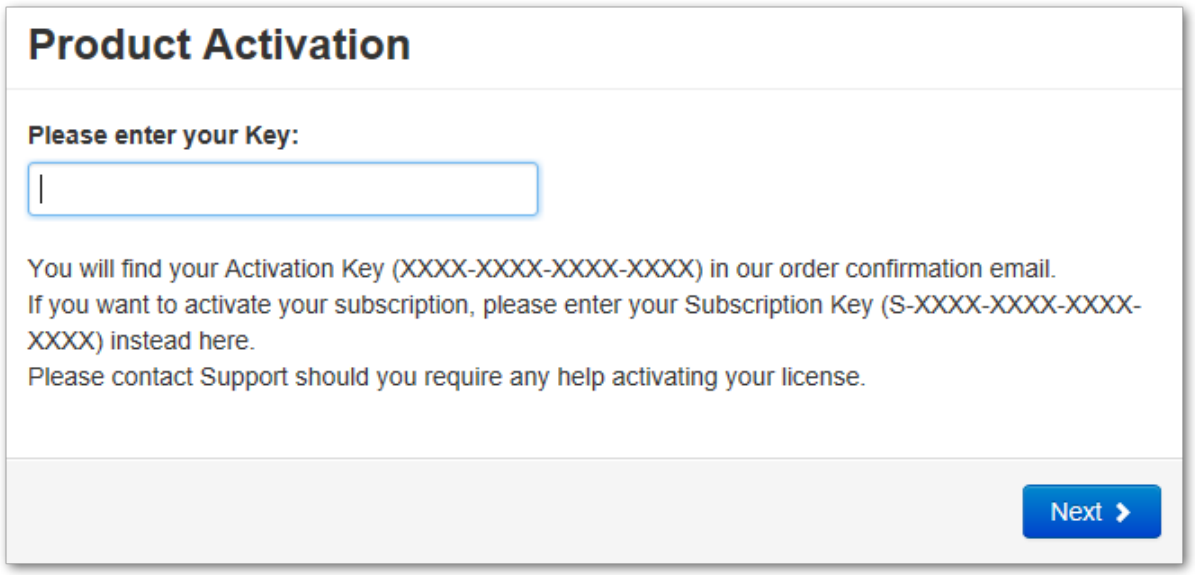
Puedes ir a la pestaña de Licencia del AdminTool, hacer clic en el botón "Activar tu Licencia", ingresar esta clave de activación y hacer clic en "Siguiente".

Encontrará su clave de activación permanente. **(XXXX-XXXX-XXXX-XXXX)** en nuestro correo

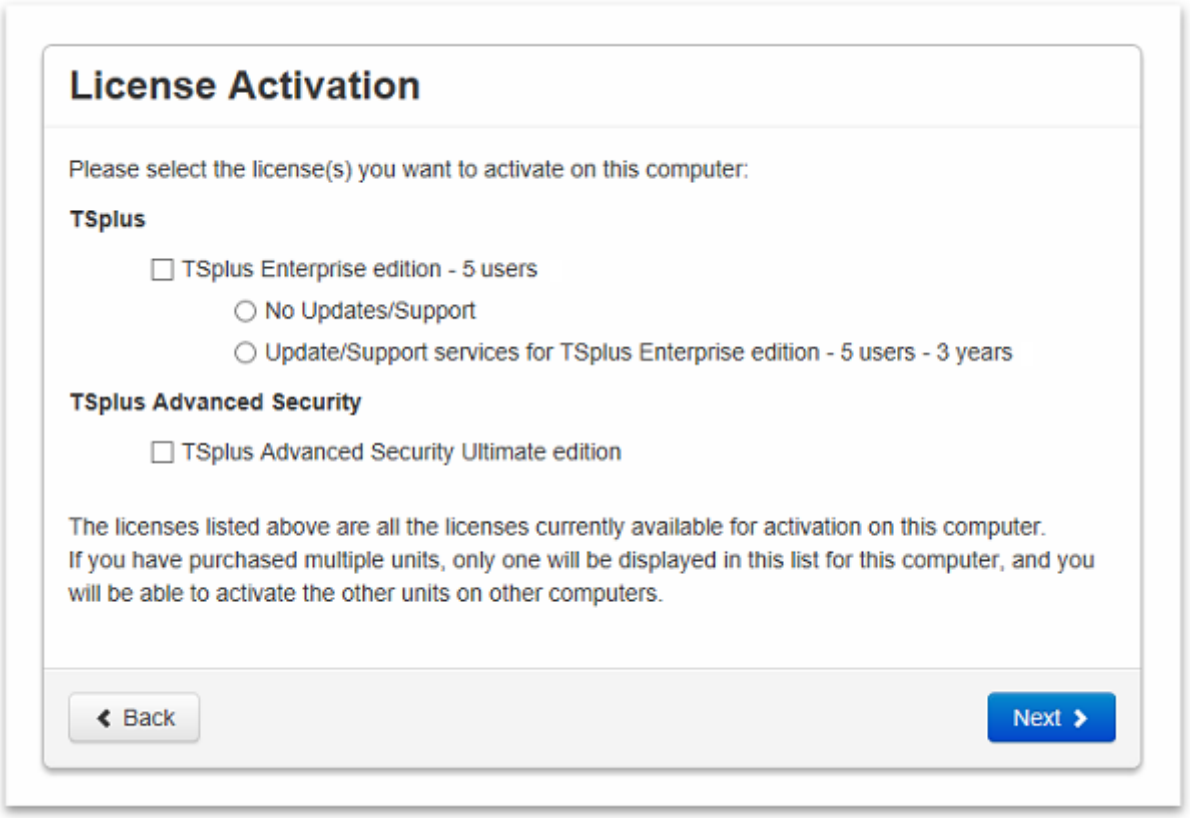
electrónico de confirmación de pedido.

Si desea activar su suscripción, ingrese su clave de suscripción. **S-XXXX-XXXX-XXXX-XXXX** .

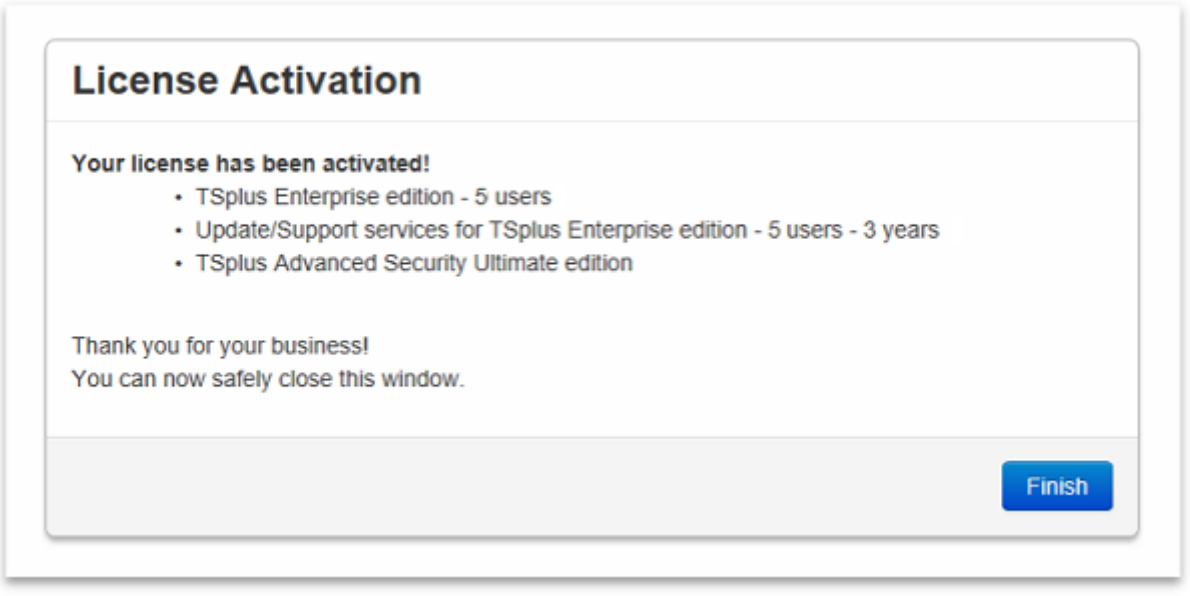




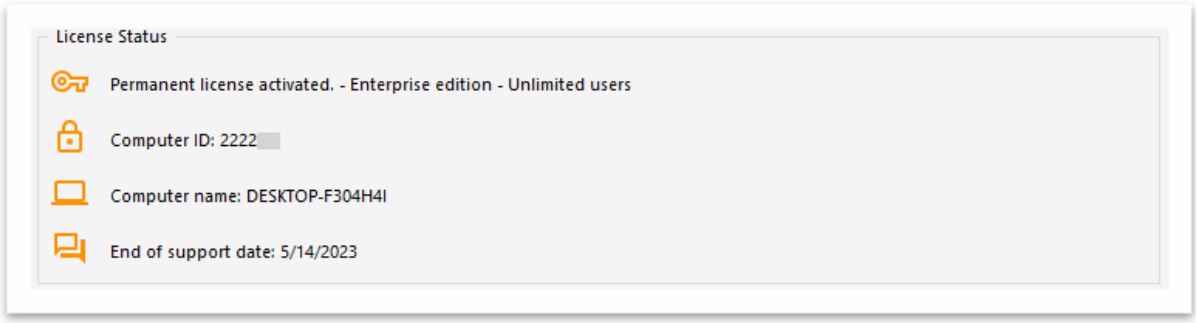
Obtendrá una lista de todas las licencias/soportes disponibles asignados a esta clave de activación, es decir, todas las licencias/soportes que aún no están activados:



Marque uno o más elementos y haga clic en el botón "Siguiente". Tenga en cuenta que puede activar varios productos al mismo tiempo marcando varios productos/soporte.



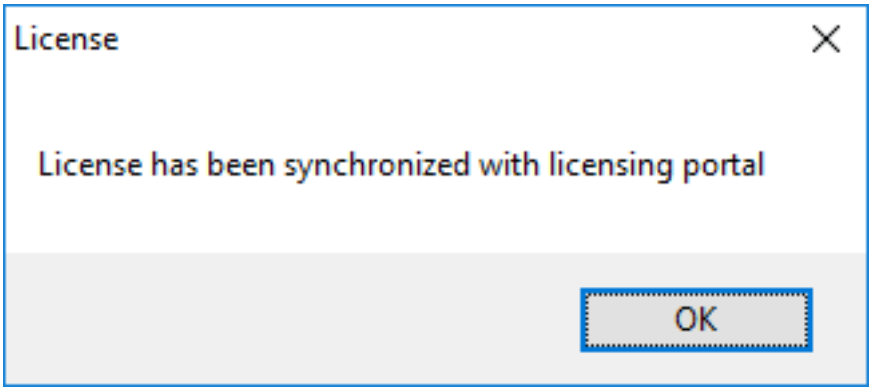
Todos sus productos/soporte están ahora activados (en este ejemplo, tanto TSplus con soporte como TSplus Advanced Security han sido activados a la vez).





Actualiza los datos de tu licencia haciendo clic en el botón correspondiente en la parte inferior de la página, se sincronizará la información con nuestro Portal de Licencias:





N.B Aún puedes descargar archivos license.lic en el Portal de Licencias para las Versiones Legadas de TSplus. Descargar la Guía del Usuario del Portal del Cliente .

Problema de activación:

Error de página o el botón "SIGUIENTE" no está funcionando. Aquí hay algunas soluciones.

Desactive su antivirus durante la activación de la licencia y verifique la configuración de su firewall y antivirus.

Verifique su navegador para el mensaje OK haciendo clic en este enlace: https://licenseapi.dl-files.com/licensing/ping

Si tiene un problema con un programa antivirus, el procedimiento es excluir los siguientes directorios: C:\Program Files (x86)\TSplus y C:\wsession

URLs para permitir en su antivirus y firewall para actualizaciones: setup.dl-files.com dl-files.com secure-download-file.com

Licencia / Telemetría: 93.88.241.55 Actualizaciones: 51.254.22.117 Actualizaciones de compatibilidad de TSplus / Buscar actualizaciones / Ver registro de cambios: 83.166.153.206

Puertos a permitir: (Puerto 3389 para RDP desde WAN, Puerto 80 para HTTP y 443 para HTTPS)

Verifica la configuración de seguridad de tu Internet
Panel de control > Opciones de Internet > Nivel personalizado Scripts > Scripts activos > Habilitar

Código de alerta fatal 40 70

Si encuentra códigos de alerta fatales 40/70 TLS en el Visor de eventos durante cada intento de sincronización o actualización.

Algunos conjuntos de cifrado TLS pueden estar deshabilitados. Puede usar software gratuito como **IIS Crypto 4.0** para verificarlos y habilitarlos.

Activando su licencia de soporte

La versión 15 de TSplus introdujo una nueva y fácil manera de gestionar su contrato de soporte anual.

La suscripción de soporte está disponible solo para licencias perpetuas. Las licencias de suscripción incluyen actualizaciones.

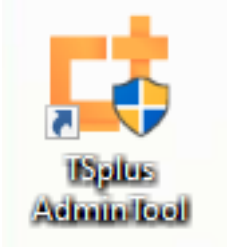
Los servicios de soporte incluyen nuestro servicio de soporte por Ticket/Email a nivel mundial, acceso al foro, rehosting de licencias, soporte de FAQ y tutoriales.

Los Servicios de Actualización incluyen la entrega de códigos de actualización, el derecho a instalar y utilizar cualquier nueva versión, parche y actualizaciones.

Estamos invirtiendo todos los días para mejorar TSplus y solucionar todos los problemas conocidos. Por lo tanto, recomendamos a todos nuestros clientes que mantengan su instalación de TSplus actualizada. La tarifa anual no es cara y está disponible en nuestra página de la tienda.

Paso Uno

Localiza la herramienta de administración en tu escritorio:



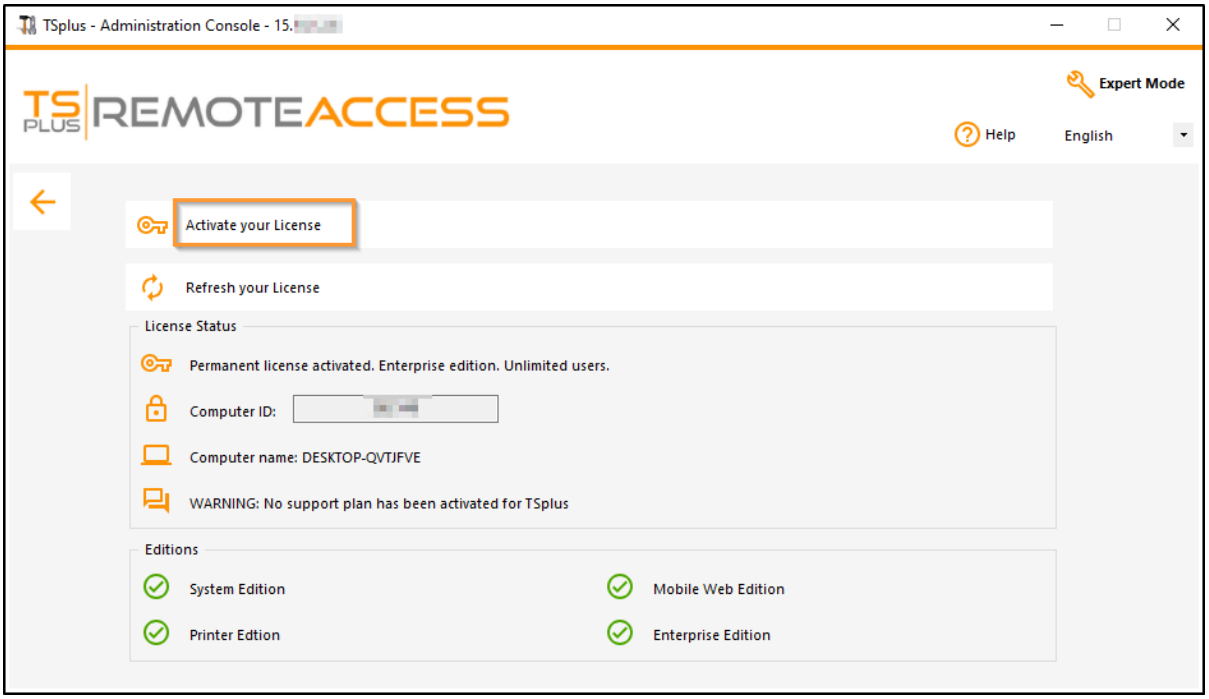
Haga doble clic en él, luego haga clic en el mosaico de la licencia.

- Si no puedes encontrar el acceso directo de la herramienta de administración, debería estar ubicado en la carpeta de escritorio de la cuenta de administrador utilizada para descargar TSplus. También puedes encontrar la carpeta de TSplus en esta ruta: ‘C:\Program Files (x86)\TSplus\UserDesktop\files’.

Haga clic en la pestaña de Licencia Ahora puede ver el número de serie:

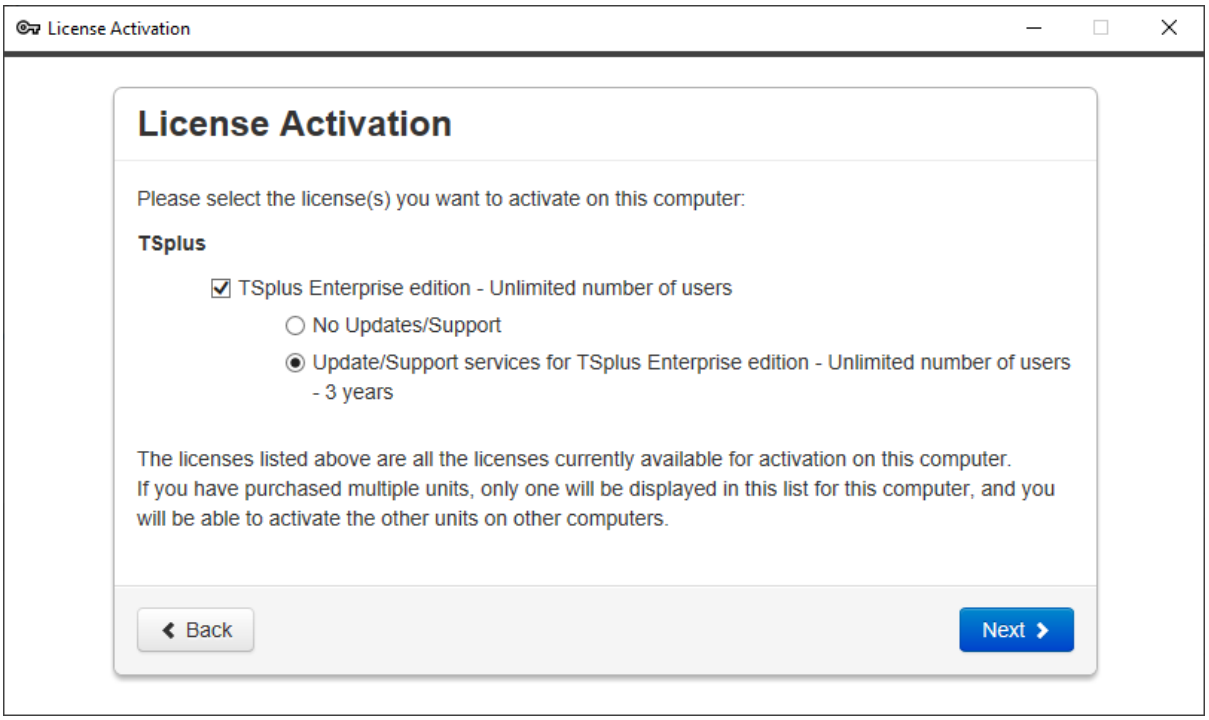
Paso Dos

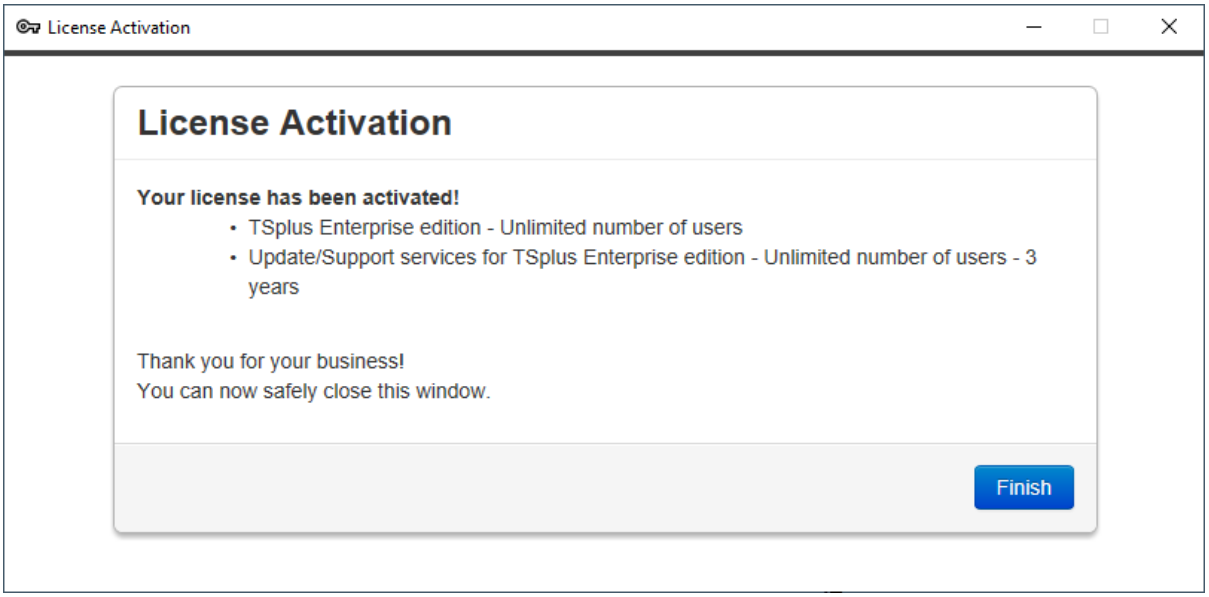
Haz clic en el mosaico "Activar tu licencia" e ingresa tu clave de activación.



Paso Tres

Luego selecciona "Extender el período de soporte":



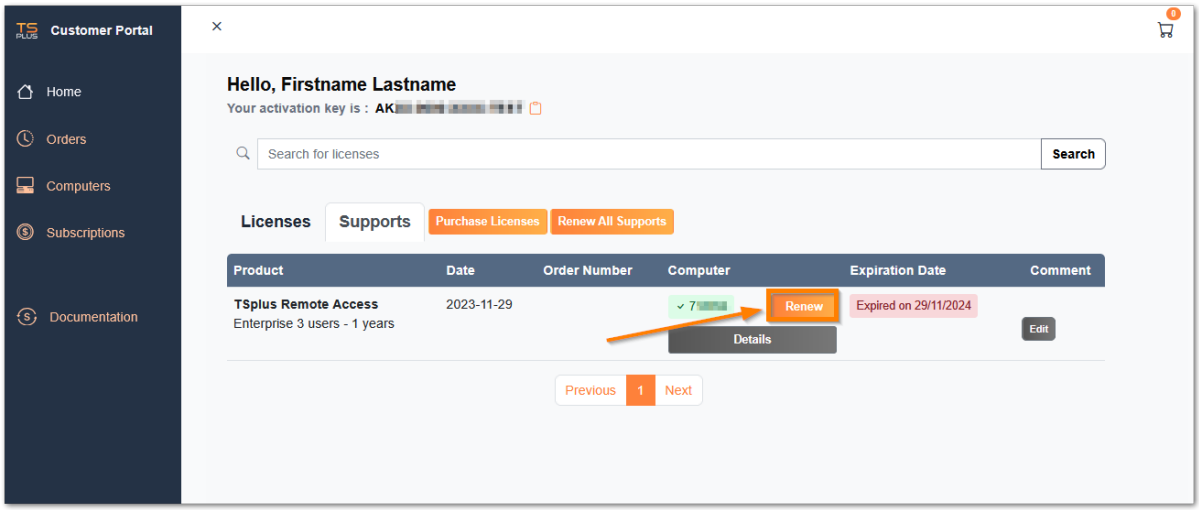


Extender una suscripción de actualización/soporte

Accede a tu portal de licencias: https://license.tsplus.net/login
ID: “Dirección de correo electrónico de compra”
Contraseña: “Número de orden de compra de su elección”

Luego, ve a la pestaña de Soporte e ingresa tu ID de computadora (visible en la pestaña de Licencia de AdminTool).

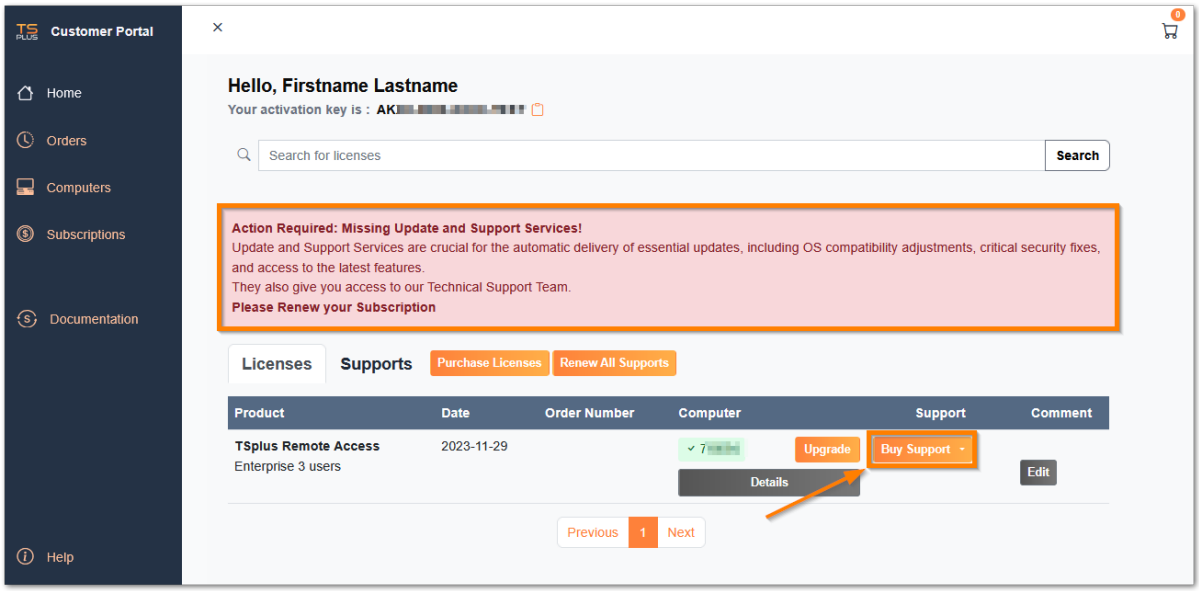
Luego haga clic en el botón "Renovar" para elegir la duración del soporte de 1, 2 o 3 años.



Si no tiene una suscripción de soporte para una licencia, aparecerá un mensaje en la pestaña de licencia que dice

Acción requerida: ¡Faltan actualizaciones y servicios de soporte!

Puedes comprar tu suscripción de soporte directamente haciendo clic en el botón “COMPRAR SOPORTE”.



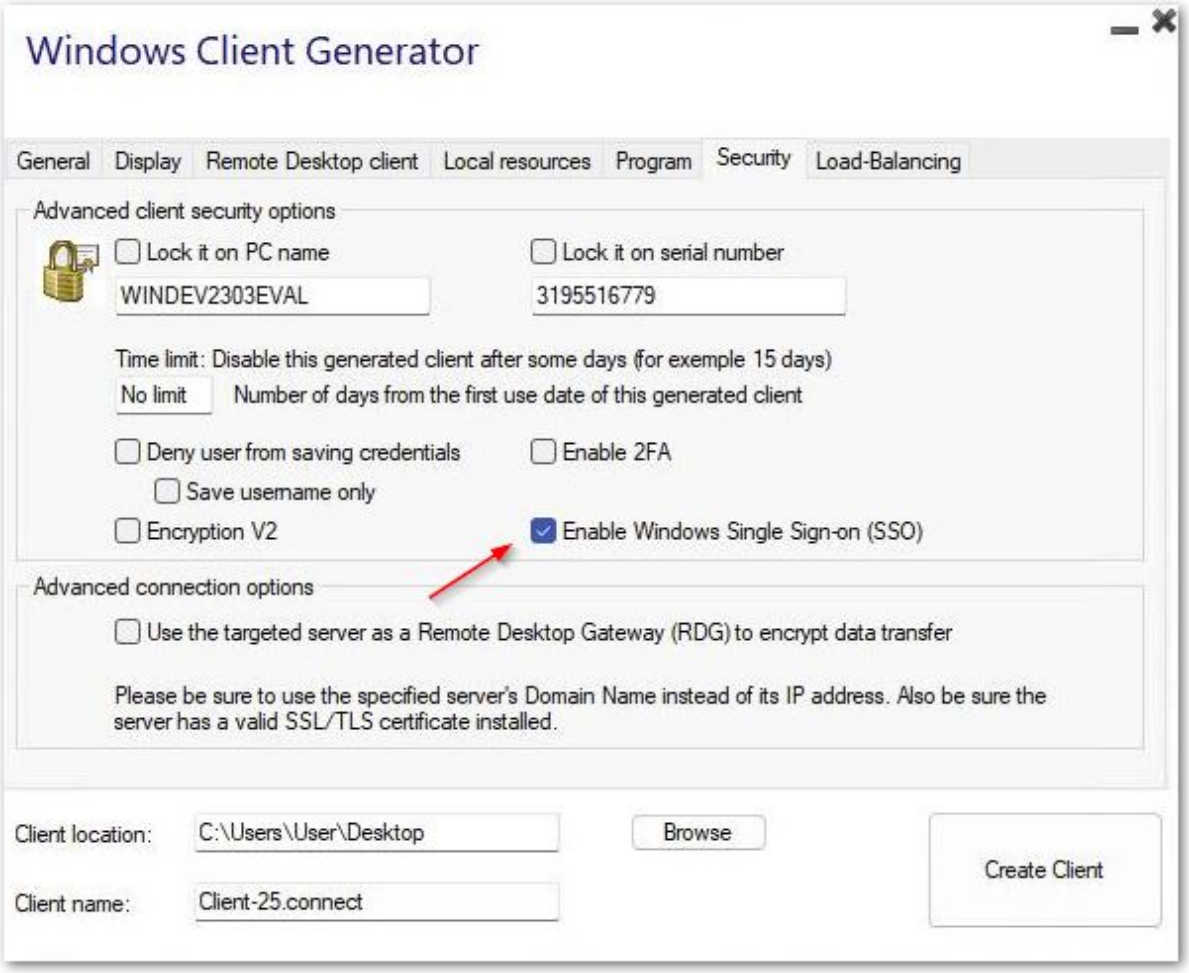
Directorio Activo Inicio de Sesión Único

Para habilitar la autenticación SSO de Windows para los clientes generados:

Actualiza TSplus Remote Access a la última versión en un servidor unido al dominio.

Generar un cliente desde el Generador de Clientes, marcando la casilla “Habilitar Inicio de Sesión Único (SSO)” en la pestaña “Seguridad”.

Conéctese desde una máquina unida al dominio utilizando el cliente generado.



Configurando la Directiva de Grupo para el Inicio de Sesión Único (SSO) de Windows a través del Cliente de Escritorio Remoto

Desde el controlador de dominio:

1. Abre la Consola de Administración de Políticas de Grupo.

2. Haga clic derecho en la Unidad Organizativa (OU) donde se debe aplicar el Objeto de Directiva de Grupo (GPO) y seleccione “Crear un GPO en este dominio y vincularlo aquí…”.

3. Nombra el GPO (por ejemplo, SSO_RDS_MI_SERVIDOR) y haz clic en "Aceptar".

4. Haga clic derecho en la política creada y seleccione "Editar".

5. Navegue a la siguiente ubicación: “Configuración del equipo / Políticas / Plantillas administrativas / Sistema / Delegación de credenciales.”

6. Haga doble clic en "Permitir delegar credenciales predeterminadas" para abrir la configuración.

7. Habilite la configuración y haga clic en "Mostrar..."

8. En el campo Valor, ingrese el(los) servidor(es) en el formato TERMSRV/ nombre_de_dominio_completo_del_servidor y haga clic en "Aceptar".

9. Haga clic en "Aplicar" y "Aceptar" para cerrar la ventana. Desde la máquina cliente:

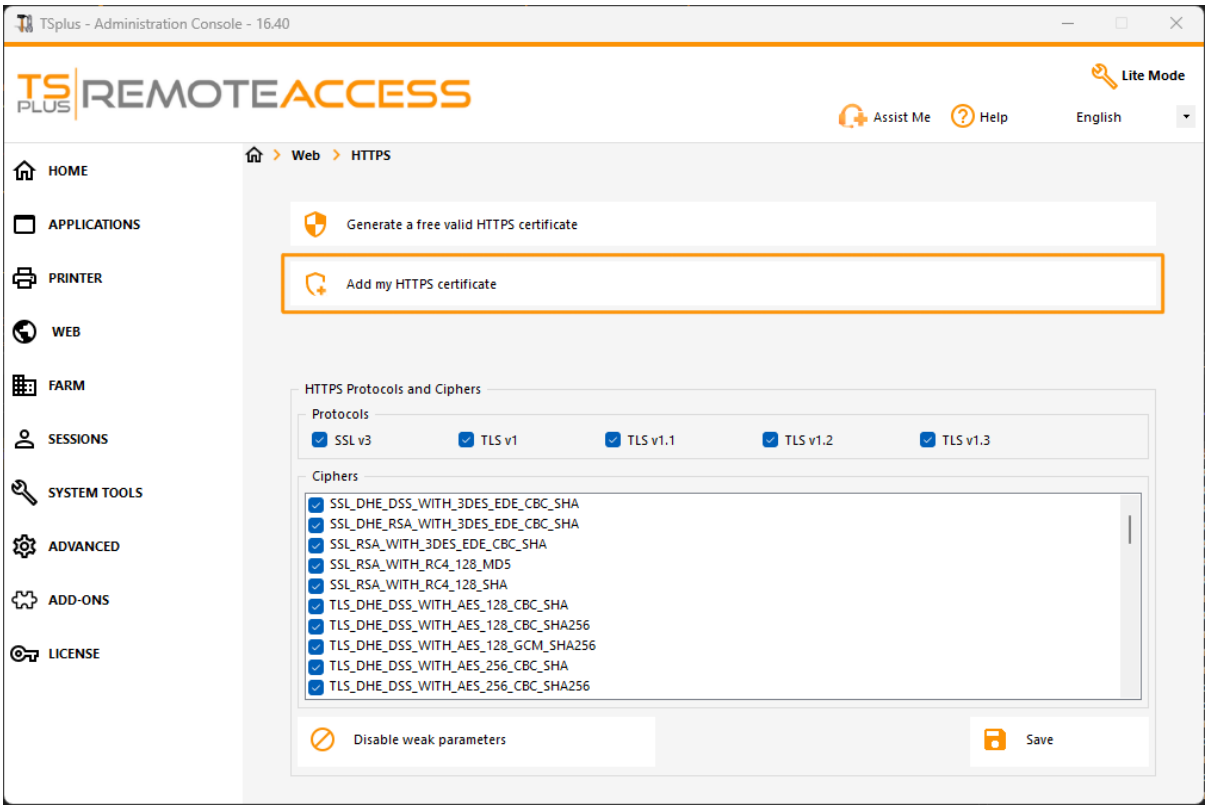
10. Actualice las políticas de grupo ejecutando el siguiente comando como administrador: gpupdate /force.

HTTPS y certificados SSL de terceros

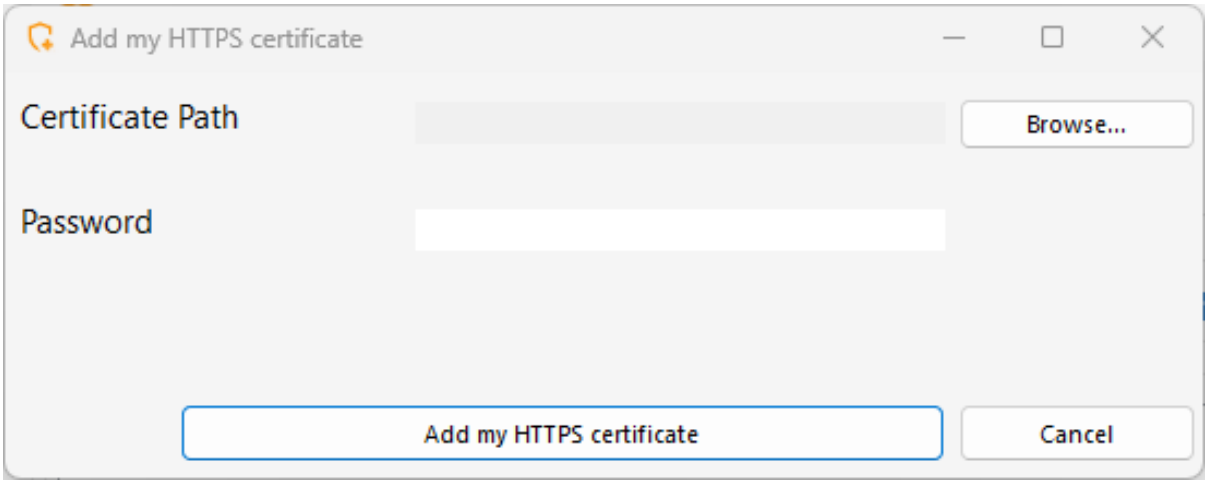
Agrega tu propio certificado

Si ya tiene un certificado HTTPS válido, puede agregarlo a su servidor web.

Abre TSPlus AdminTool, haz clic en la pestaña “Web”, ve al menú “HTTPS” y luego haz clic en “Agregar mi certificado HTTPS” como se muestra en la captura de pantalla a continuación:



Se abrirá una ventana donde podrás seleccionar tu certificado:



Su archivo de certificado debe utilizar el formato “.pfx”.

Si su certificado está protegido por una contraseña, puede ingresarla en el campo correspondiente.

Haga clic en el botón "Agregar mi certificado" para agregar su certificado.

Por favor, tenga en cuenta que necesitará renovar su certificado manualmente.

Enlaces adicionales

Proveedores de certificados SSL de confianza:

- GoDaddy
- DigiCert

Puedes convertir tu .pem en formato pfx con herramientas o sitios en línea. Por ejemplo, en este sitio: https://www.sslshopper.com/ssl-converter.html

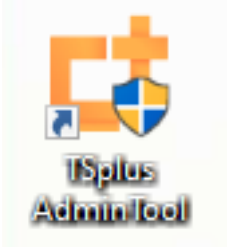
Puedes usar esto Herramienta de prueba de servidor SSL para validar la buena calidad de un portal web en HTTPS.

Resumen de la herramienta de administración de TSplus

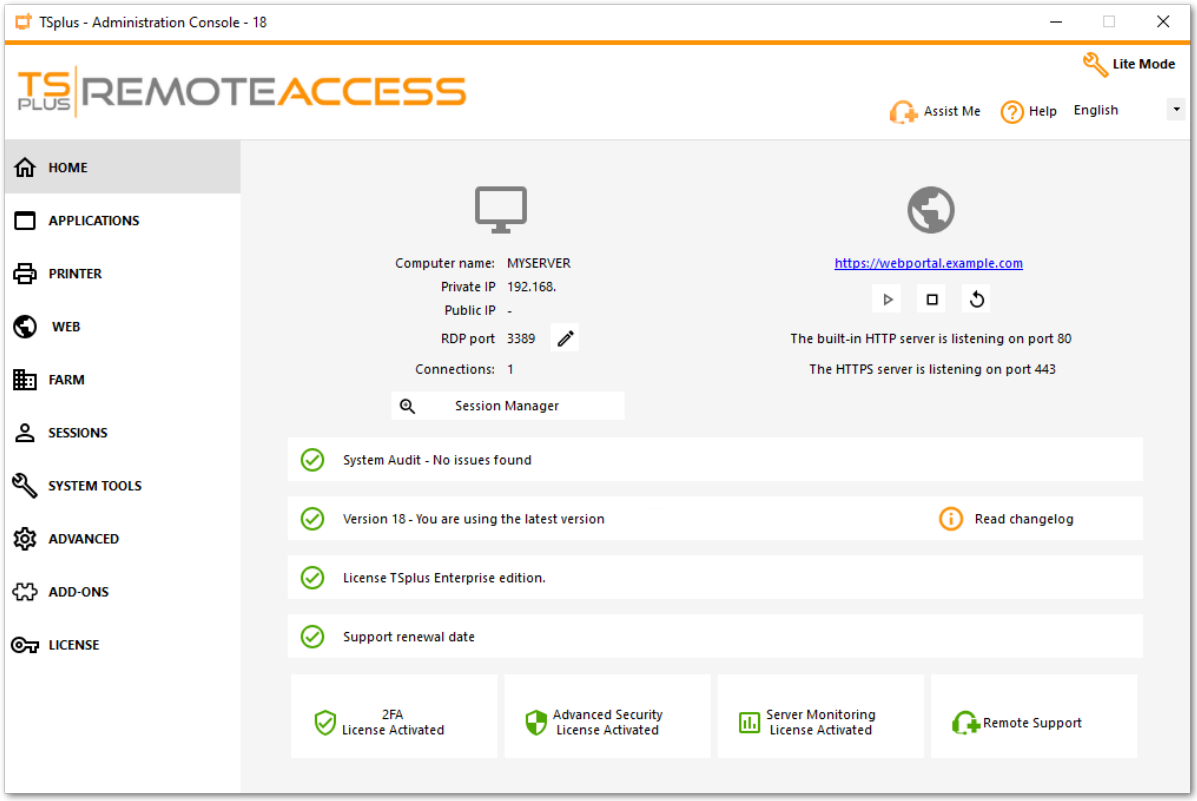
Después instalando TSplus su servidor está listo para funcionar de inmediato.

Sin embargo, puedes **personalizar todos los parámetros del sistema** con una poderosa herramienta de administrador.

Para hacerlo, haga clic en el siguiente ícono creado en su Escritorio:



La herramienta de administrador se mostrará a continuación:

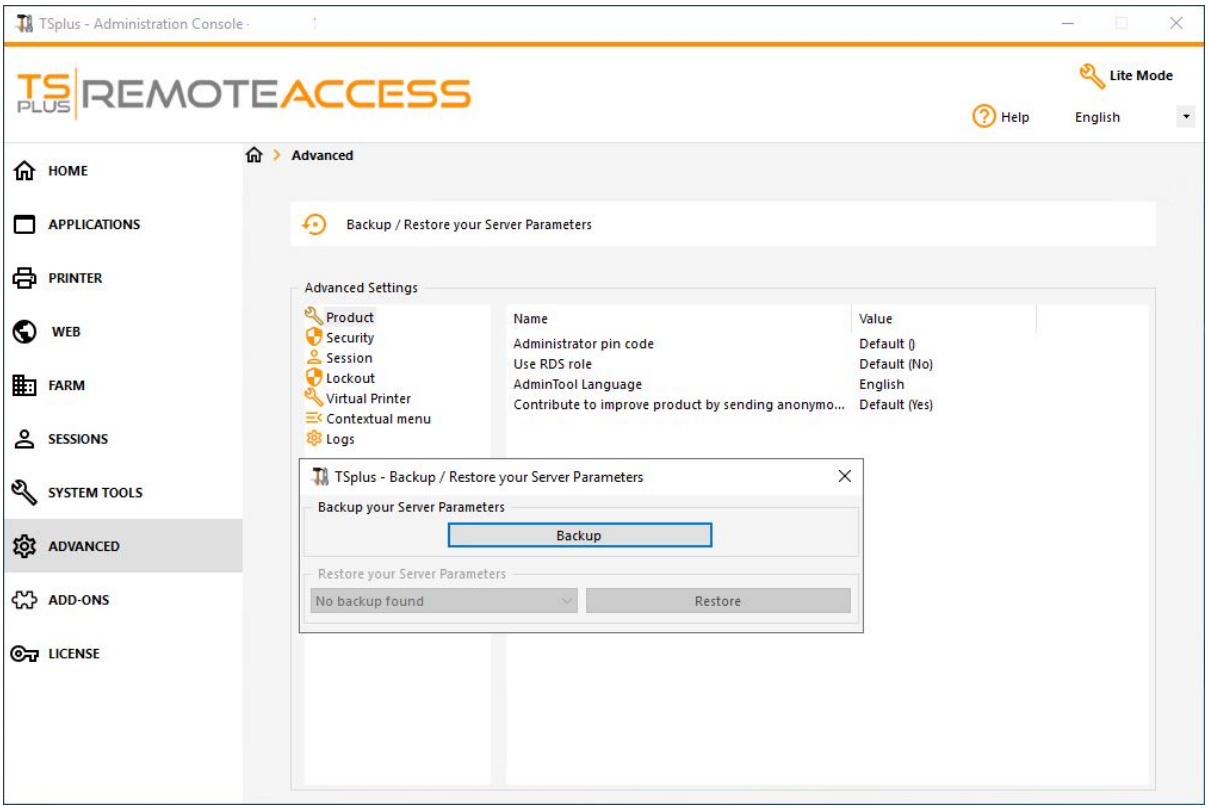


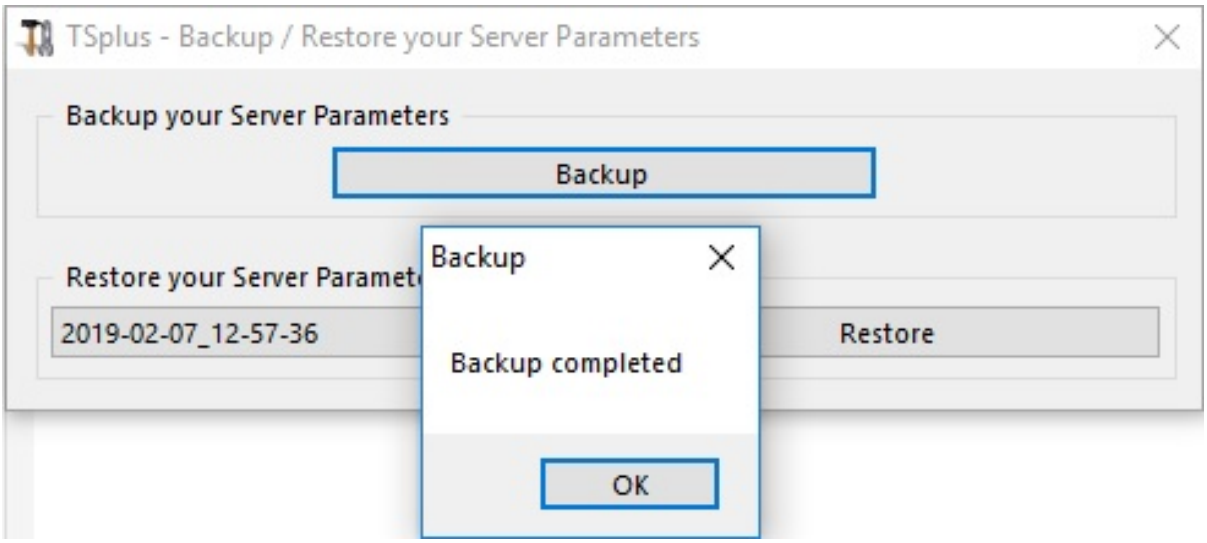
¿Quieres obtener ayuda sobre una función de TSplus Admin Tool rápidamente? Solo **haga clic en un mosaico o en una pestaña** ¡Ir a la ayuda correspondiente!

Copia de seguridad y restauración

Desde la versión 14 en el **Avanzado** pestaña, puedes configurar la configuración de TSplus.

Puedes hacer una copia de seguridad o restaurar los datos y configuraciones de TSplus haciendo clic en el botón “Copia de seguridad/Restaurar” en la parte superior:





El uso del comando se describe a continuación:

- **Copia de seguridad** :

admintool.exe /backup [ruta opcional a un directorio]

Por defecto, la copia de seguridad se creará en el directorio de archivos ubicado en la carpeta de configuración de seguridad de TSplus. Sin embargo, la copia de seguridad puede guardarse en una carpeta especificada. Se permiten rutas relativas y absolutas.

- **Restaurar** :

admintool.exe /restore [ruta a un directorio de respaldo]

El directorio de respaldo especificado debe contener una carpeta de datos y una carpeta de configuraciones, como se creó con el comando /backup.

si te gusta usar líneas de comando y te preguntas qué otras líneas de comando están disponibles, por favor ve a este documentación específica)

Por favor, siga los pasos a continuación para migrar TSplus de la computadora A a la computadora B:

1. En la computadora A, haga clic en el botón de Copia de seguridad para crear una nueva copia de seguridad. La configuración y los datos se guardarán en el directorio de archivos, ubicado en la carpeta C:\Backupparam.

2. Copia la nueva carpeta de respaldo creada (por ejemplo, llamada backup-2021-01-29_15-01-29), incluyendo todo el contenido, del directorio de archivos en la computadora A al directorio de archivos en la computadora B.

3. En la computadora B, desde la ventana de Copia de seguridad / Restaurar, en la sección "Restaurar", seleccione el nombre de copia de seguridad relevante que se va a restaurar.

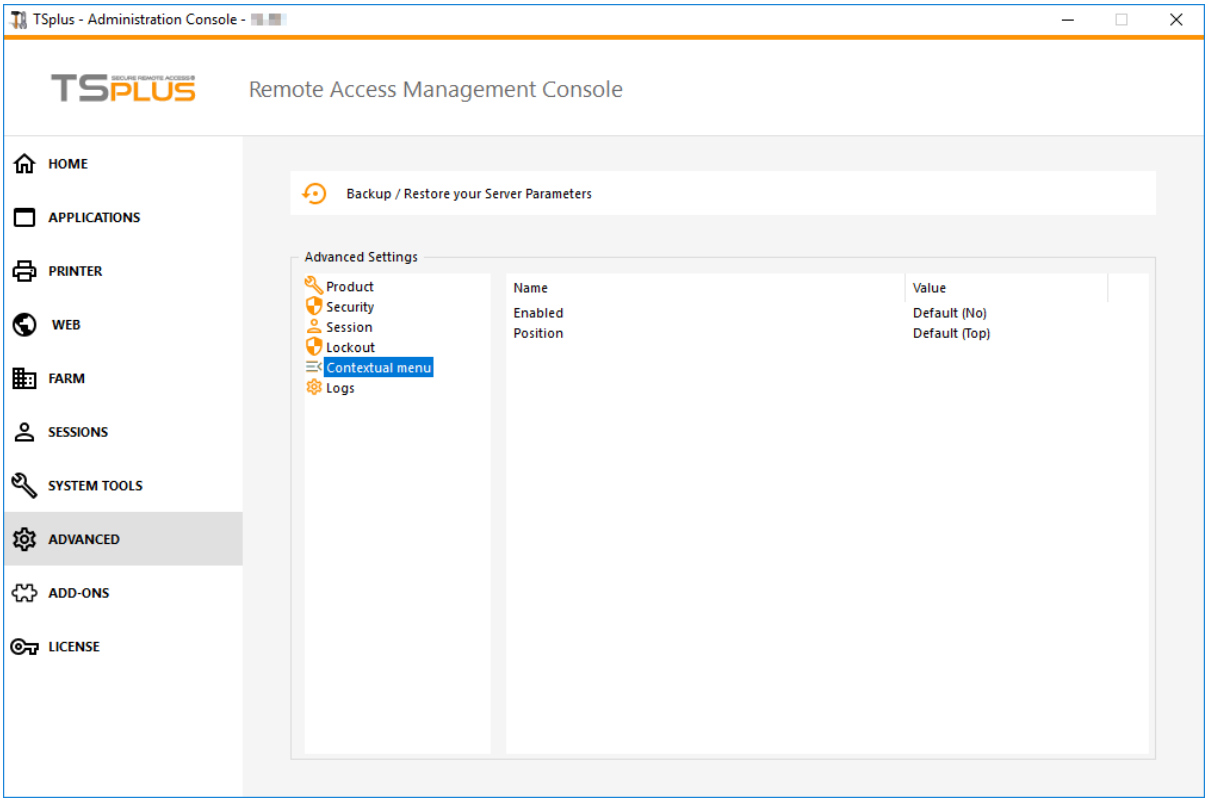
4. Luego, haga clic en Restaurar solo configuraciones para restaurar la configuración. Alternativamente, es posible hacer clic en Restaurar para restaurar todos los datos y configuraciones, lo cual no se recomienda para una migración, pero es útil para restaurar TSplus en la computadora A.

5. Por favor, espere un máximo de 2 minutos para que la configuración sea recargada por las funciones de TSplus.

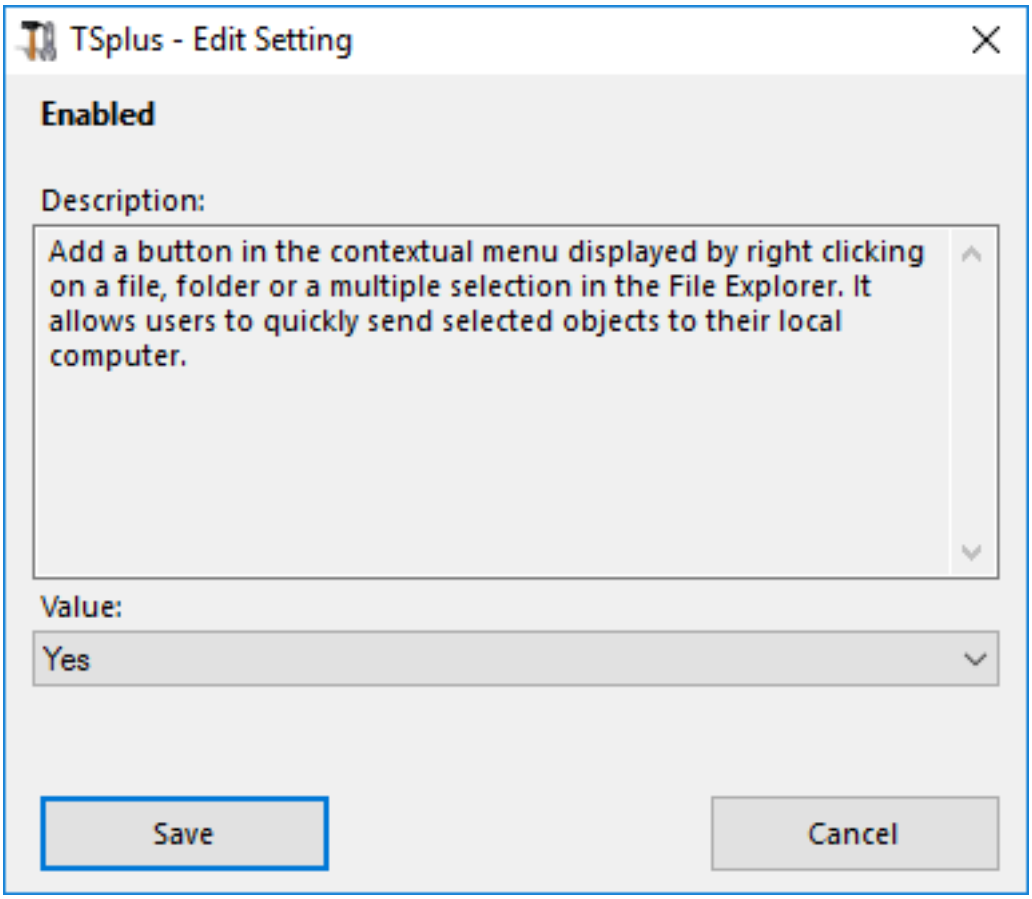
Funciones Avanzadas - Menú Contextual

Resumen

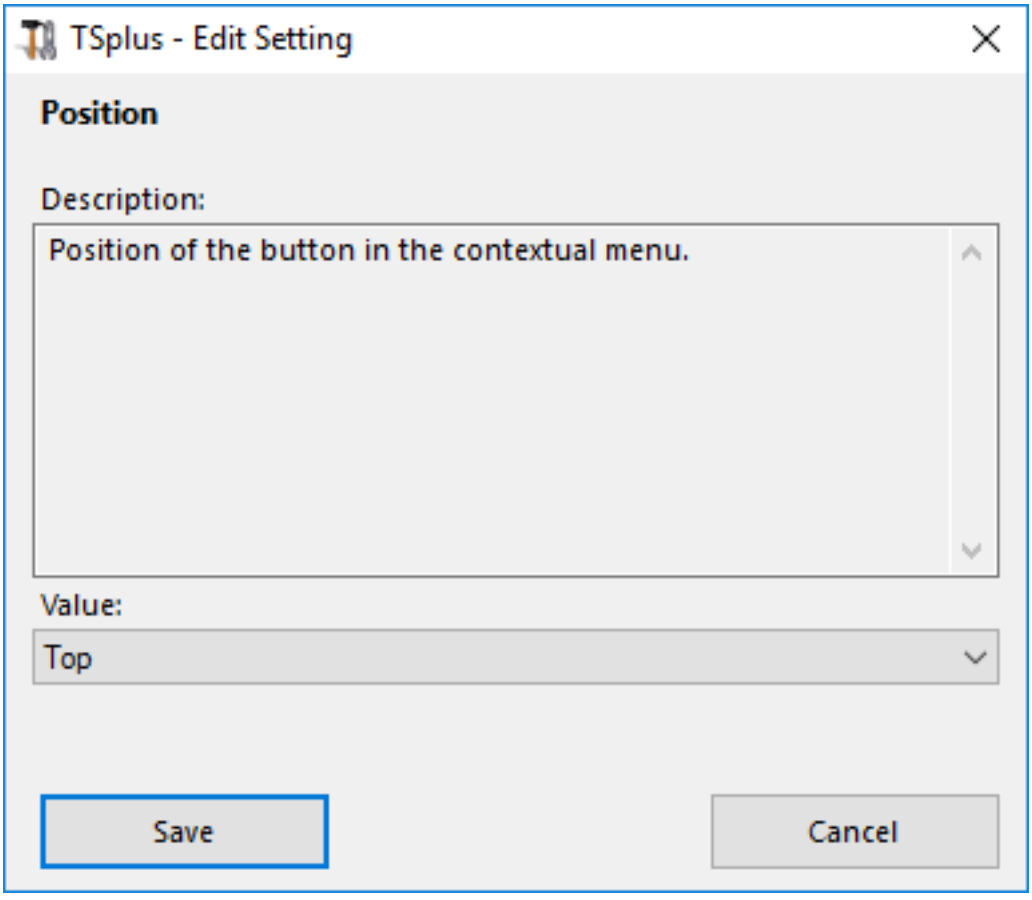
Desde la versión 12.50 de TSplus, un nuevo **Menú "Enviar al Cliente"** se puede habilitar en la pestaña Avanzado > Menú contextual para enviar fácilmente archivos a la estación de trabajo del cliente. Esta función funciona con todos los métodos de conexión.



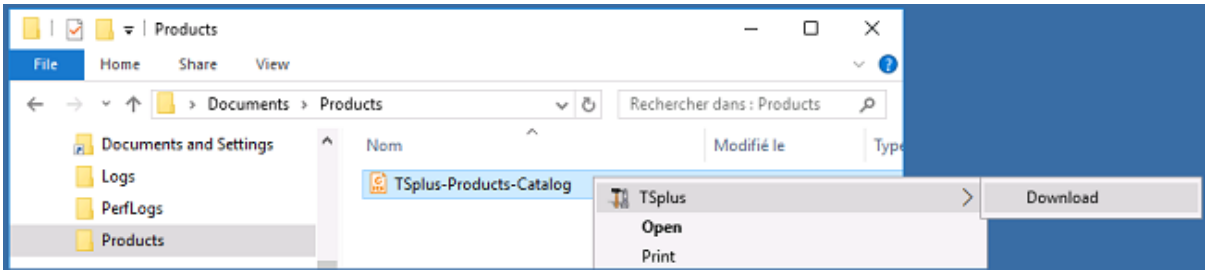
Por defecto, esta función está desactivada. Seleccione el valor "Sí" y luego haga clic en "Guardar" para habilitarla.



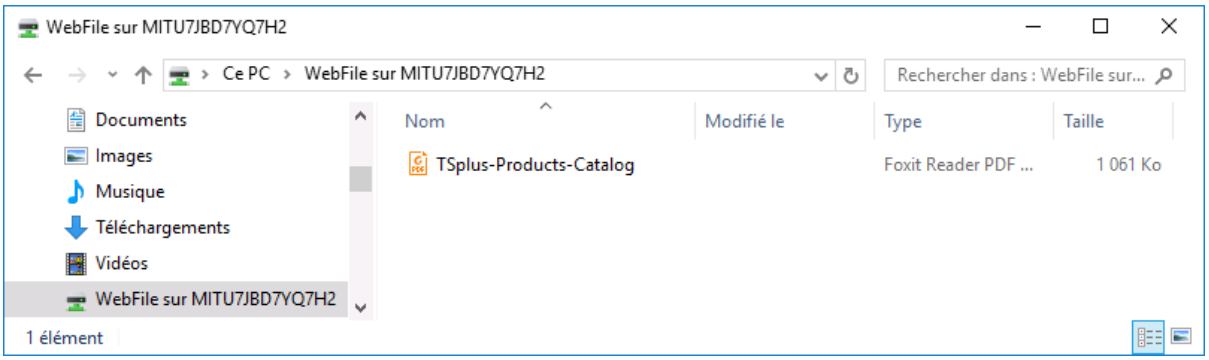
También puedes cambiar su posición. Por defecto, se mostrará en la parte superior:



Este es un menú contextual de clic derecho. Simplemente seleccione la carpeta o archivos deseados, haga clic derecho sobre ellos, seleccione la pestaña “TSplus” y simplemente haga clic en “Descargar”:



Encontrará su descarga en la carpeta Webfile y en la carpeta "Descargas" de su navegador web.

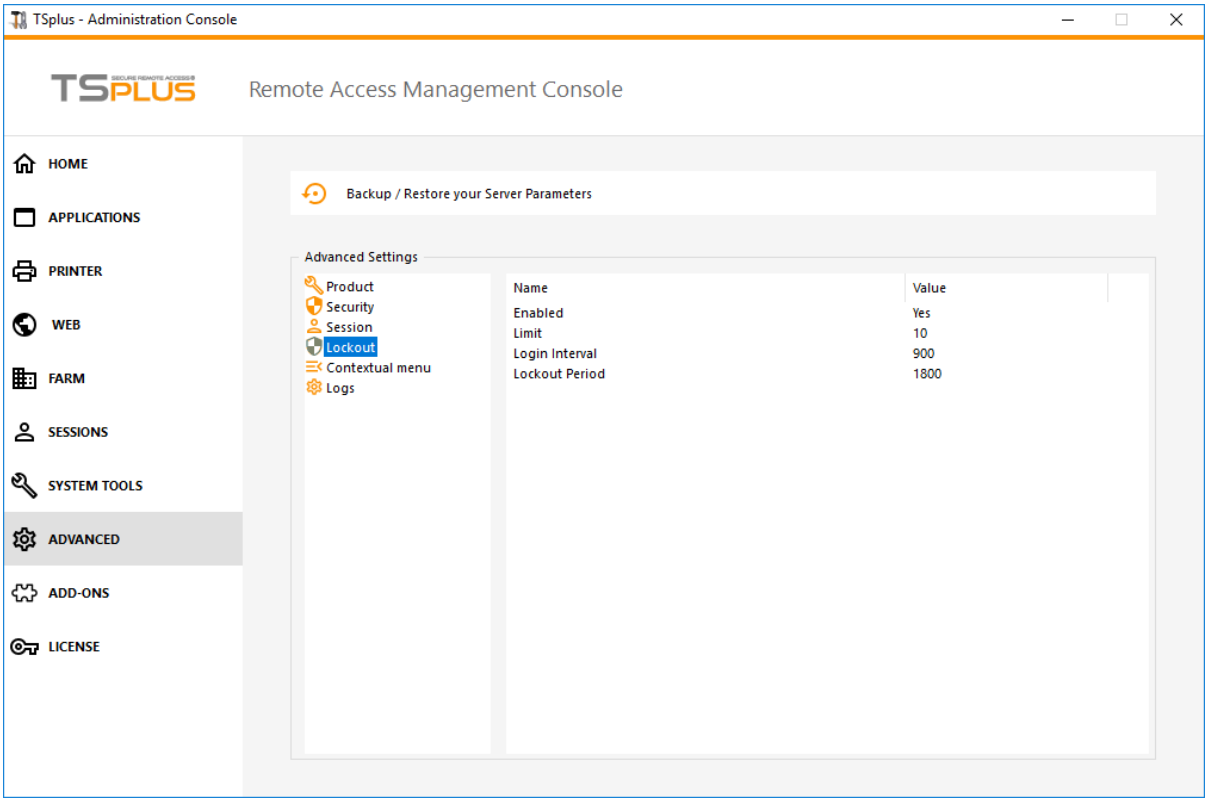


Cada carpeta descargada se comprime automáticamente en un archivo zip.

Funciones Avanzadas - Bloqueo

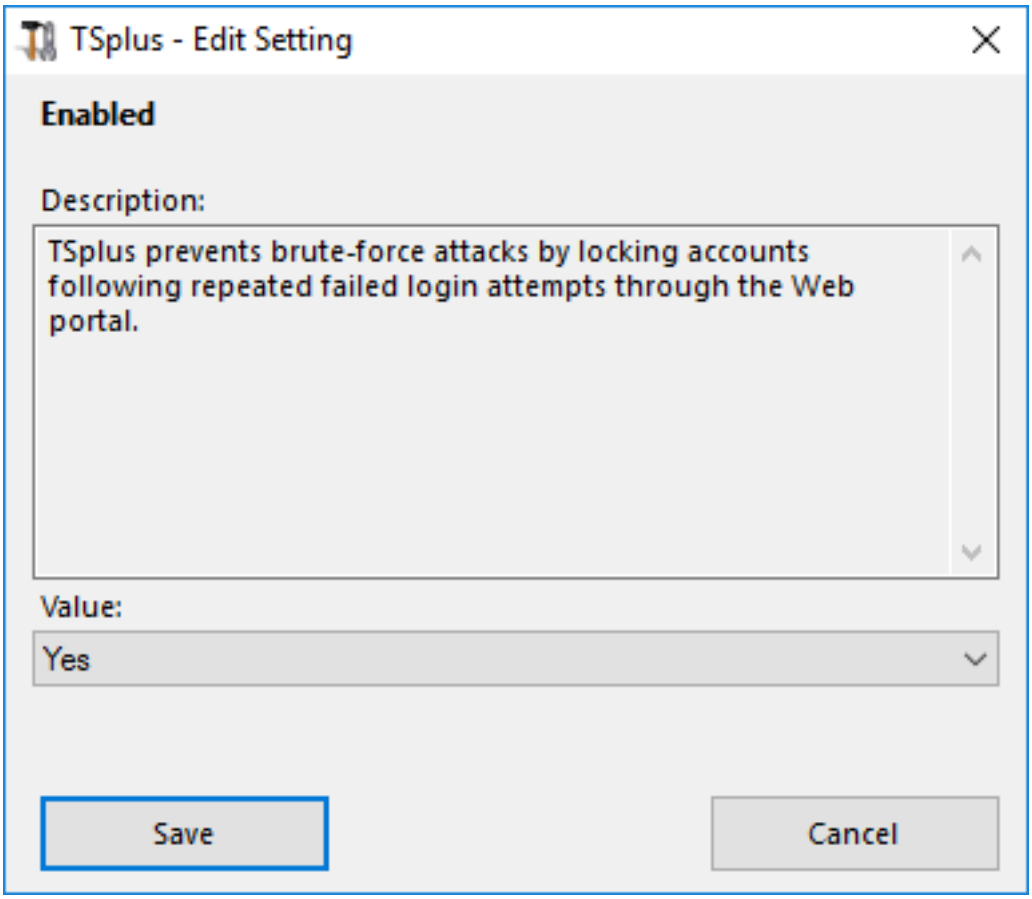
Resumen

En esta pestaña, puedes habilitar/deshabilitar y configurar TSplus Lockout configuración.



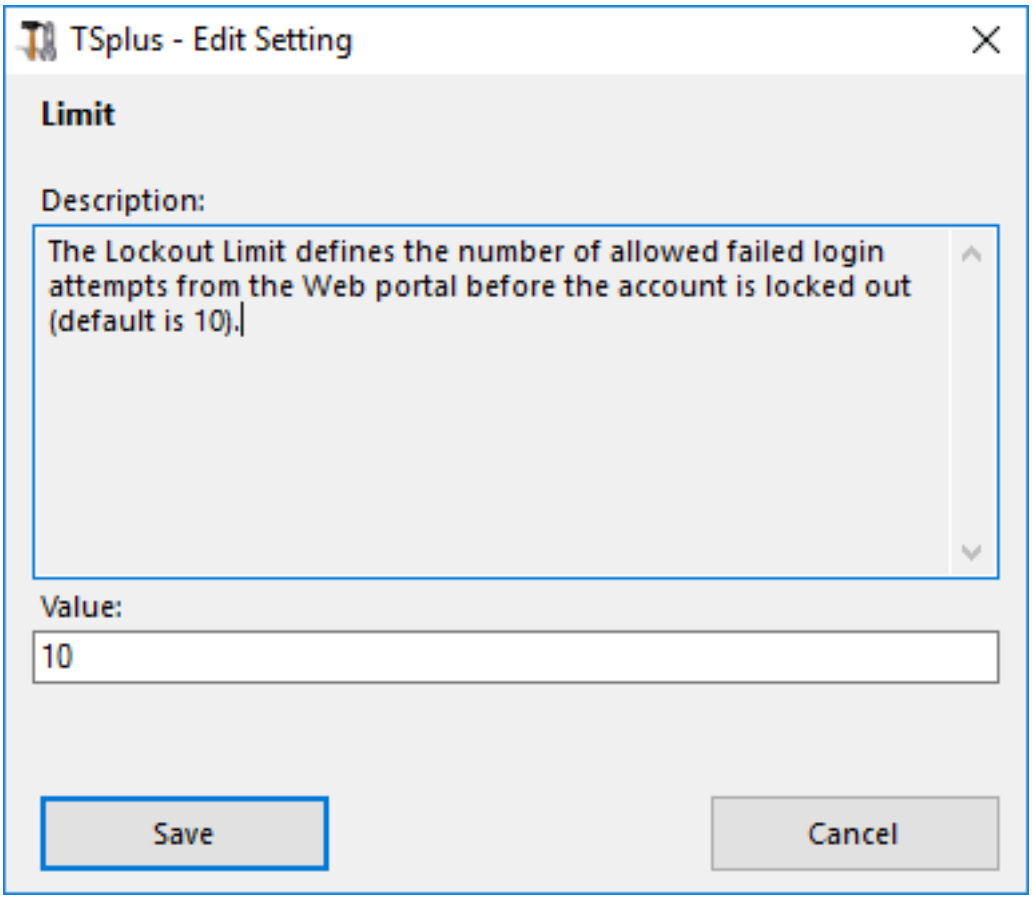
Habilitar/Deshabilitar la función de bloqueo

La función de bloqueo está habilitada por defecto. Puedes desactivarla cambiando el valor de "Sí" a "No" en esta ventana, luego haz clic en guardar.



Límite

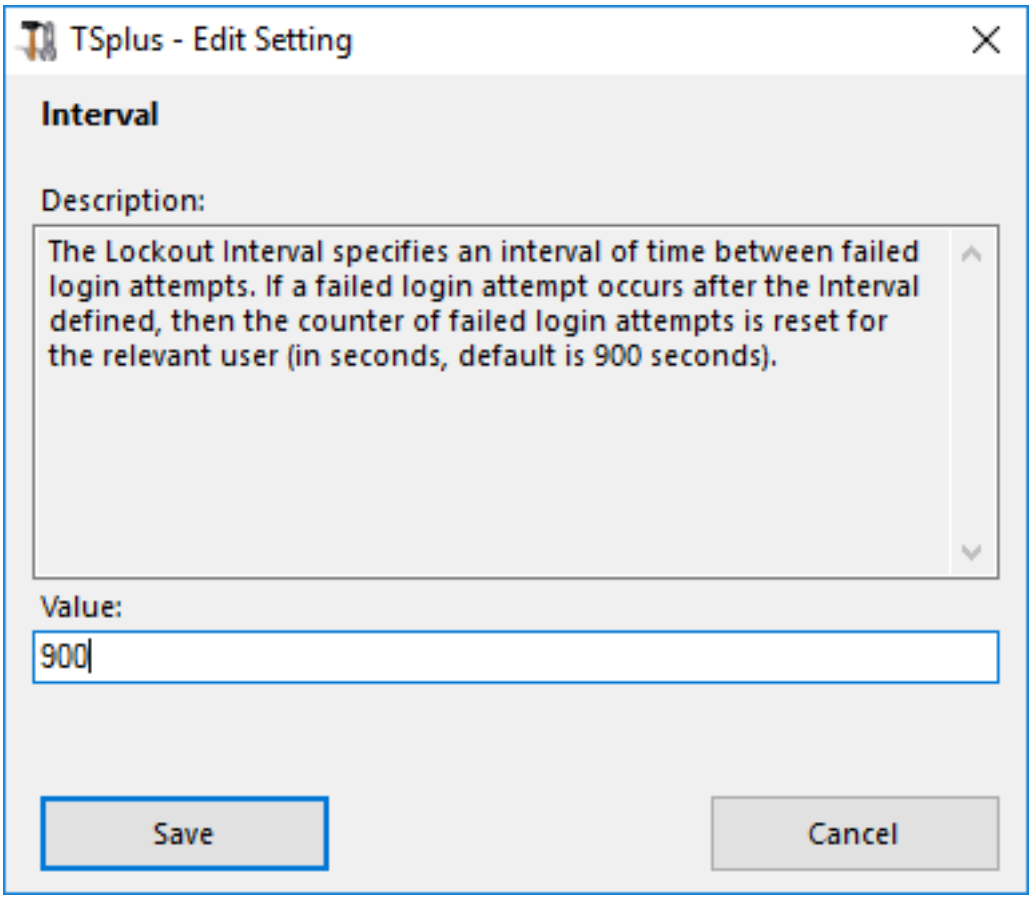
El límite de bloqueo define el número de intentos de inicio de sesión fallidos permitidos desde el portal web antes de que la cuenta sea bloqueada (el valor predeterminado es 10). Puede modificar este valor ingresando el valor deseado en el campo correspondiente y haciendo clic en guardar.



Interval

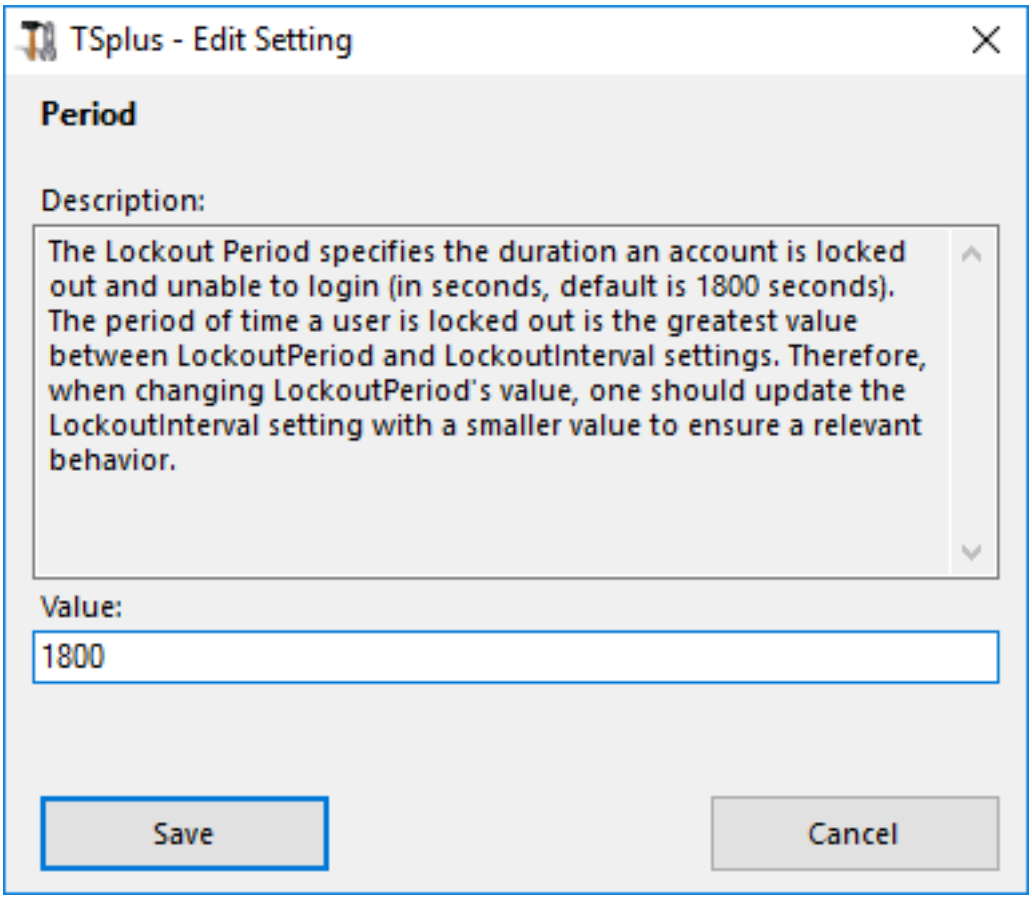
El intervalo de bloqueo especifica un intervalo de tiempo entre intentos de inicio de sesión fallidos.

Si ocurre un intento de inicio de sesión fallido después del intervalo definido, entonces el contador de intentos de inicio de sesión fallidos se restablece para el usuario correspondiente (en segundos, el valor predeterminado es 900 segundos). Puedes modificar este valor ingresando el valor deseado en el campo correspondiente y haciendo clic en guardar.



Período

El período de bloqueo especifica la duración durante la cual una cuenta está bloqueada y no puede iniciar sesión (en segundos, el valor predeterminado es 1800 segundos). El período de tiempo durante el cual un usuario está bloqueado es el mayor valor entre las configuraciones de LockoutPeriod y LockoutInterval. Por lo tanto, al cambiar el valor de LockoutPeriod, se debe actualizar la configuración de LockoutInterval con un valor menor para garantizar un comportamiento relevante. Puede modificar este valor ingresando el valor deseado en el campo correspondiente y haciendo clic en guardar.


TSplus - Edit Setting
Period
Description:
The Lockout Period specifies the duration an account is locked out and unable to login (in seconds, default is 1800 seconds). The period of time a user is locked out is the greatest value between LockoutPeriod and LockoutInterval settings. Therefore, when changing LockoutPeriod's value, one should update the LockoutInterval setting with a smaller value to ensure a relevant behavior.
Value:
1800
Save
Cancel

Funciones Avanzadas - Registros

Resumen

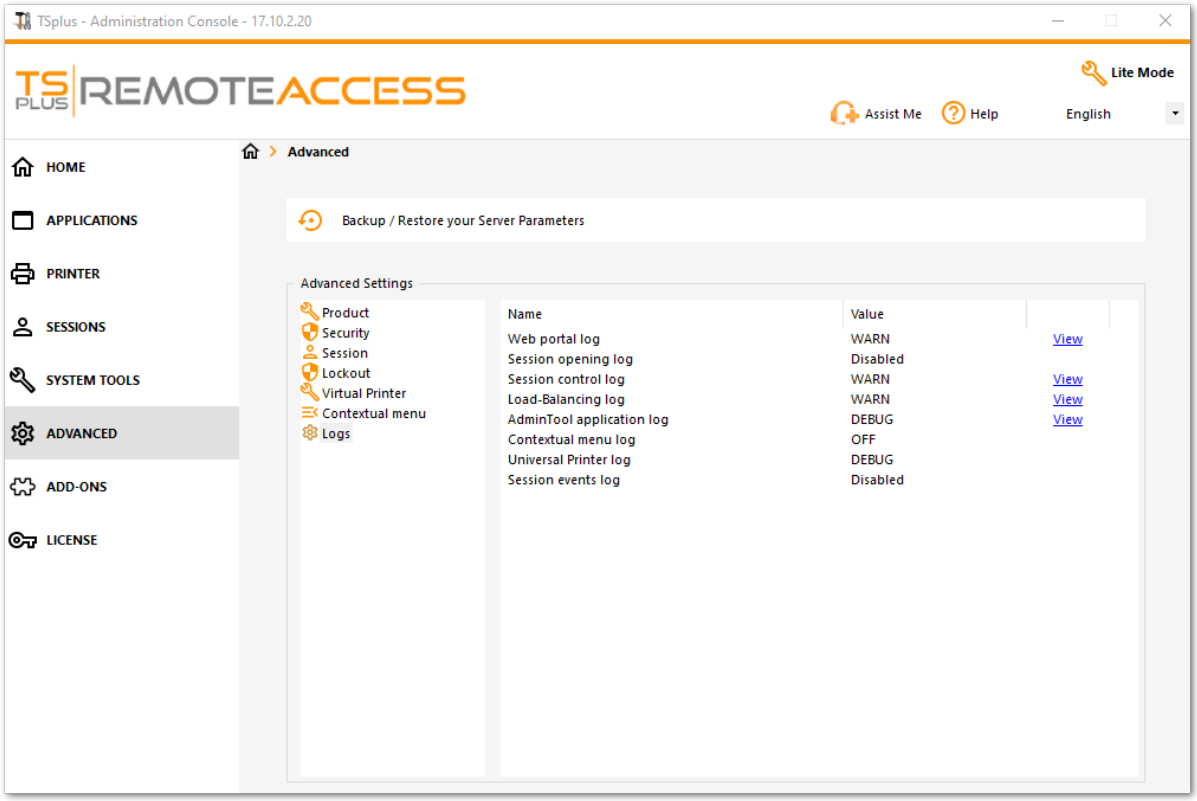
En esta pestaña, puedes configurar la configuración de los registros de TSplus.

Por defecto, TSplus no crea registros para evitar problemas de rendimiento.

Los registros existen para encontrar más fácilmente el origen de los errores encontrados en TSplus y puedes habilitarlos de la siguiente manera:

- ir a C:\wsession
- crea la carpeta 'Trace'. Los registros se crearán automáticamente allí, por usuario.

Deberá activar la generación de registros en AdminTool > Avanzado > Registros



Hay 5 tipos de registros:

- El registro del Portal Web,
- El registro de apertura de sesión,
- El registro de control de sesión,
- El registro de balanceo de carga y
- El registro de la aplicación AdminTool (interfaz).

Los niveles de registro corresponden a diferentes componentes, nuestro equipo de soporte te dirá qué valor poner según el problema encontrado.

Aquí están los diferentes nombres y ubicaciones de los archivos de registro:

- Web Portal log: “C:\Program Files (x86)\TSplus\Clients\www\cgi-bin\hb.log”

- Registro de apertura de sesión: “C:\wsession\trace”
- Registro de control de sesión: “C:\Program Files (x86)\TSplus\UserDesktop\files\APSC.log”
- Registro de Balanceo de Carga: “C:\Program Files (x86)\TSplus\UserDesktop\files\svcenterprise.log”
- AdminTool aplicación registro: “C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.log”
- RDS-Knight / TSplus Advanced Security: “C:\Program Files (x86)\TSplus-Security\logs”

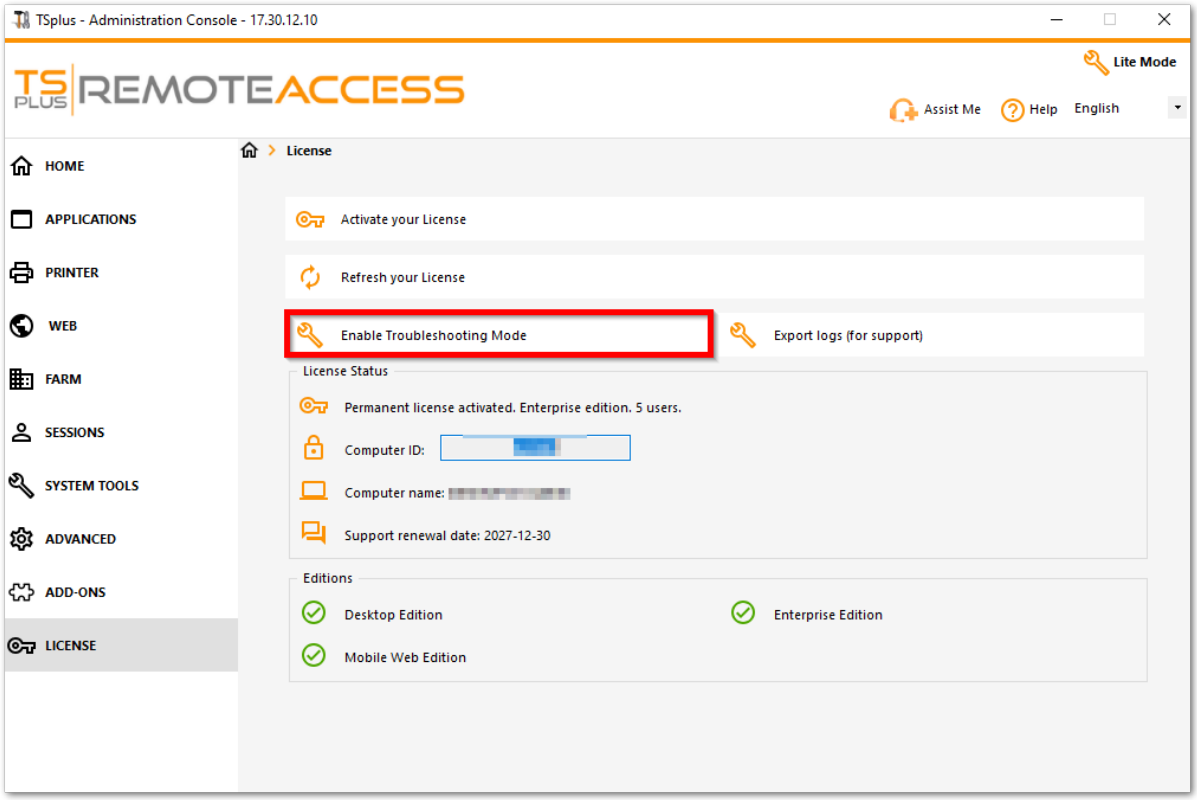
Puede habilitar los registros para el Cliente de Conexión en el lado del cliente agregando la siguiente clave del registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\ConnectionClient “Debug”=“true”

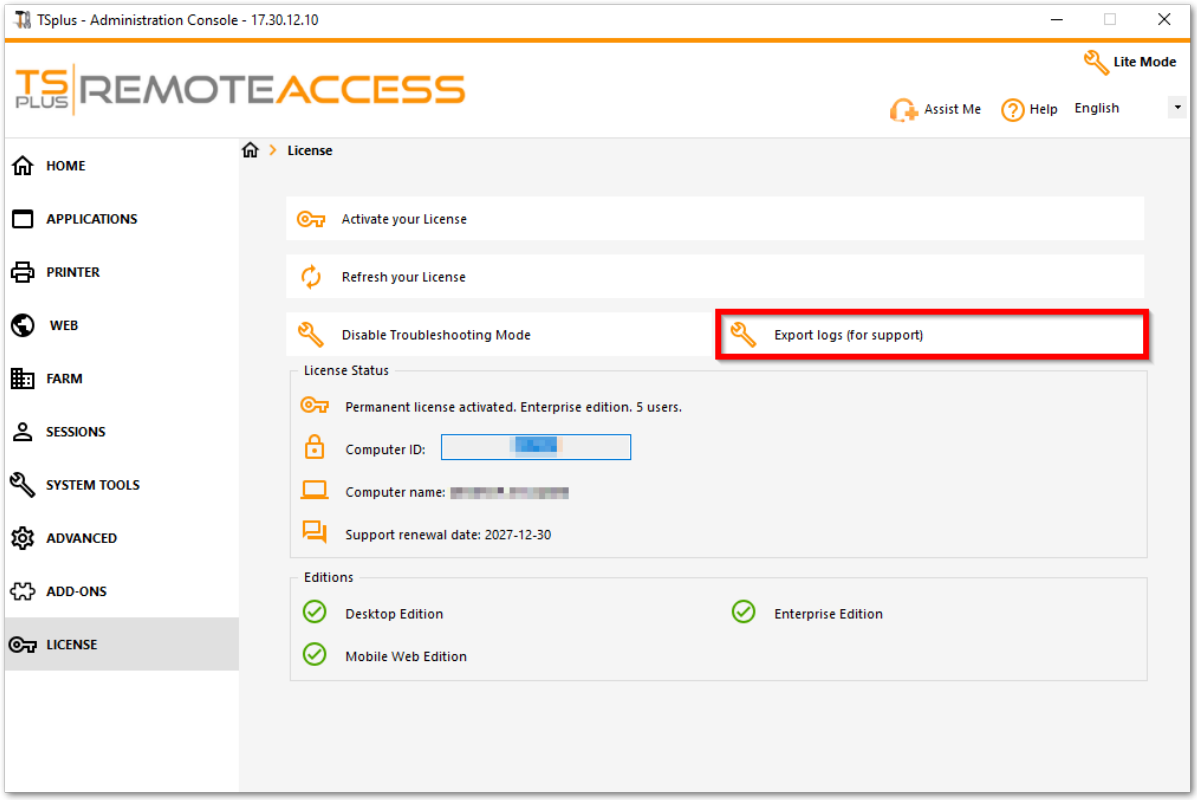
Los registros se encuentran en C:\Users RDP6\logs directory si la instalación es por usuario o en C:\Program Files (x86)\Connection Client\RDP6\logs directory si la instalación es para todos los usuarios.

Habilitar el modo de solución de problemas

Ve a la pestaña "Licencia" Haz clic en el **Habilitar el modo de solución de problemas** botón.



Reproduzca su problema, luego haga clic en el **Exportar registros (para soporte)** botón para enviar los registros al equipo de soporte por correo electrónico.



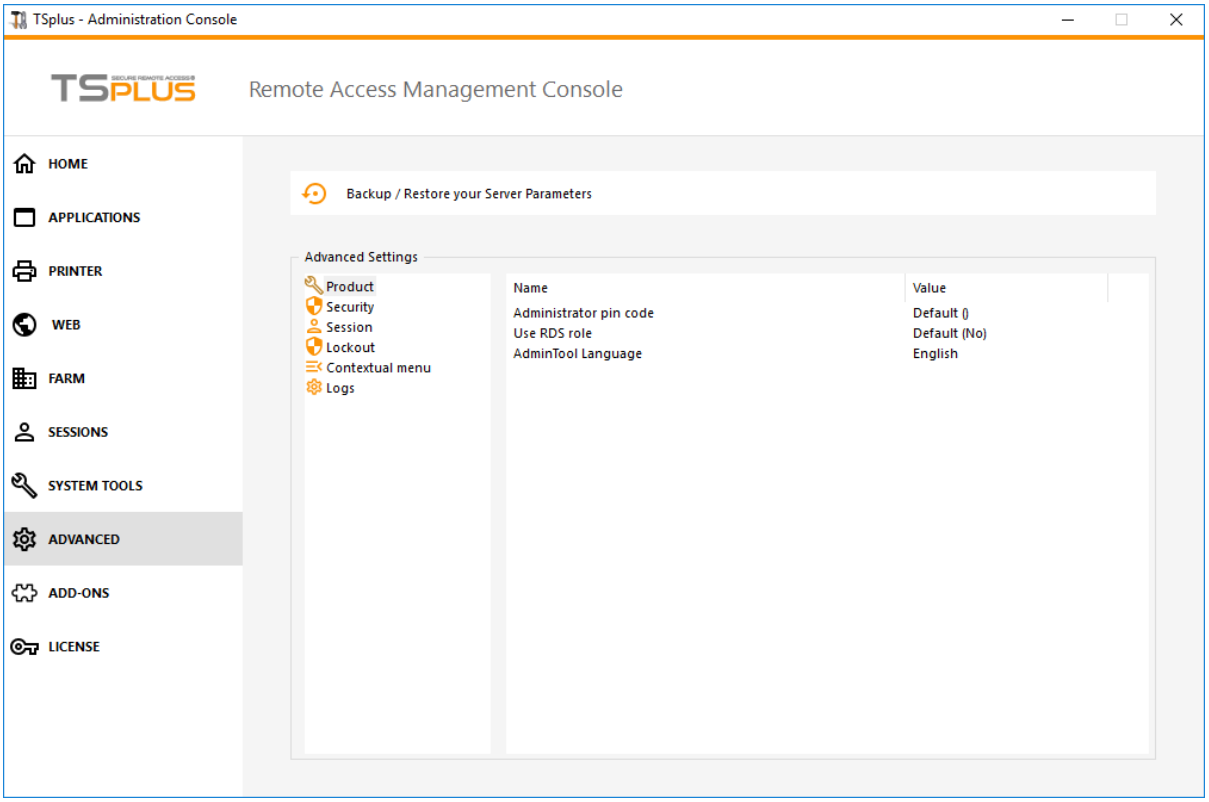


El formato del archivo a enviar es **.zip.logs** archivos y está protegido por la contraseña **contraseña** .

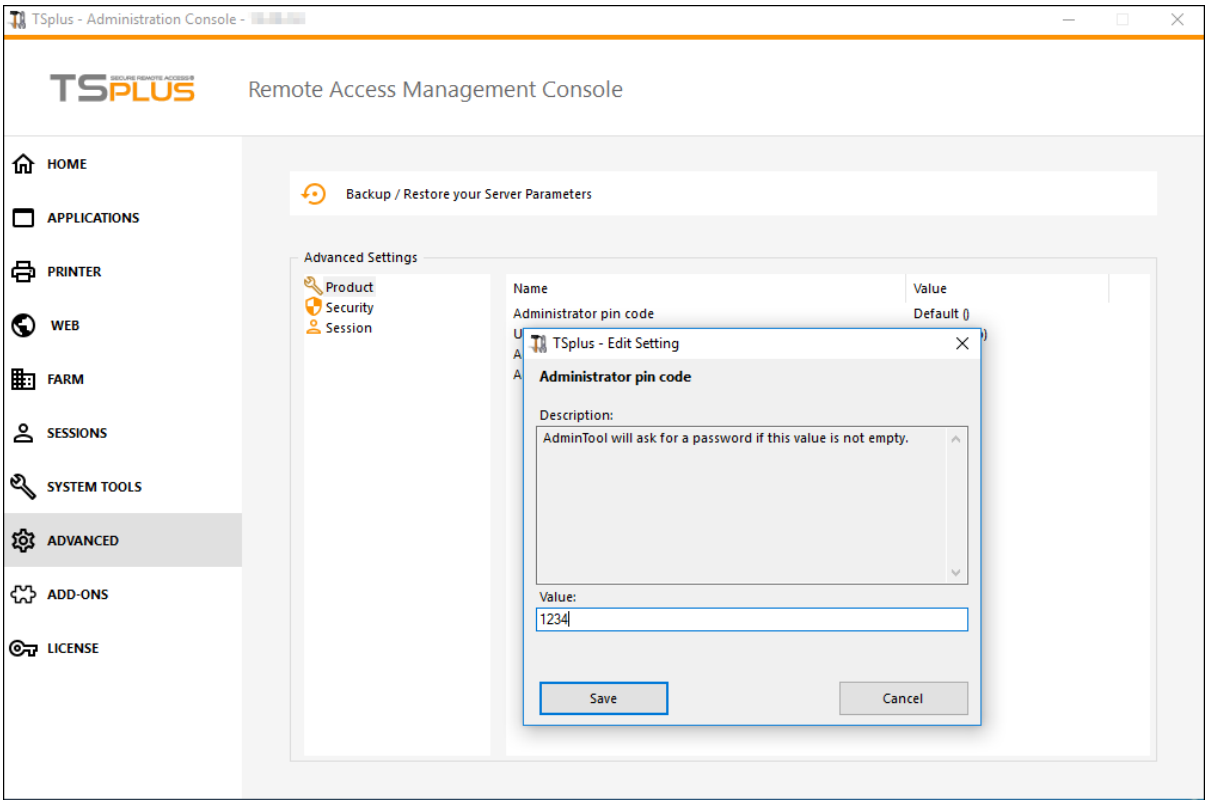
Funciones Avanzadas - Producto

Resumen

En esta pestaña, puedes modificar la configuración de TSplus añadiendo un código PIN de AdminTool, utilizar el rol de RDS de Windows y personalizar el color de fondo y el idioma de AdminTool.



El Administrador puede asegurar el acceso a la Herramienta del Administrador configurando un código PIN que se solicitará en cada inicio, en la pestaña Avanzada de la AdminTool, bajo la Configuración del Producto:

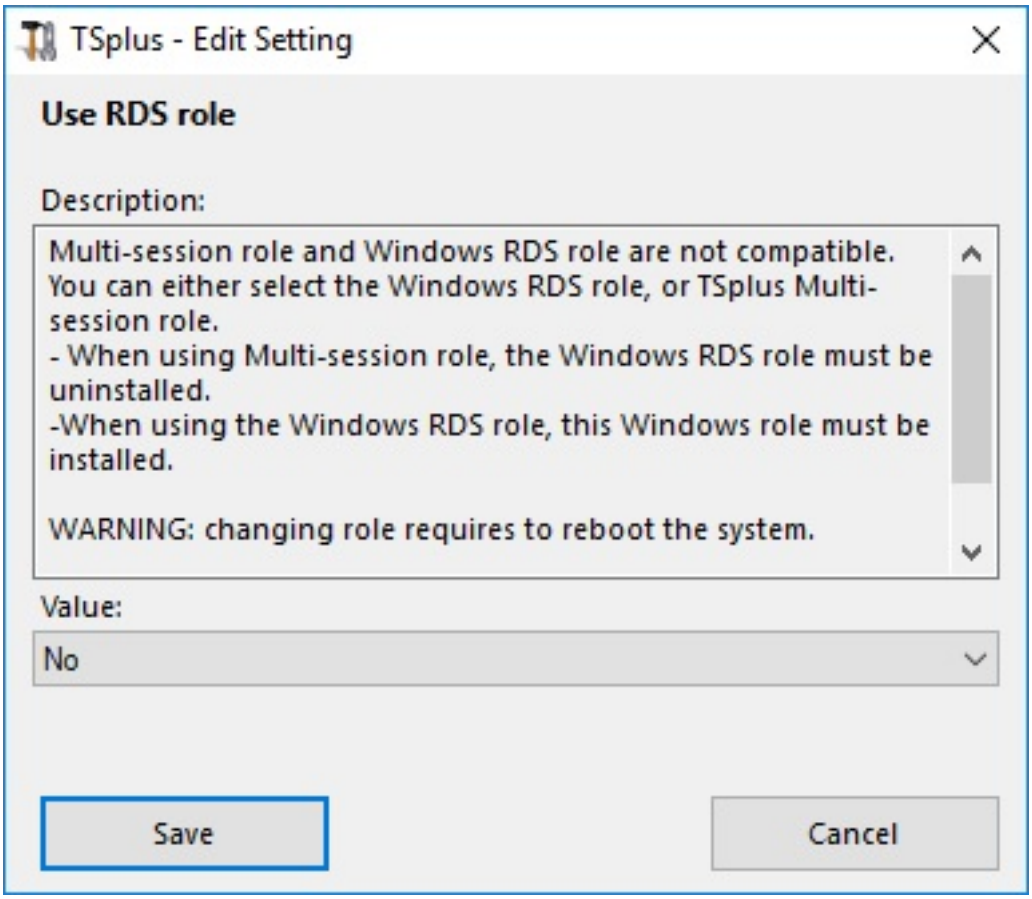


Usar el rol de RDS

El rol de múltiples sesiones y el rol de Windows RDS no son compatibles. Puedes seleccionar el rol de Windows RDS o el rol de múltiples sesiones de TSplus.

- Al utilizar el rol de múltiples sesiones, el rol de RDS de Windows debe ser desinstalado.
- Al utilizar el rol de RDS de Windows, este rol de Windows debe estar instalado.

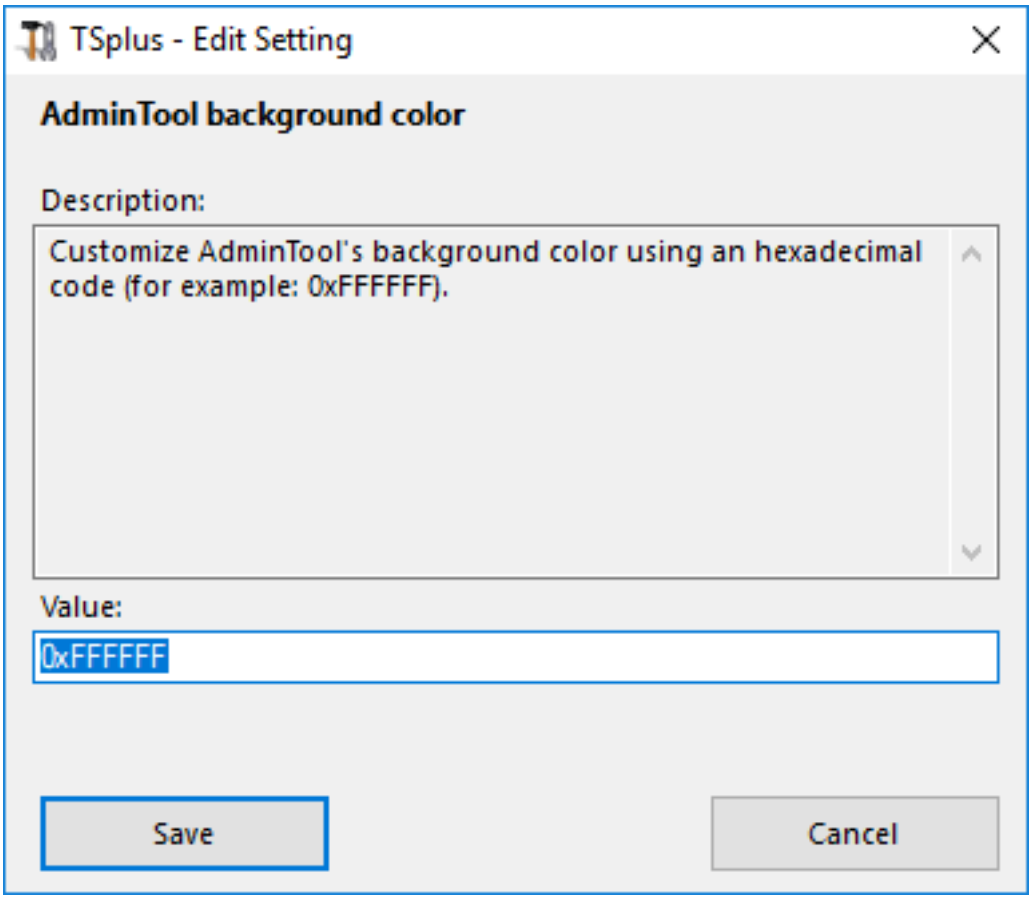
ADVERTENCIA cambiar de rol requiere reiniciar el sistema. Al seleccionar el Escritorio Remoto de Windows, solo se permitirá un usuario a la vez en un sistema de estación de trabajo.



Para usar el rol de RDS de Windows, seleccione el valor "Sí" y guarde.

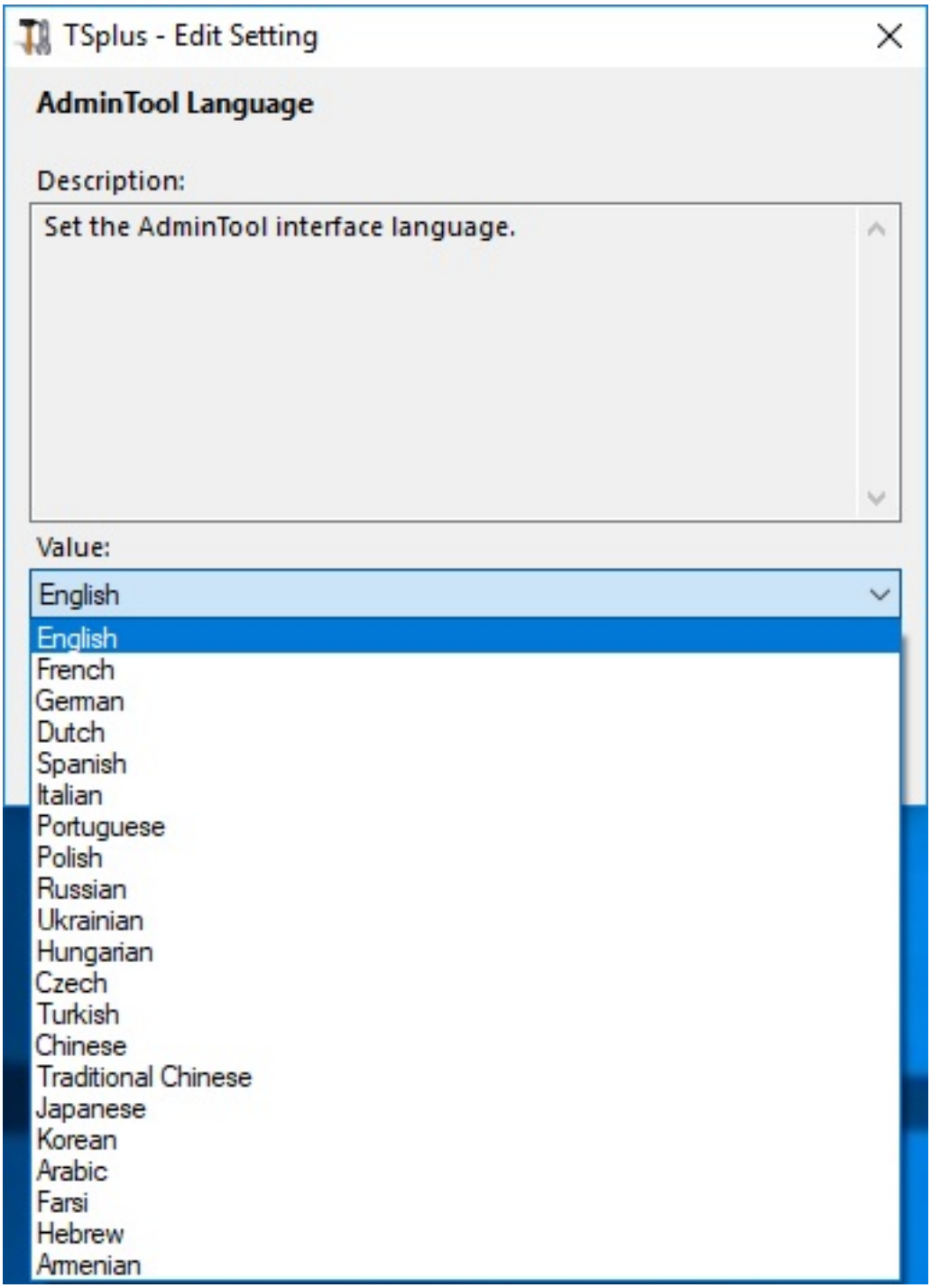
Modificar el color de fondo de AdminTool

Personaliza el color de fondo de AdminTool utilizando un código hexadecimal (por ejemplo: 0xFFFFFF).



Modificar el idioma de AdminTool

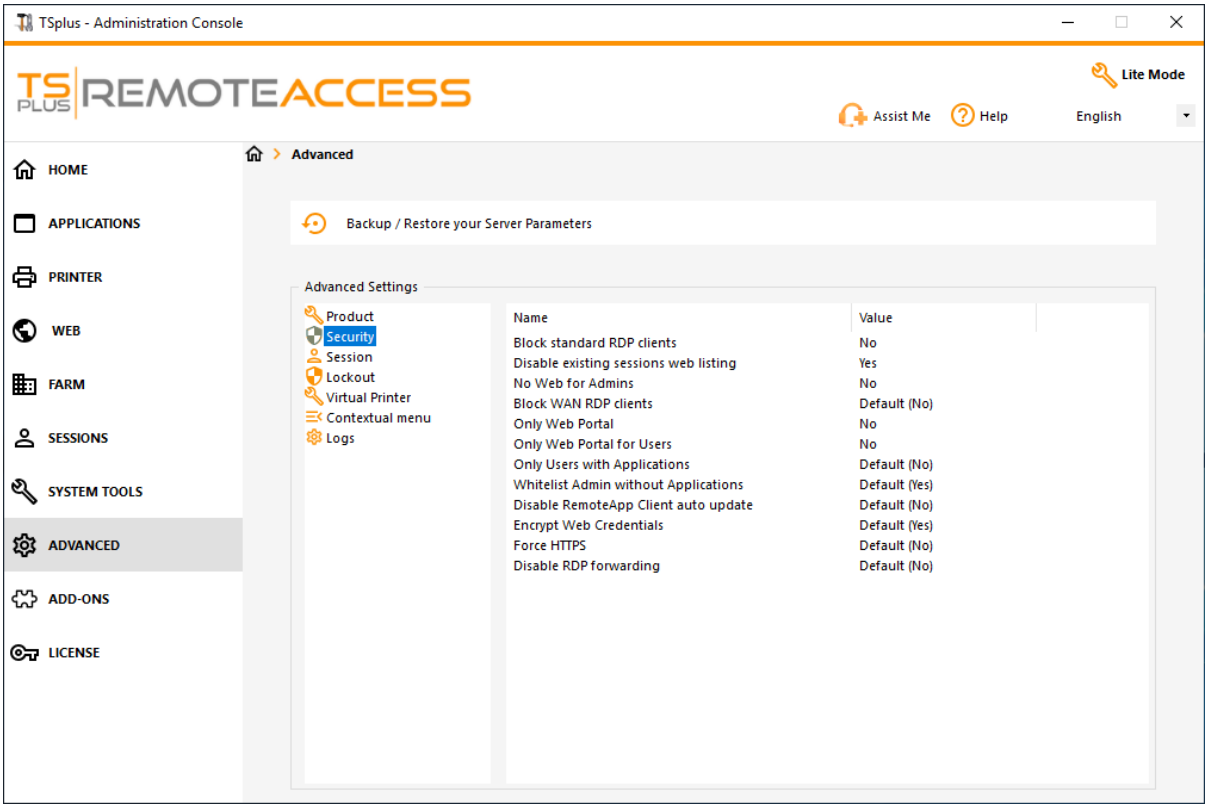
Seleccione su idioma preferido para el AdminTool entre los 21 disponibles.


TSplus - Edit Setting
AdminTool Language
Description:
Set the AdminTool interface language.
Value:
English
English
French
German
Dutch
Spanish
Italian
Portuguese
Polish
Russian
Ukrainian
Hungarian
Czech
Turkish
Chinese
Traditional Chinese
Japanese
Korean
Arabic
Farsi
Hebrew
Armenian

Funciones Avanzadas - Seguridad

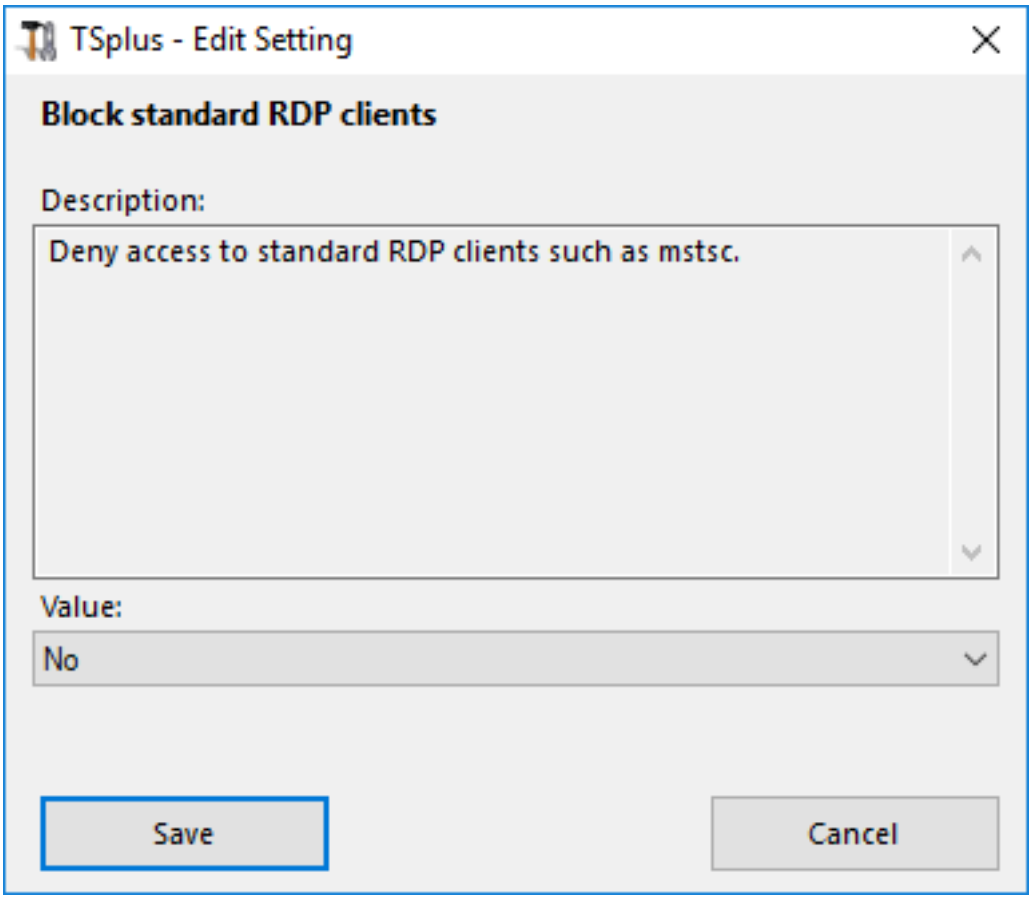
Resumen

En la sección de Seguridad de las funciones Avanzadas, puedes bloquear, deshabilitar o personalizar los tipos de conexión para los usuarios.



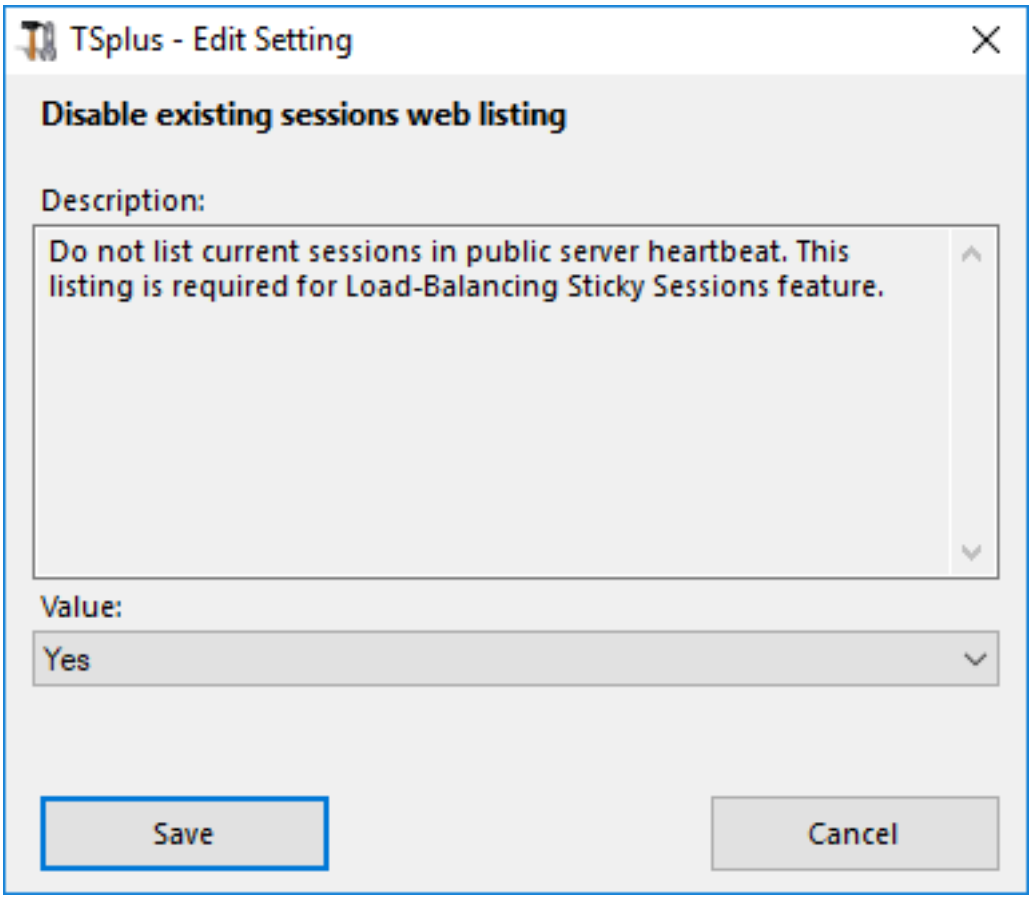
Bloquear clientes RDP estándar

Seleccione el valor "Sí" si desea denegar el acceso a los clientes RDP estándar como mstsc a sus usuarios.



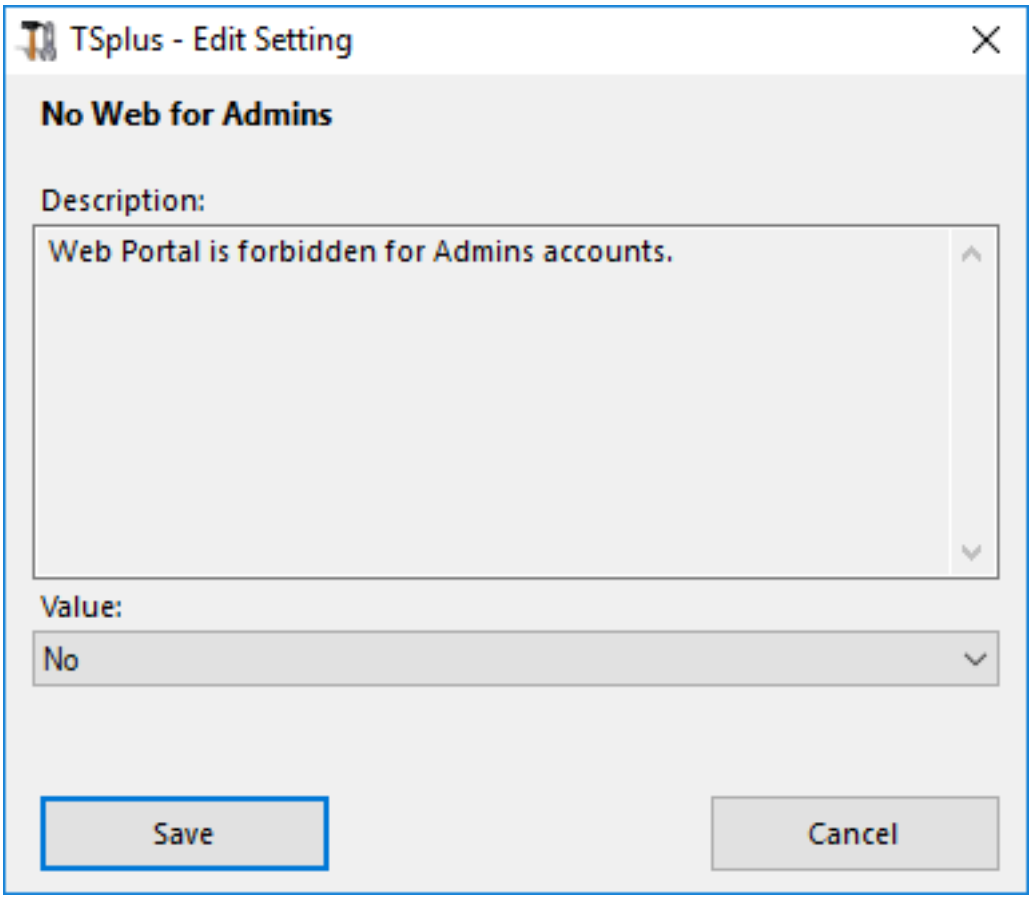
Deshabilitar la lista web de sesiones existentes

Esta lista es necesaria para la función de Sesiones Pegajosas de Balanceo de Carga y está habilitada por defecto. Si desea desactivarla, seleccione el valor "No" en esta ventana y luego haga clic en guardar:



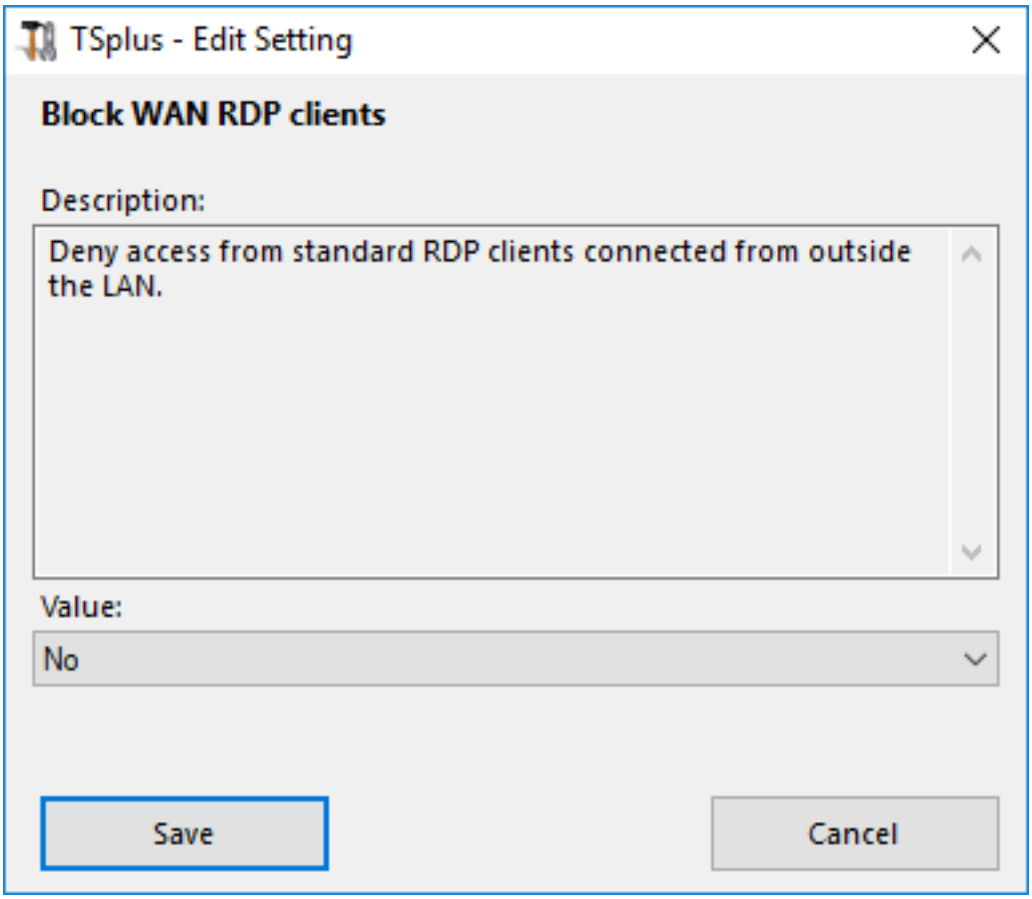
No Web para Administradores

Desactive el Portal Web para Administradores seleccionando el valor "Sí":



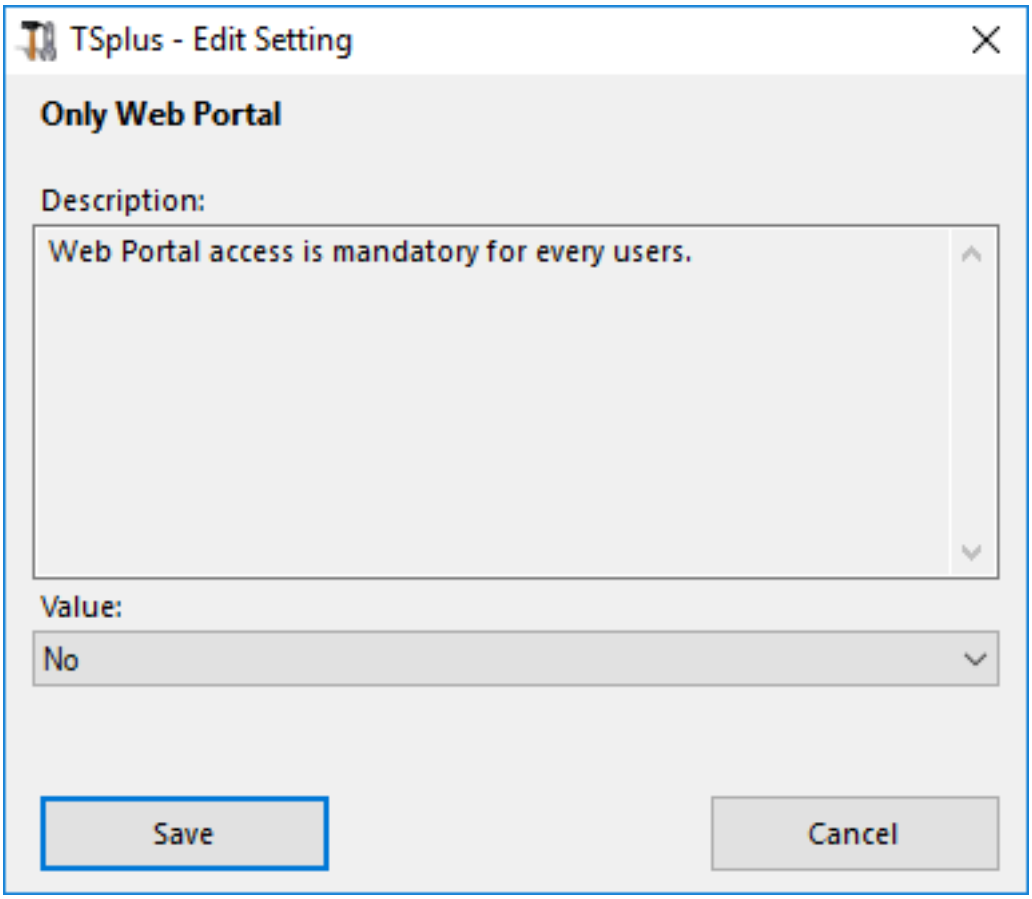
Bloquear clientes RDP WAN

Denegar el acceso desde clientes RDP estándar conectados desde fuera de la LAN seleccionando el valor "Sí".



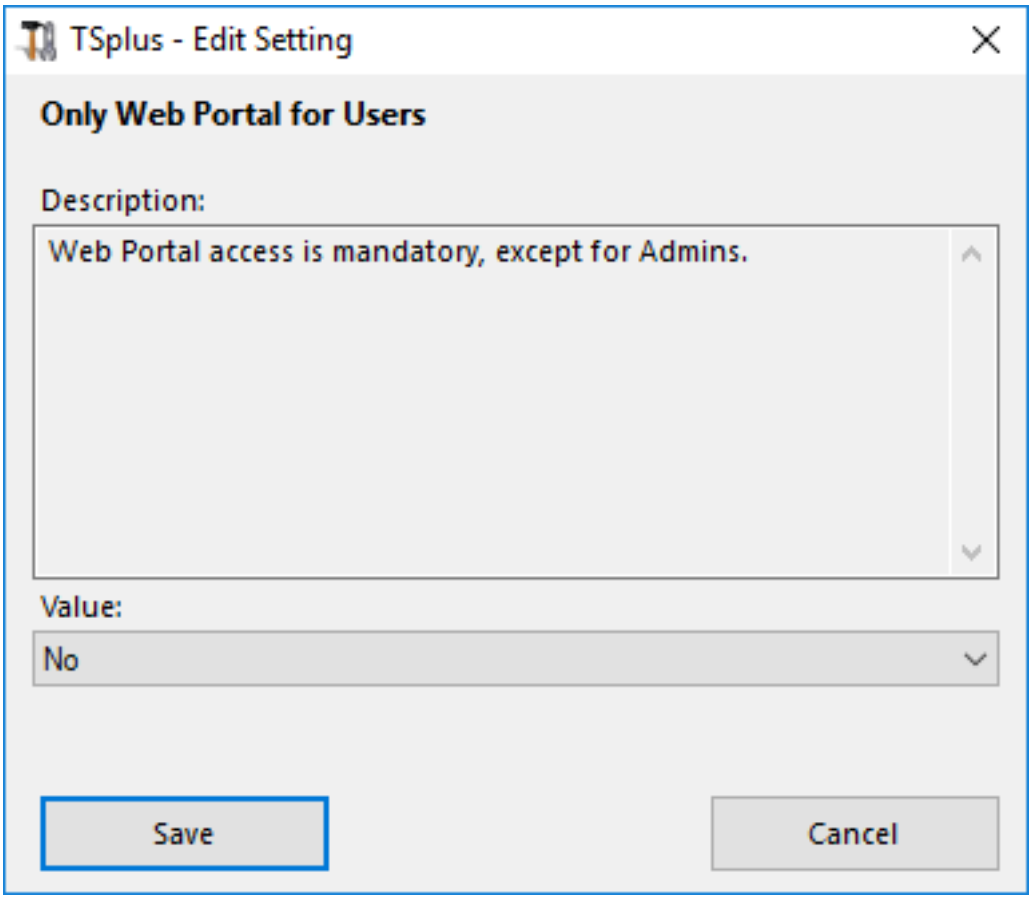
Solo Portal Web

Haga que el acceso al portal web sea obligatorio para cada usuario seleccionando el valor "sí".



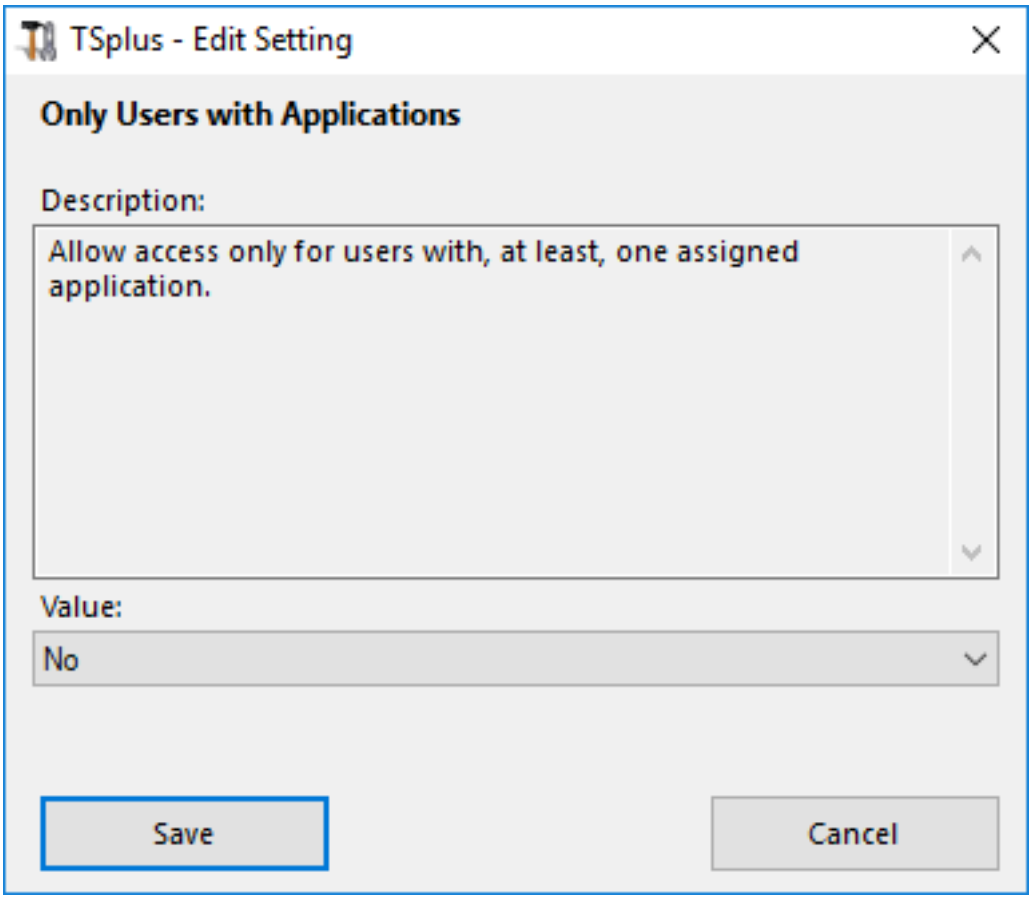
Solo Portal Web para Usuarios

Hacer que el acceso al Portal Web sea obligatorio para cada usuario, excepto los administradores, seleccionando el valor "sí".



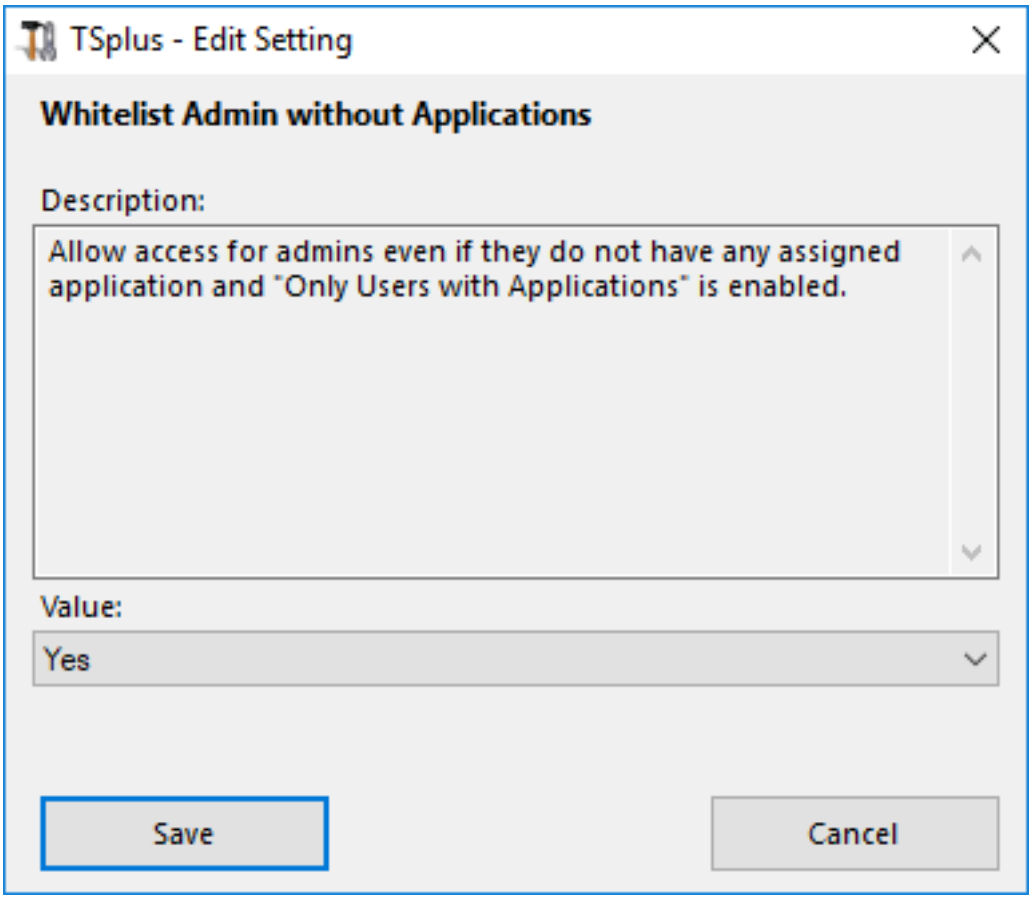
Solo usuarios con aplicaciones

Permitir acceso solo a usuarios con al menos una aplicación asignada seleccionando el valor "sí".



Administradores en la lista blanca sin aplicaciones

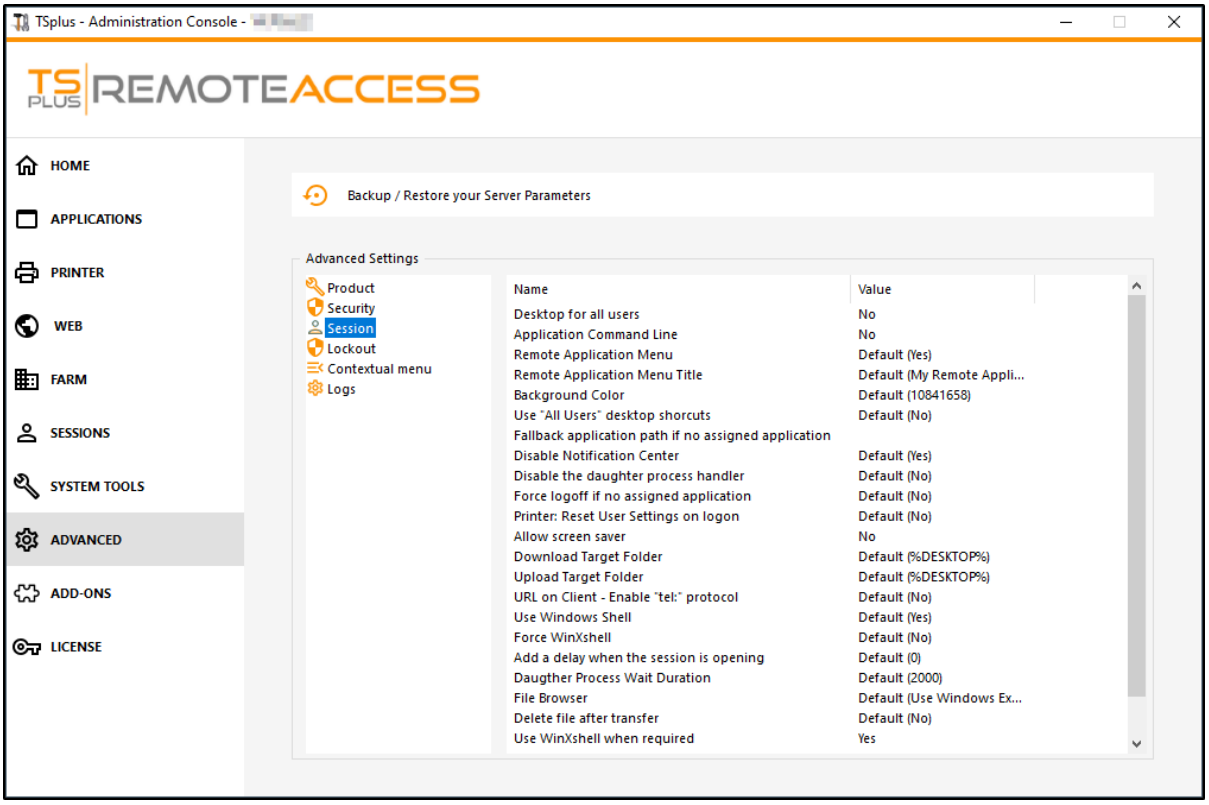
Permitir acceso a los administradores incluso si no tienen ninguna aplicación asignada y "Solo usuarios con aplicaciones" está habilitado. Esta función está habilitada por defecto. Si desea desactivarla, seleccione el valor "No" en esta ventana y luego haga clic en guardar:


TSplus - Edit Setting
Whitelist Admin without Applications
Description:
Allow access for admins even if they do not have any assigned application and "Only Users with Applications" is enabled.
Value:
Yes
Save
Cancel

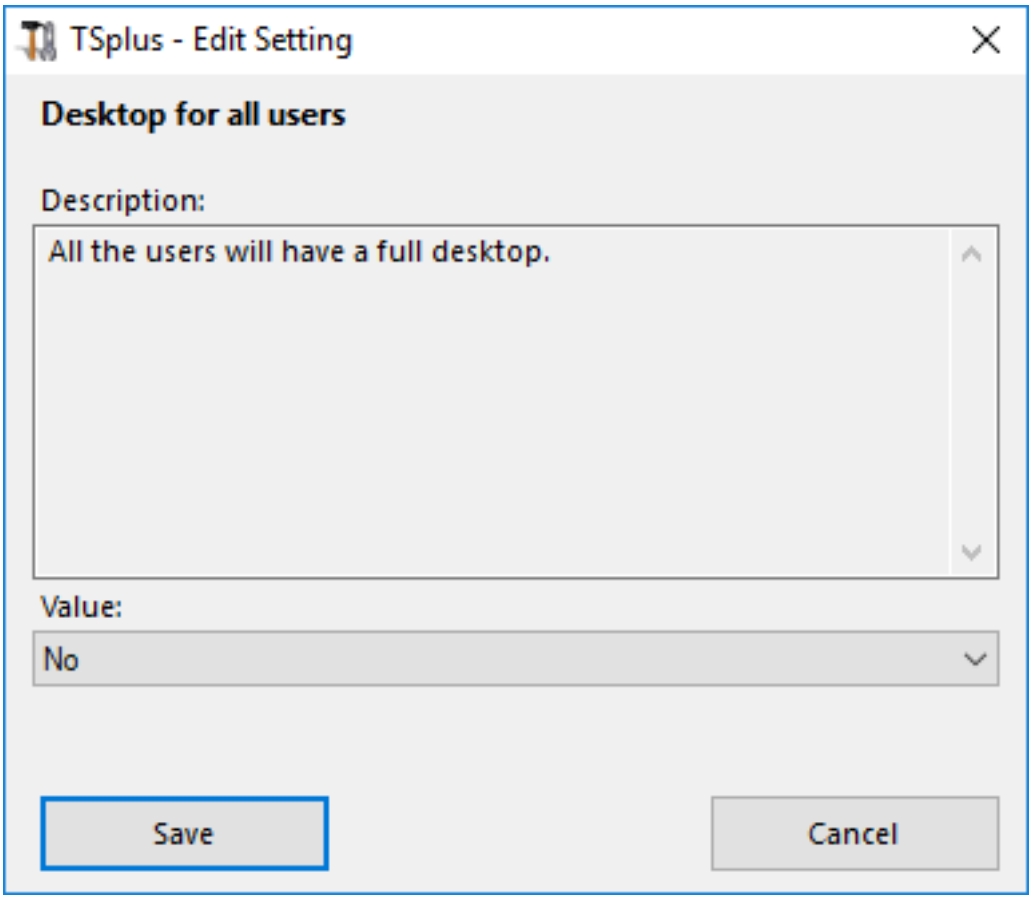
Funciones Avanzadas - Sesión

Resumen

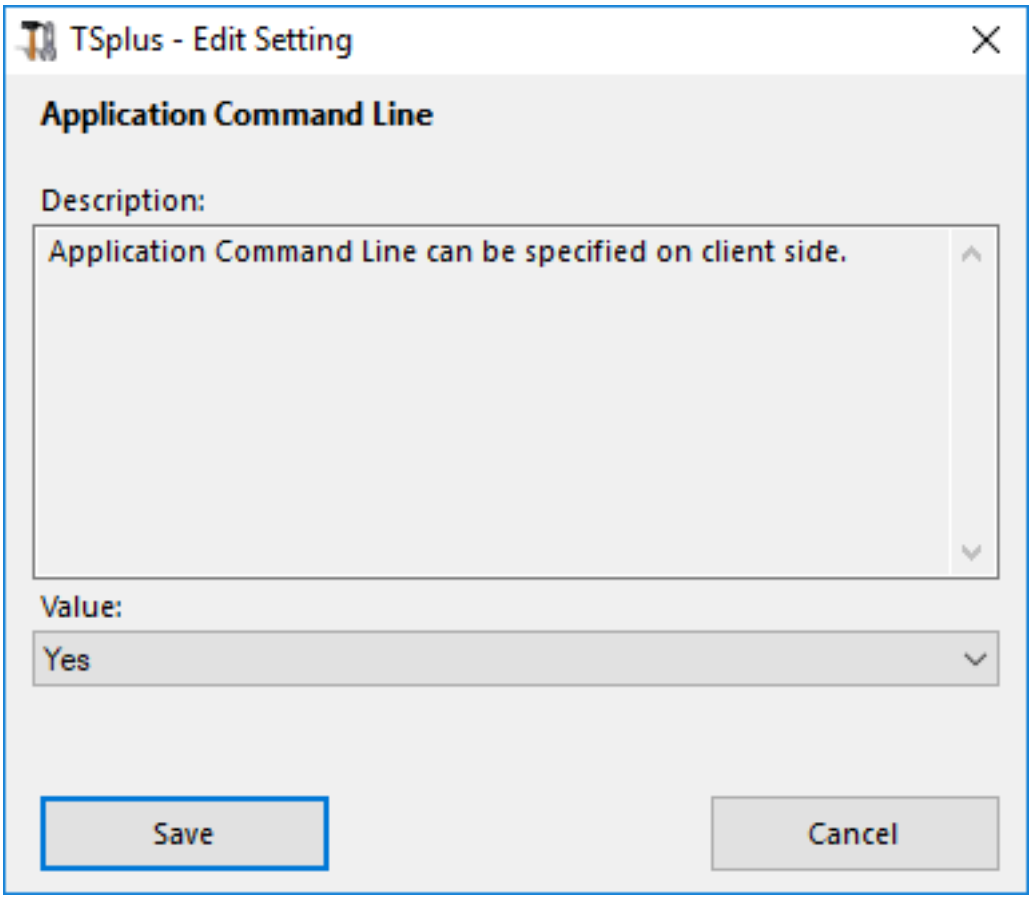
Esta sección de la pestaña Avanzado permite configurar los derechos de usuario y aspectos en sus sesiones.



Habilite un escritorio completo para todos los usuarios seleccionando el valor "Sí" en esta ventana, luego haga clic en guardar:

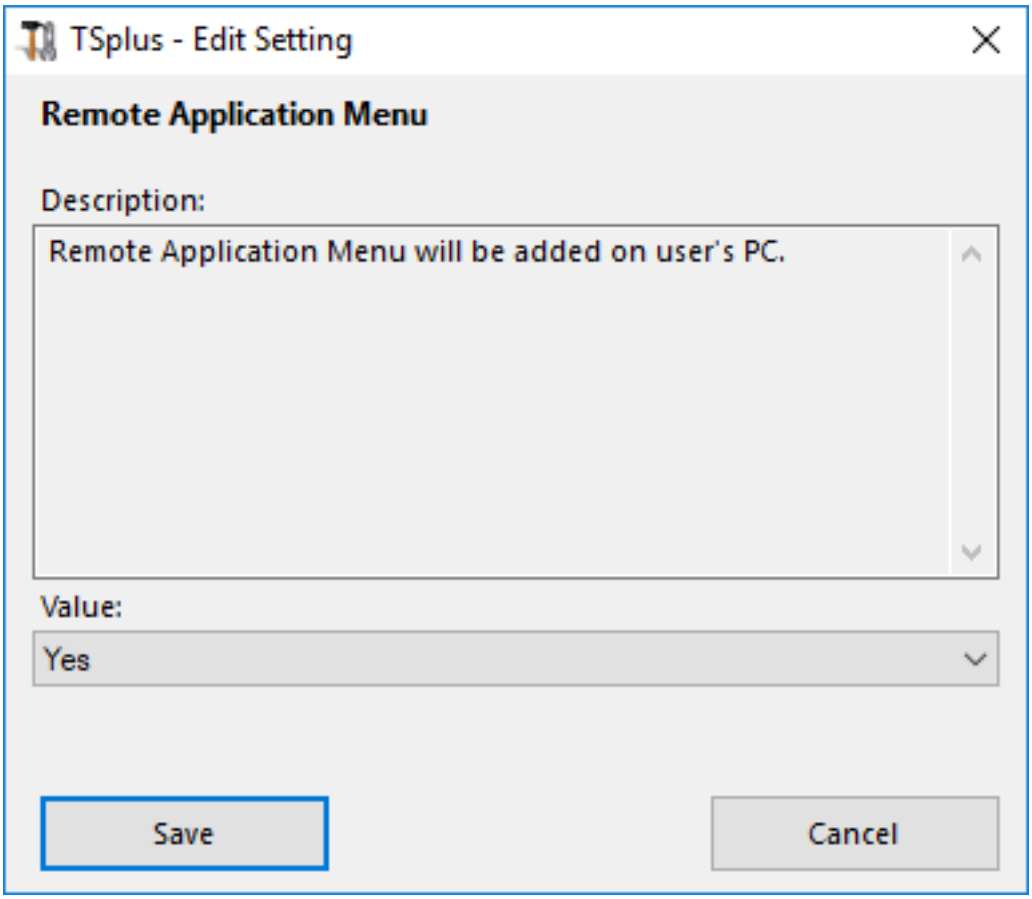


La línea de comandos de la aplicación se puede especificar en el lado del cliente. Esta función está habilitada por defecto. Si desea desactivarla, seleccione el valor "No" en esta ventana y luego haga clic en guardar:



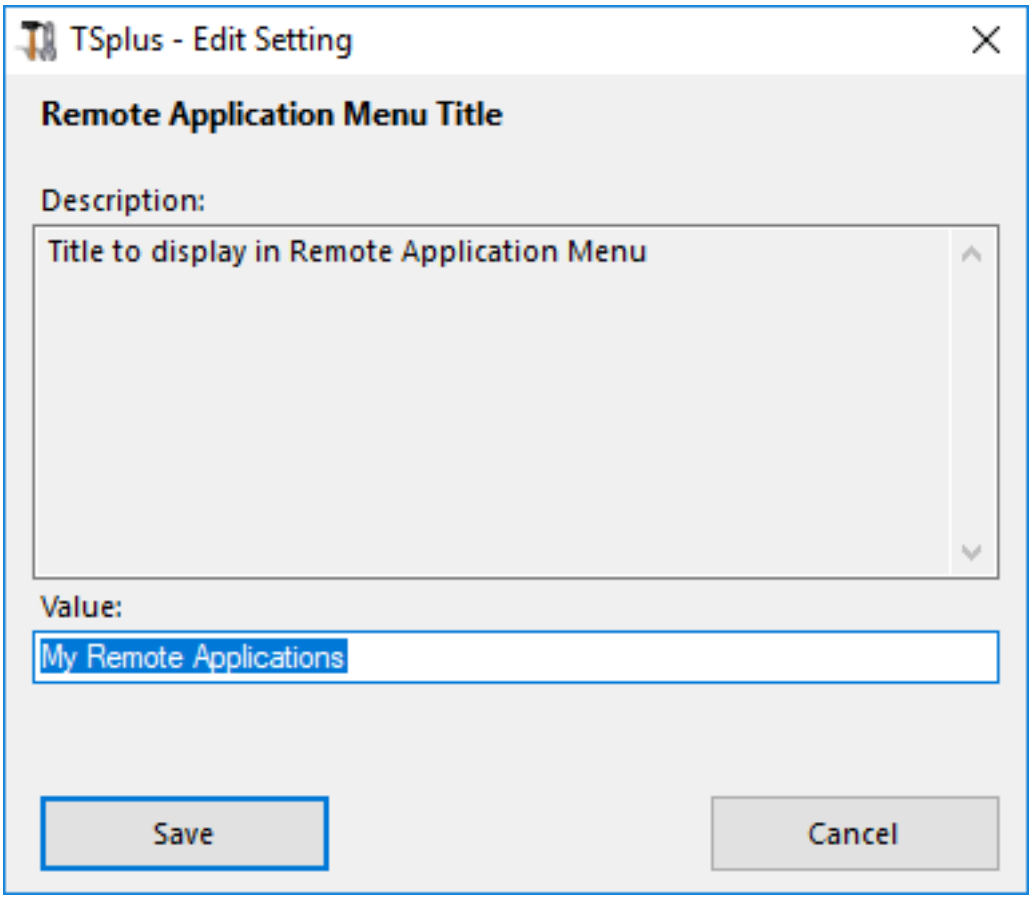
Menú de Aplicaciones Remotas

El menú de aplicación remota se añadirá en el PC del usuario. Esta función está habilitada por defecto. Si desea desactivarla, seleccione el valor "No" en esta ventana y luego haga clic en guardar.



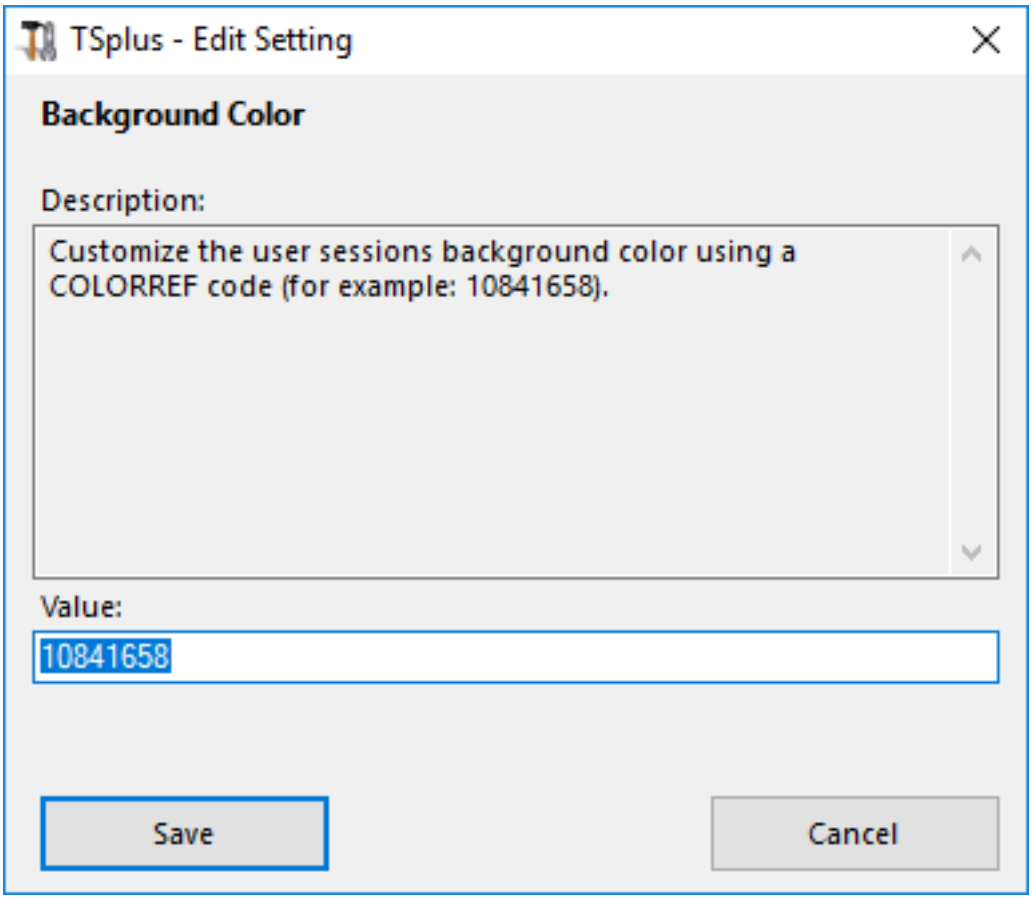
Título del Menú de Aplicaciones Remotas

Puedes modificar el título del Menú de Aplicaciones Remotas. El predeterminado es "Mis Aplicaciones Remotas". Si deseas modificarlo, ingresa el título deseado y luego haz clic en guardar:



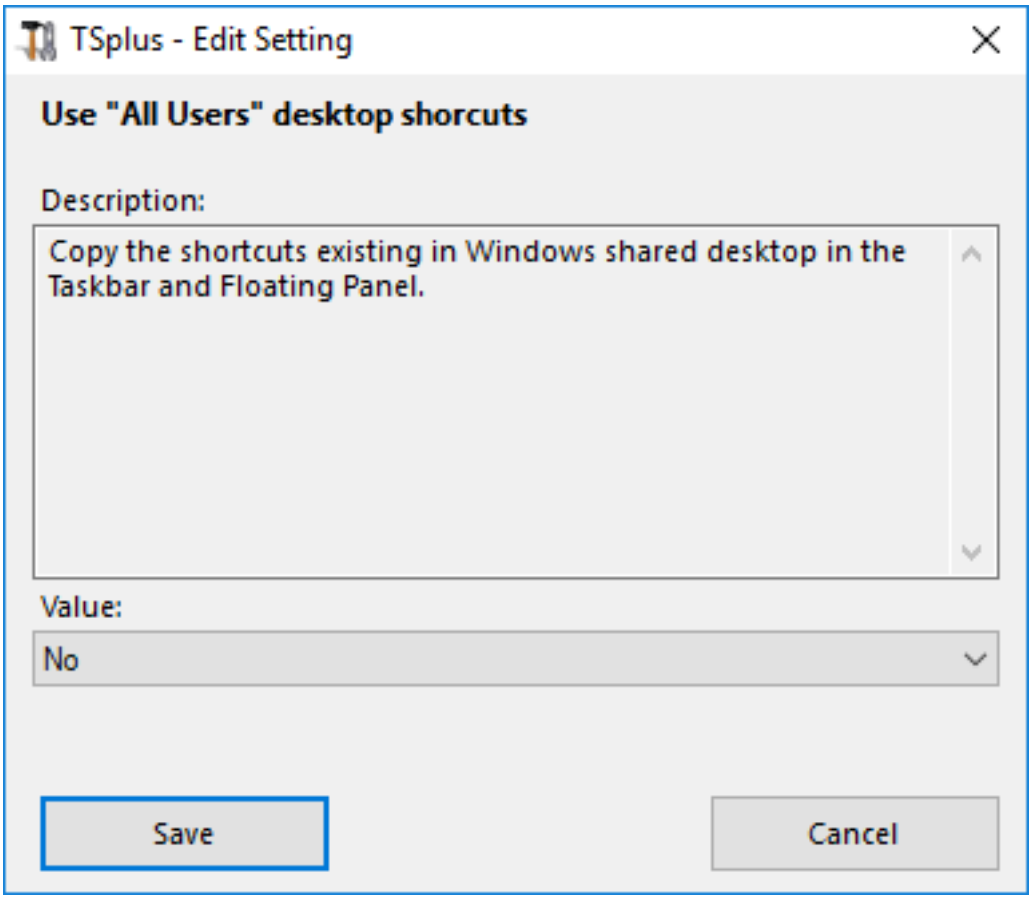
Color de fondo

Personaliza el color de fondo de las sesiones de usuario utilizando un código COLORREF (por ejemplo, el predeterminado es: 10841658).



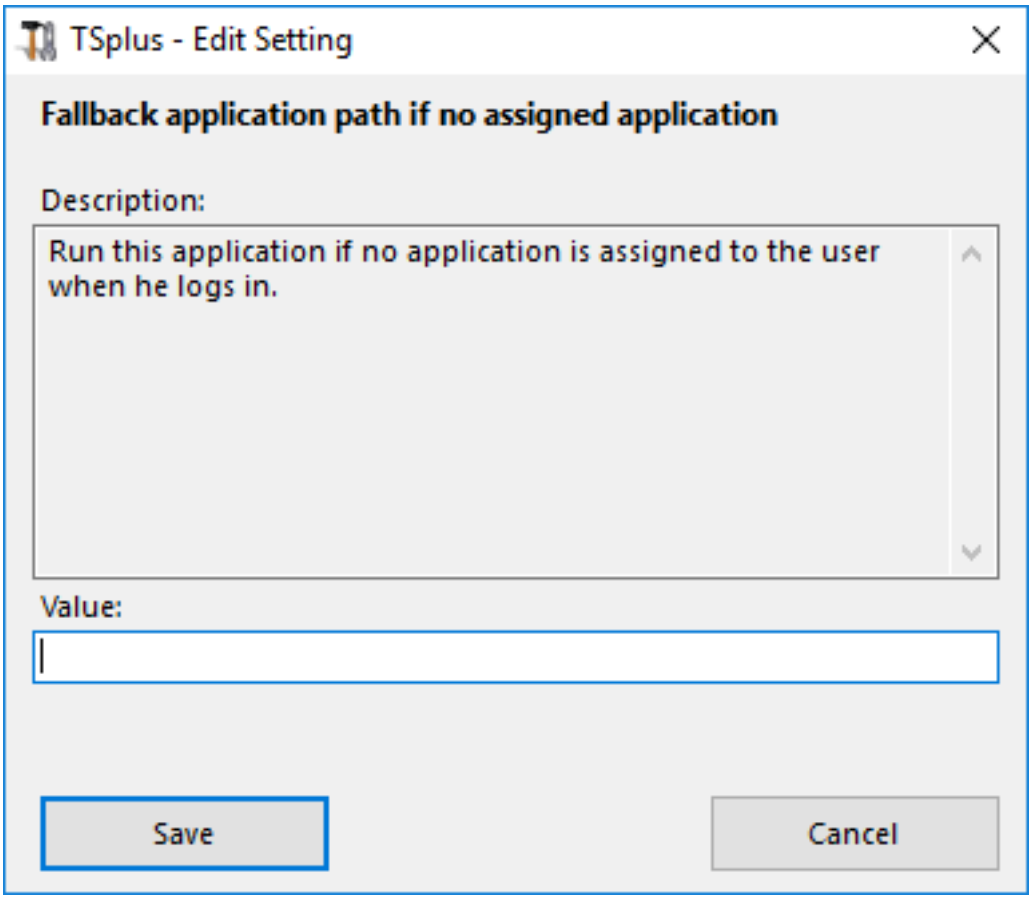
Usar accesos directos de escritorio "Todos los usuarios"

Copia los accesos directos existentes en el escritorio compartido de Windows en la barra de tareas y el panel flotante. Habilita esta función seleccionando el valor "Sí" en esta ventana, luego haz clic en guardar:



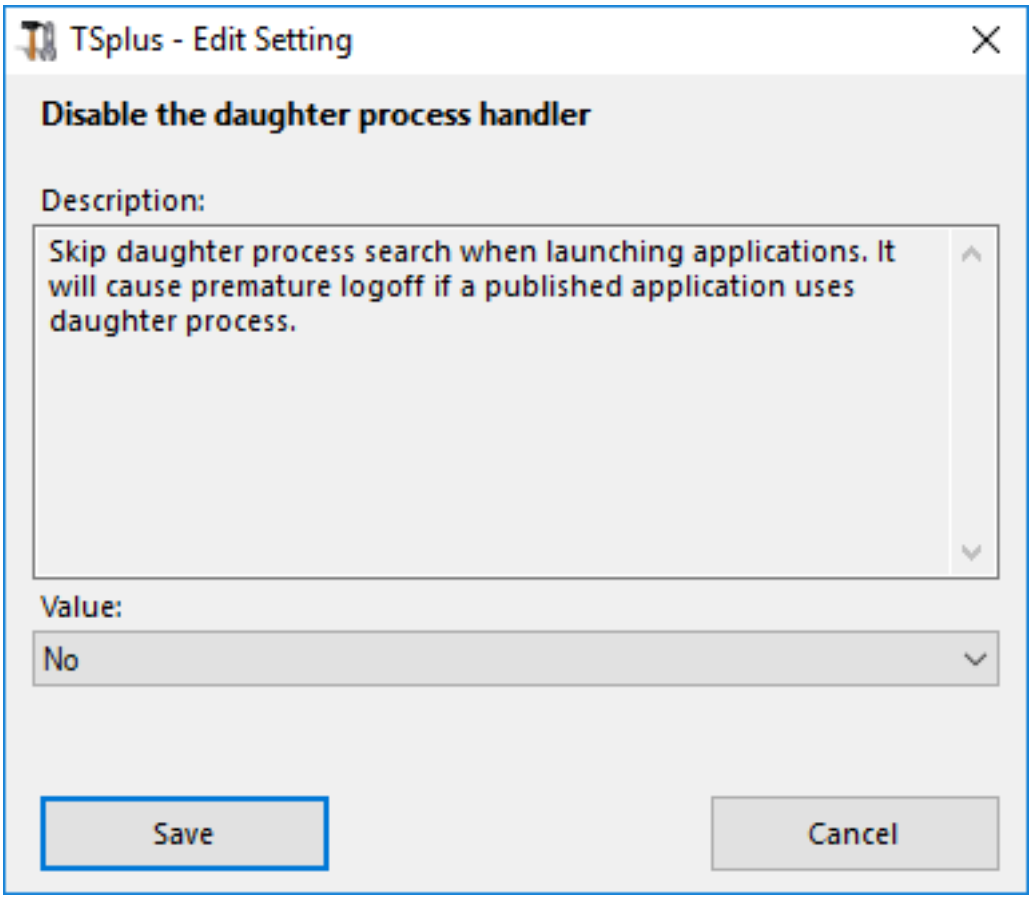
Ruta de la aplicación de respaldo si no hay una aplicación asignada

Ejecute esta aplicación si no se asigna ninguna aplicación al usuario cuando inicia sesión. No hay valor por defecto. Habilite esta función ingresando un valor de "Sí" en esta ventana, luego haga clic en guardar:



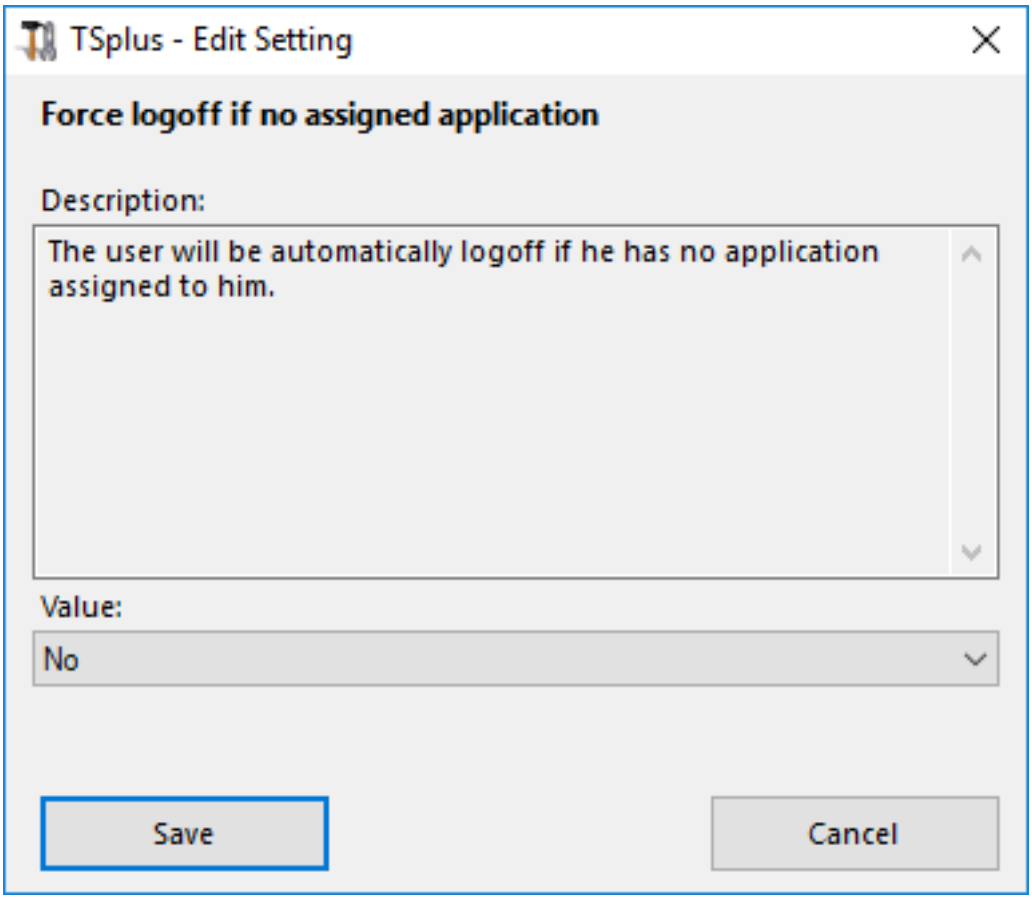
Deshabilitar el controlador de procesos hijo

Omitir la búsqueda de procesos secundarios al iniciar aplicaciones. Esto causará un cierre de sesión prematuro si una aplicación publicada utiliza un proceso secundario. Esta función está deshabilitada por defecto. Habilite esta función seleccionando el valor "Sí" en esta ventana, luego haga clic en guardar.



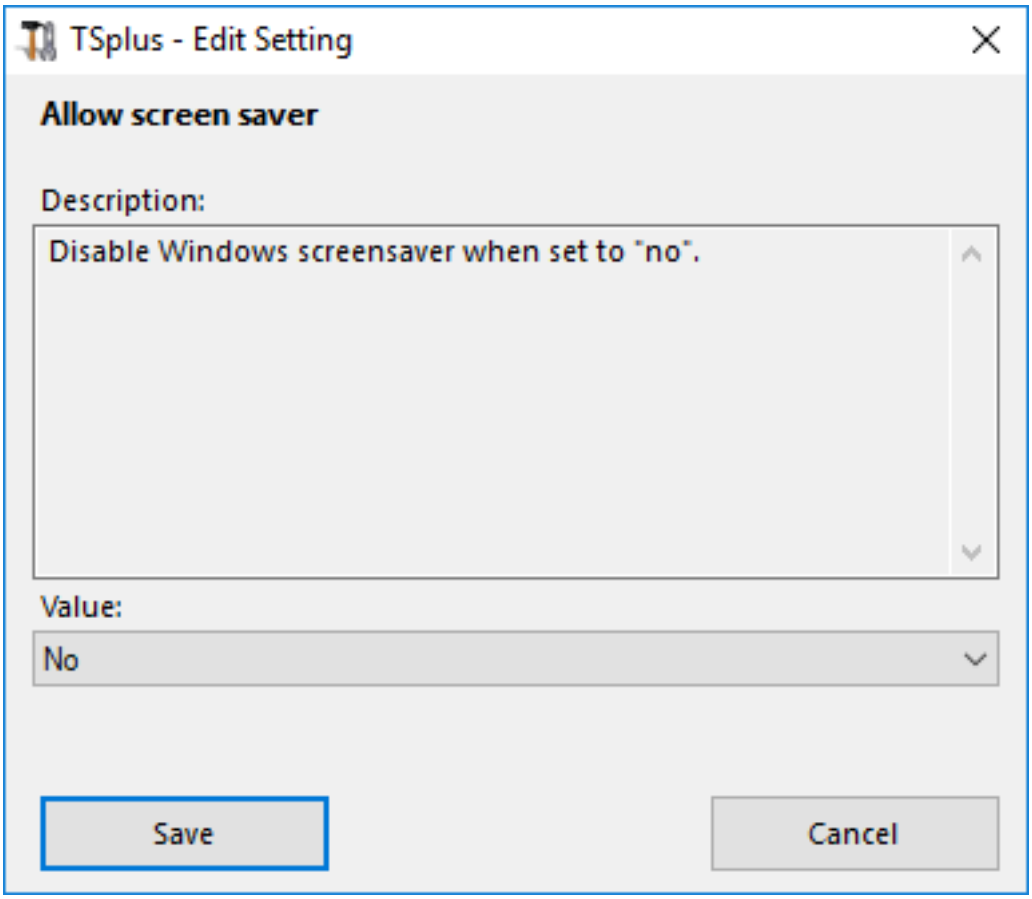
Forzar cierre de sesión si no hay aplicación asignada

El usuario se desconectará automáticamente si no tiene ninguna aplicación asignada. Esta función está desactivada por defecto. Habilite esta función seleccionando el valor "Sí" en esta ventana, luego haga clic en guardar.



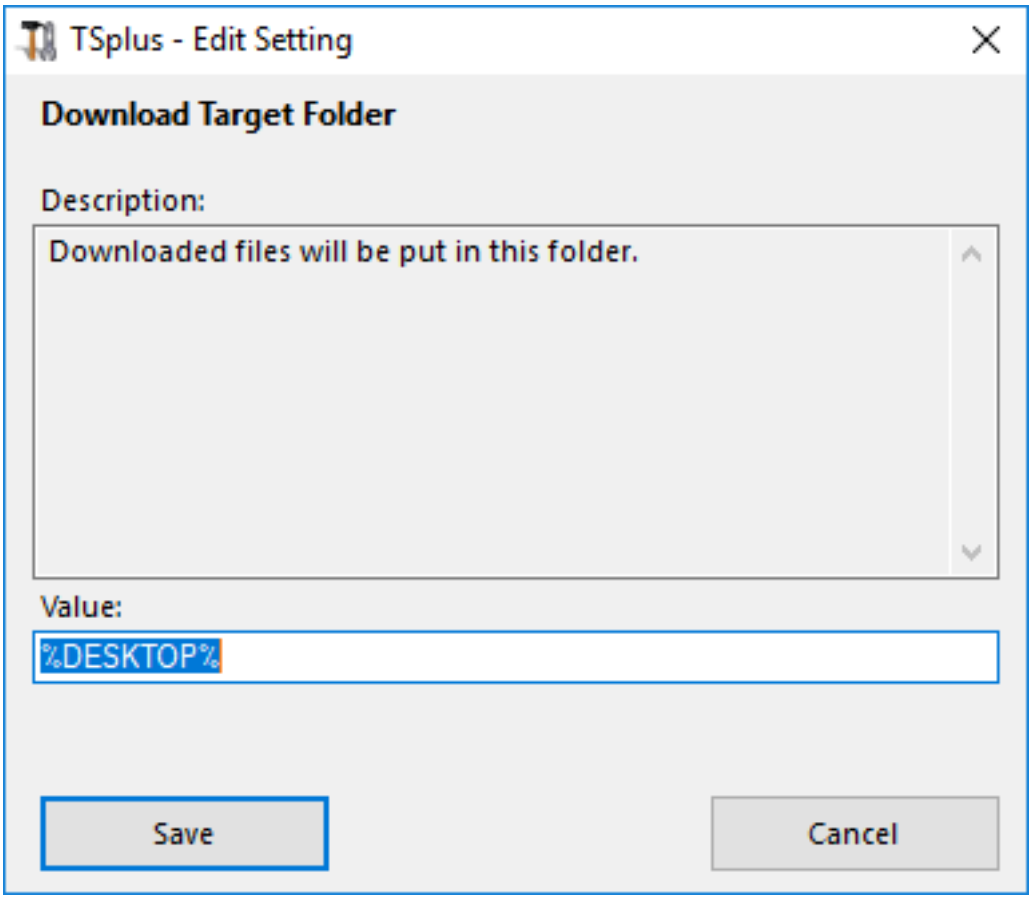
Permitir protector de pantalla

Esta función está deshabilitada por defecto. Habilite el protector de pantalla de Windows seleccionando el valor "Sí" en esta ventana, luego haga clic en guardar:



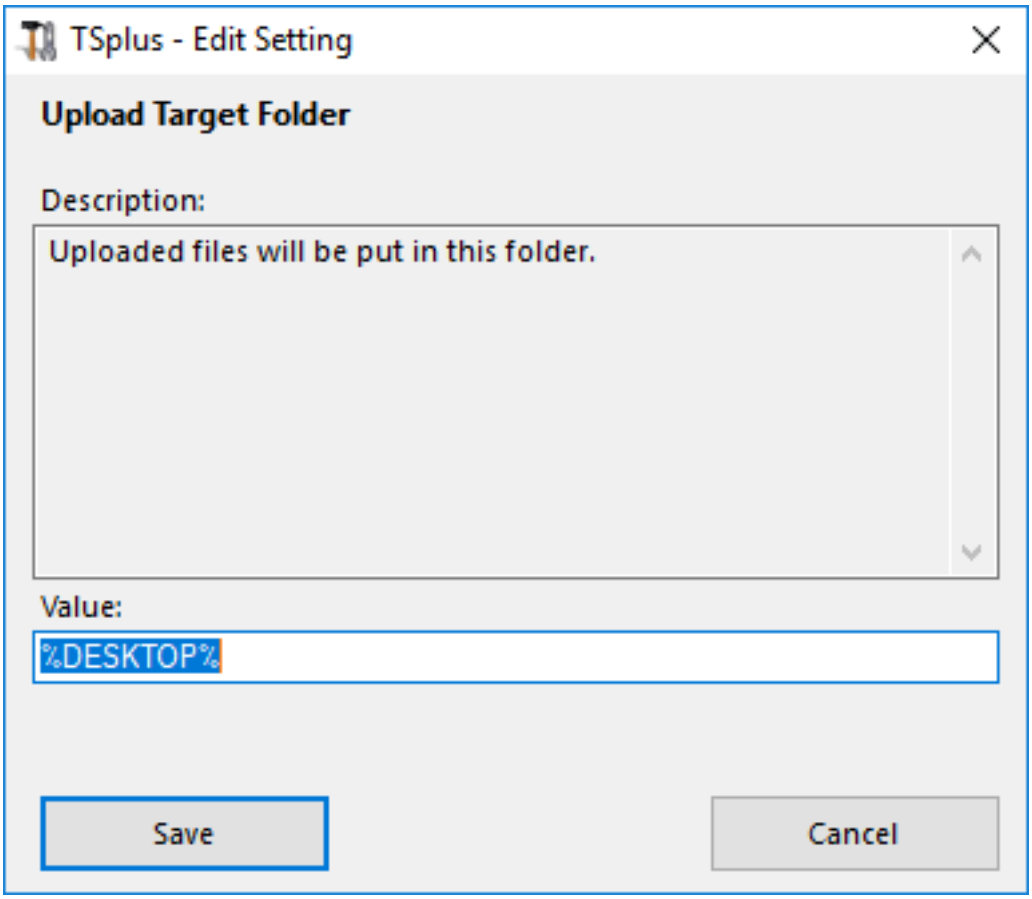
Descargar carpeta de destino

Los archivos descargados se guardarán en el Escritorio por defecto. Si desea modificarlo, ingrese la ruta de la carpeta de descarga deseada y luego haga clic en guardar.



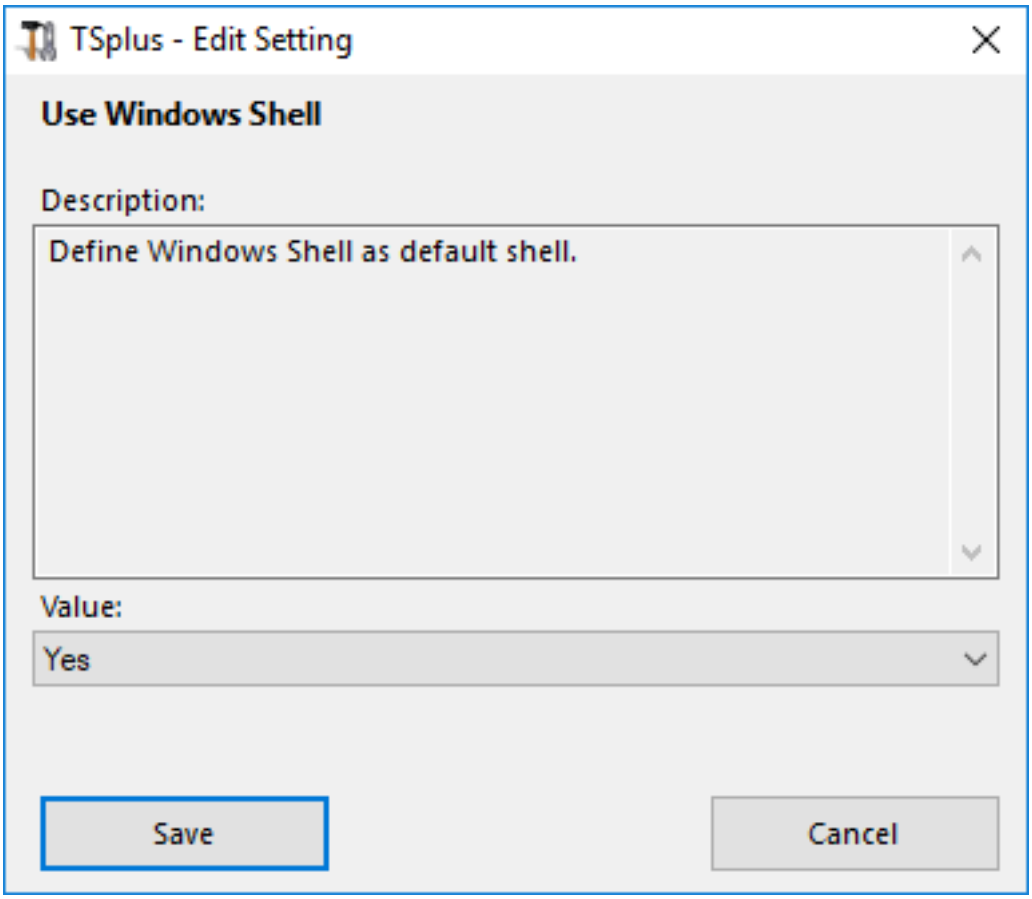
Subir carpeta de destino

Los archivos subidos se colocarán en esta carpeta. Si desea modificarla, ingrese la ruta de la carpeta de carga deseada y luego haga clic en guardar:



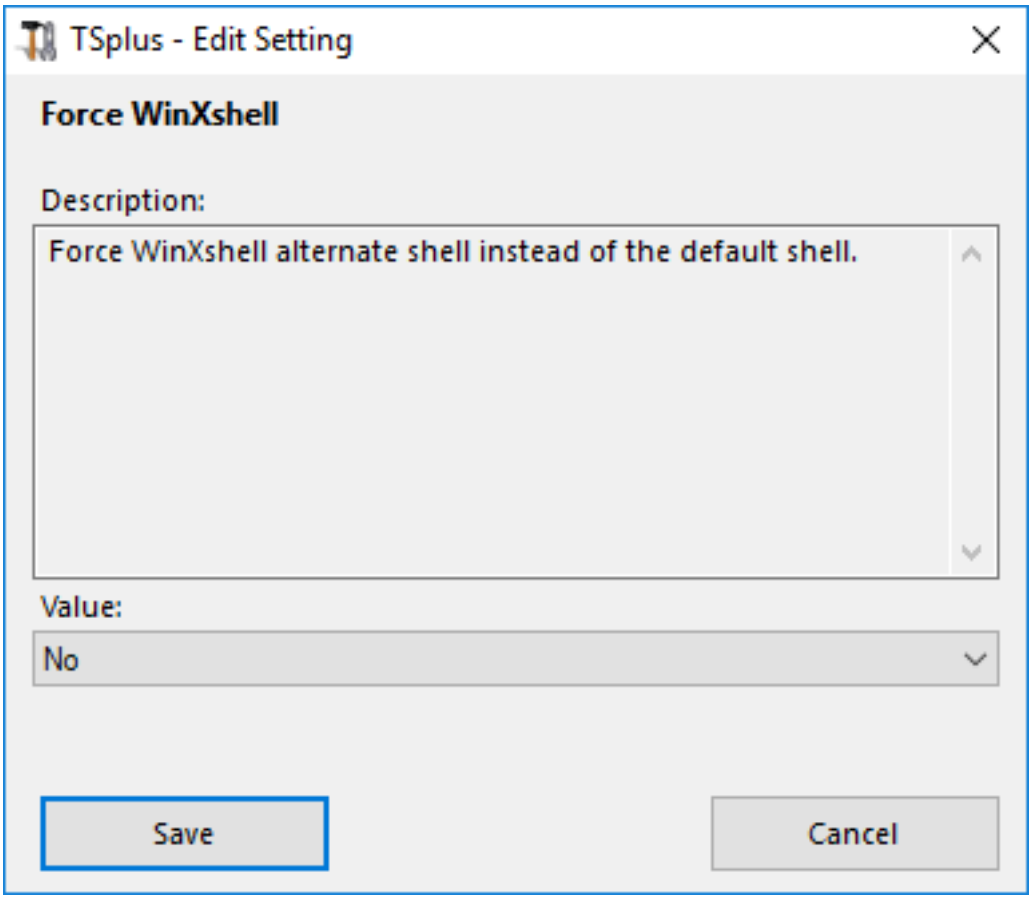
Usar Windows Shell

Defina Windows Shell como shell predeterminado. Esta función está habilitada por defecto. Si desea desactivarla, seleccione el valor "No" en esta ventana, luego haga clic en guardar:



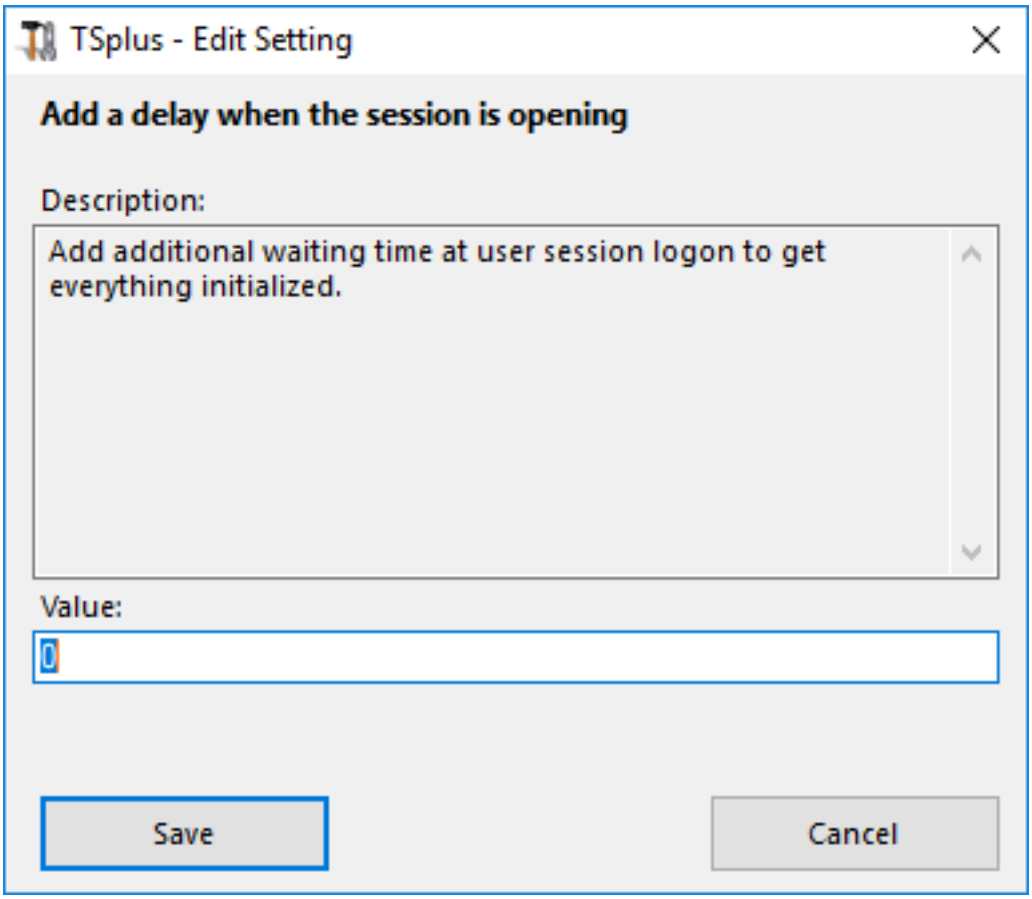
Forzar WinXshell

Esta función está deshabilitada por defecto. Fuerza el shell alternativo WinXshell en lugar del shell predeterminado seleccionando el valor "Sí" en esta ventana, luego haz clic en guardar:



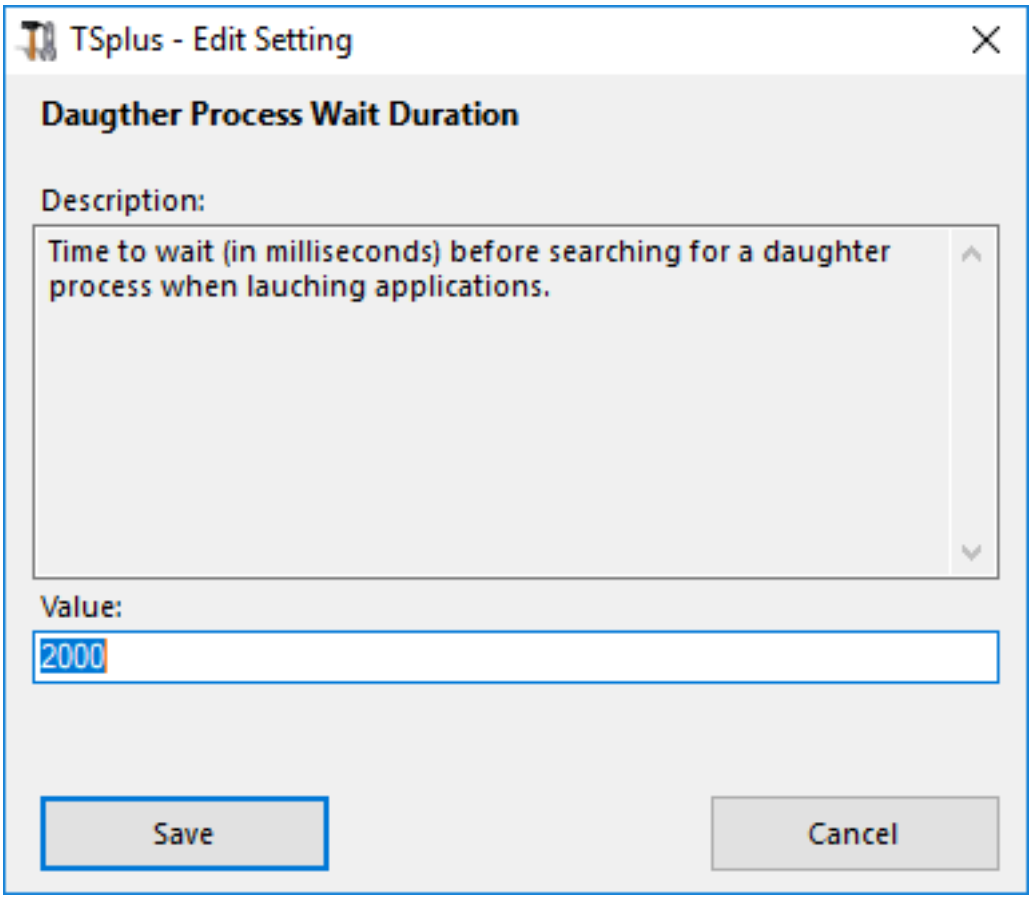
Agregue un retraso al abrir la sesión

Agregue tiempo de espera adicional en el inicio de sesión de la sesión de usuario para que todo se inicialice. El valor predeterminado es 0. Si desea modificarlo, ingrese el valor deseado (en segundos) y luego haga clic en guardar:



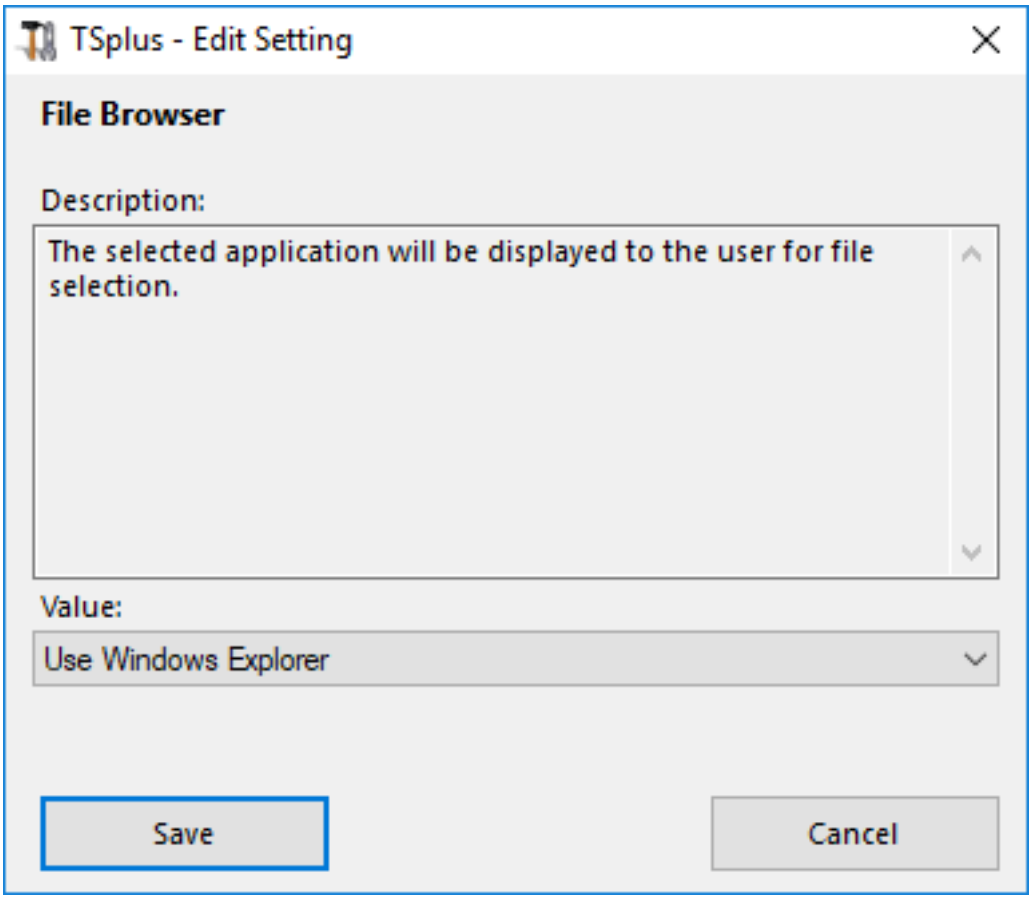
Duración de espera del proceso hijo

Tiempo de espera (en milisegundos) antes de buscar un proceso hijo al iniciar aplicaciones.



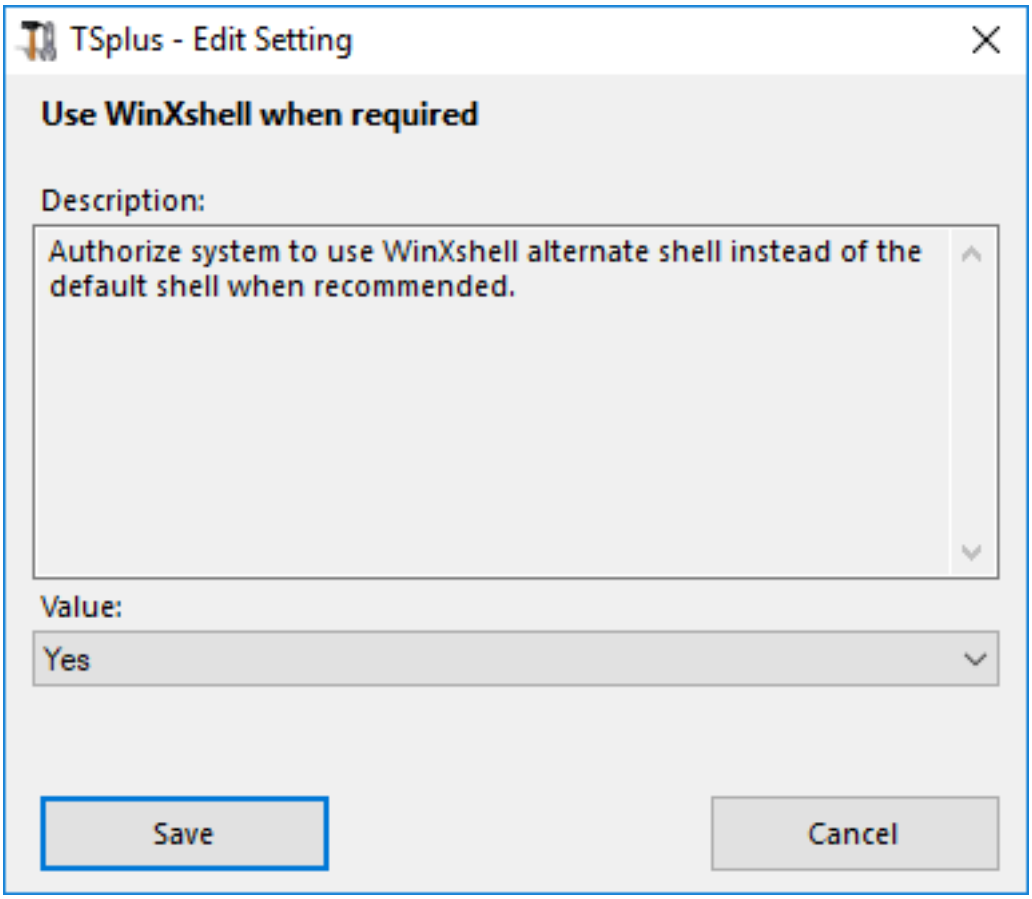
Explorador de archivos

La aplicación seleccionada se mostrará al usuario para la selección de archivos. El navegador predeterminado es el Explorador de Windows. Puede utilizar el navegador de archivos de TSplus seleccionándolo y luego hacer clic en guardar:



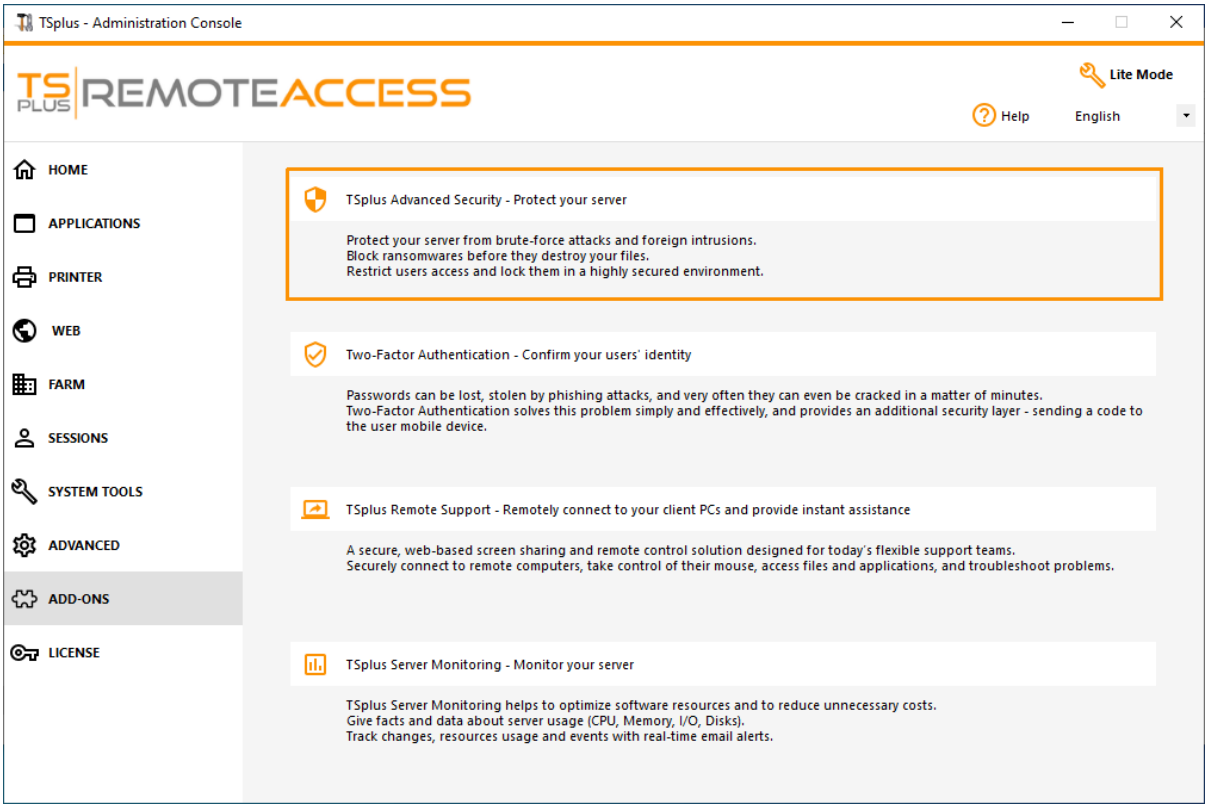
Usa WinXshell cuando sea necesario

Autorizar al sistema para usar el shell alternativo WinXshell en lugar del shell predeterminado cuando se recomiende. Esta función está habilitada por defecto. Si desea desactivarla, seleccione el valor "No" en esta ventana y luego haga clic en guardar:


TSplus - Edit Setting
Use WinXshell when required
Description:
Authorize system to use WinXshell alternate shell instead of the default shell when recommended.
Value:
Yes
Save
Cancel

TSplus Advanced Security

TSplus Advanced Security está disponible como un complemento desde TSplus AdminTool y está disponible en la pestaña de complementos:

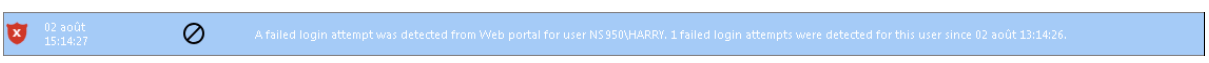


Puedes encontrar su documentación completa en esta página .

Evento de bloqueo

TSplus Lockout monitorea los intentos de inicio de sesión web fallidos en su servidor TSplus.

TSplus Advanced Security mostrará un Evento de Bloqueo, después de cualquier intento fallido en el Portal Web como el ejemplo a continuación:



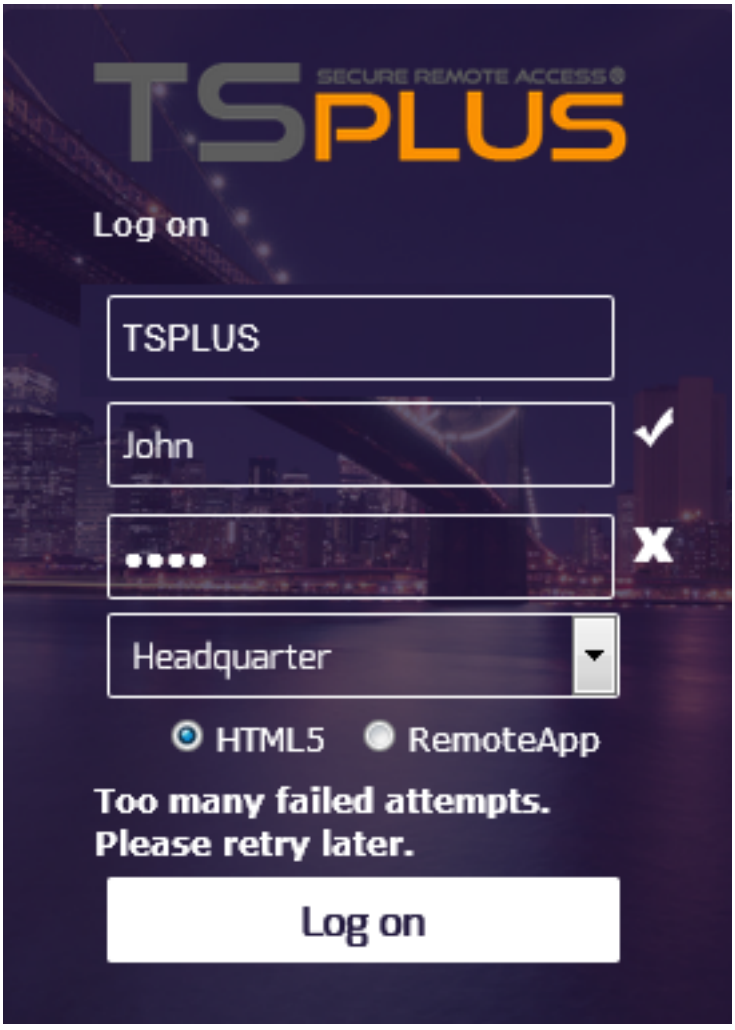
Se detectó un intento de inicio de sesión fallido desde el Portal Web para el usuario … Se detectó 1 intento de inicio de sesión fallido para este usuario desde…

La Protección contra Fuerza Bruta le permite proteger su servidor público de hackers, escáneres de red y robots de fuerza bruta que intentan adivinar su inicio de sesión y contraseña de Administrador. Utilizando inicios de sesión actuales y diccionarios de contraseñas, intentarán automáticamente iniciar sesión en su servidor cientos a miles de veces cada minuto. Obtenga más información sobre esta función en esta página .

En el Portal Web

Los ataques de fuerza bruta en el Portal Web se bloquean cuando los usuarios ingresan credenciales incorrectas.

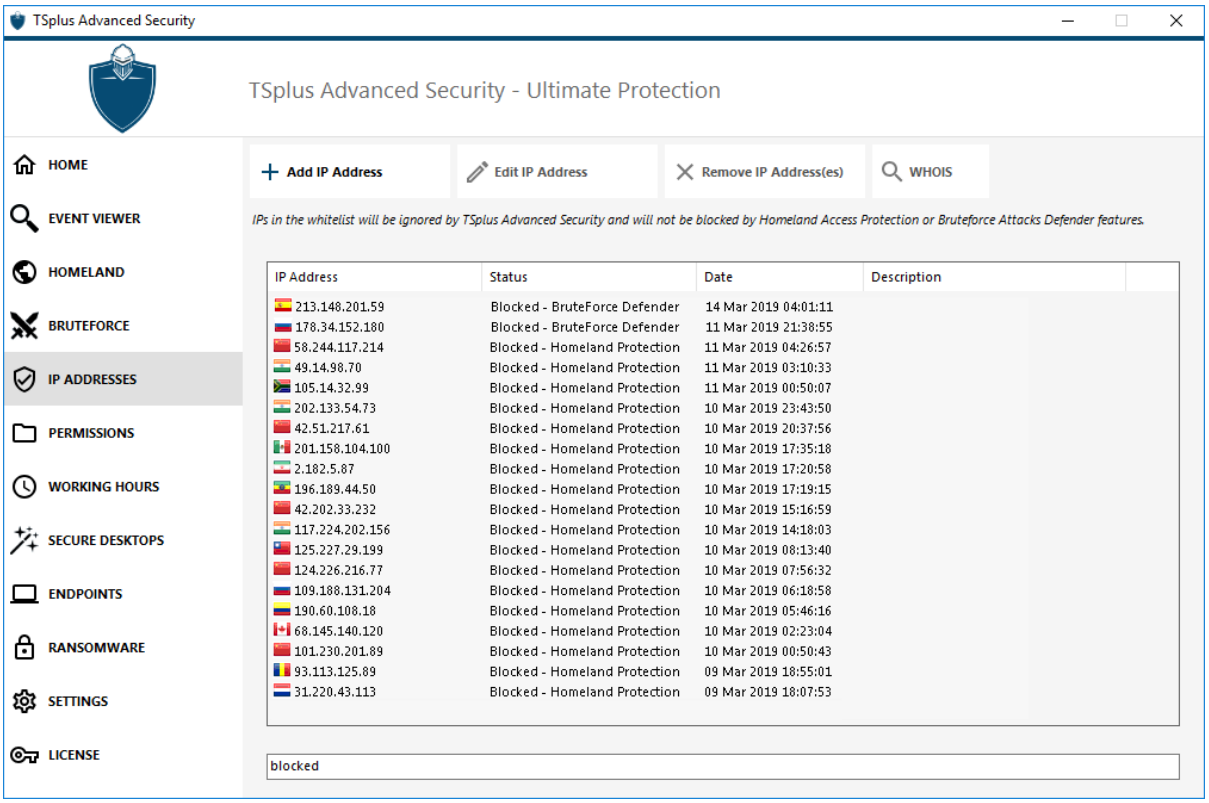
Después de 10 intentos durante un período de 10 minutos, el Portal Web prohibirá al usuario iniciar sesión durante 20 minutos.



Estas son las configuraciones predeterminadas que son personalizables en el Pestaña de

Protección contra Fuerza Bruta de TSplus Advanced Security AdminTool.

Puedes verificar todas las conexiones bloqueadas y los registros en el mosaico de Direcciones IP de TSplus Advanced Security Ultimate Protection:



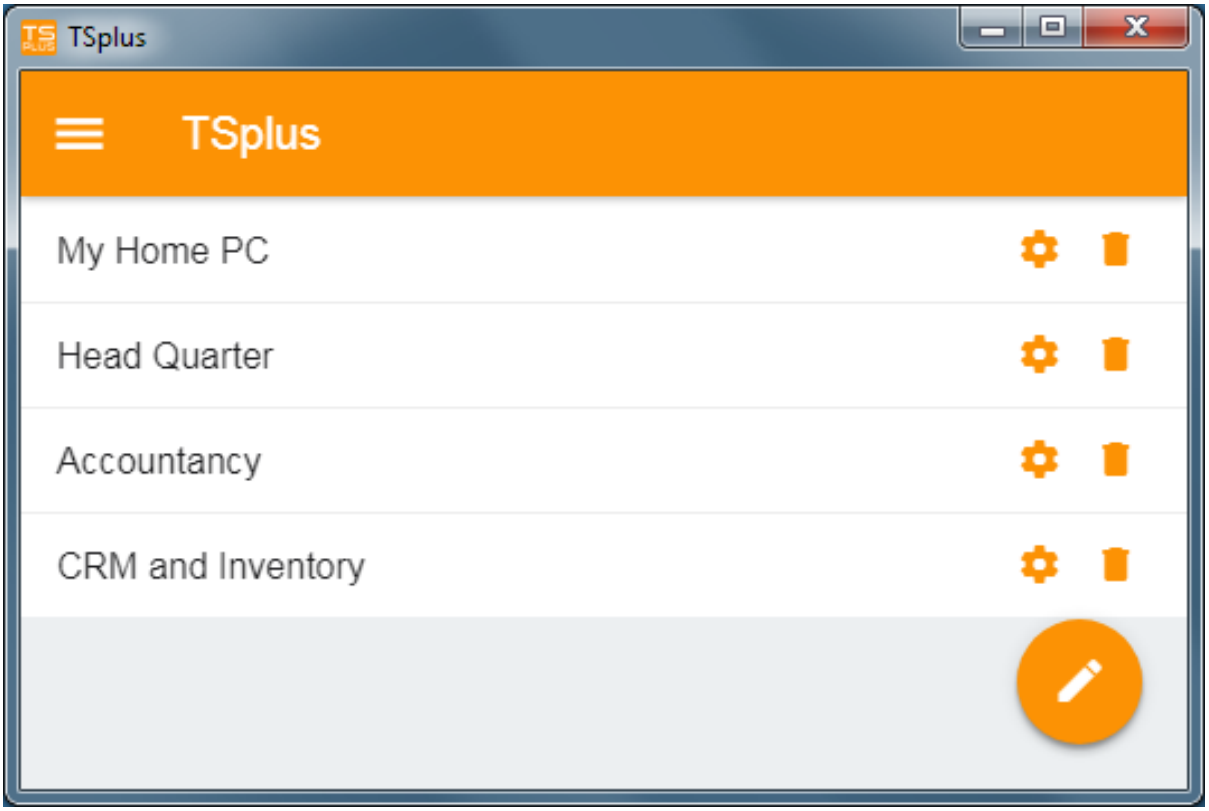
Esta funcionalidad es visible y activa después de la primera conexión al Portal Web.

La documentación completa de TSplus Advanced Security está disponible en esta página .

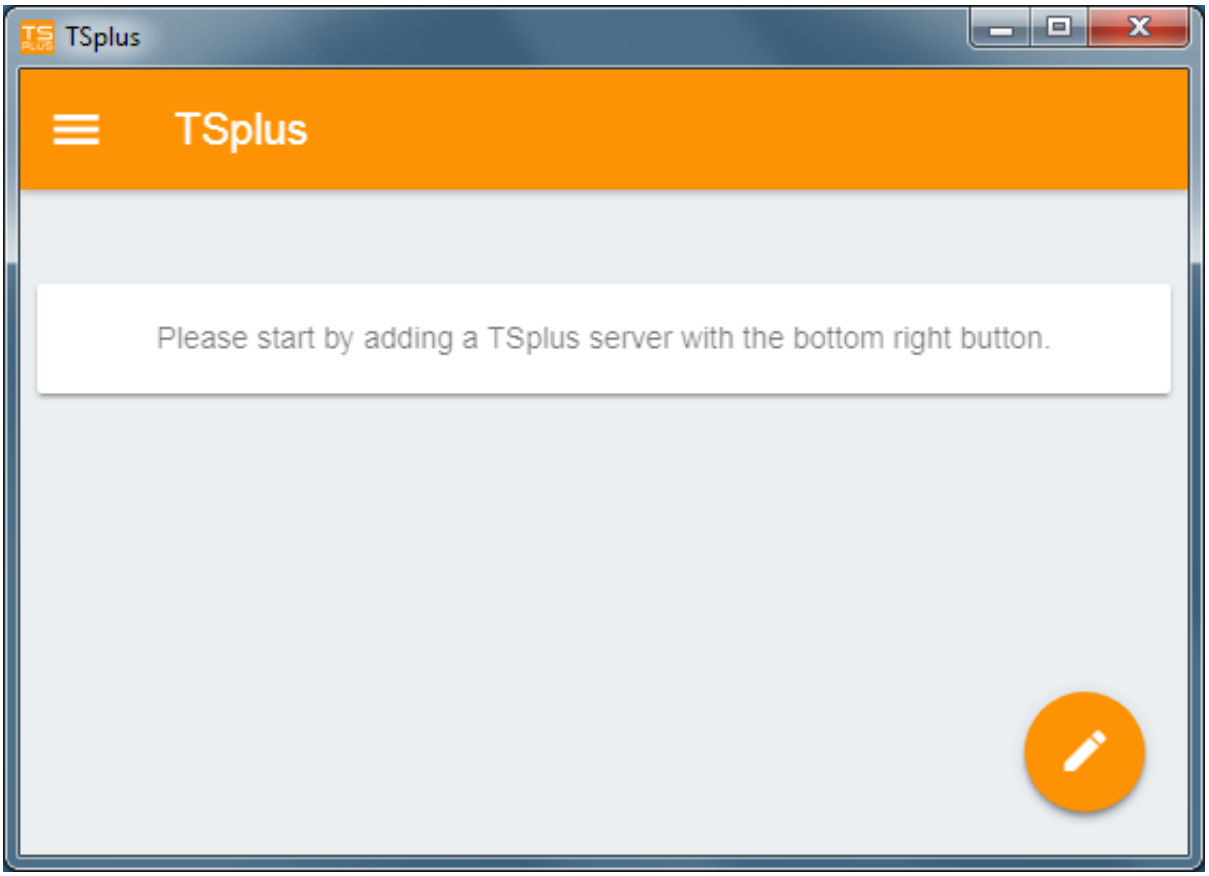
TSplus Configuración de la Aplicación

Administra tus servidores

La interfaz de usuario y la configuración son simples e intuitivas.



Primero, agrega un servidor TSplus haciendo clic en el botón de la parte inferior derecha:

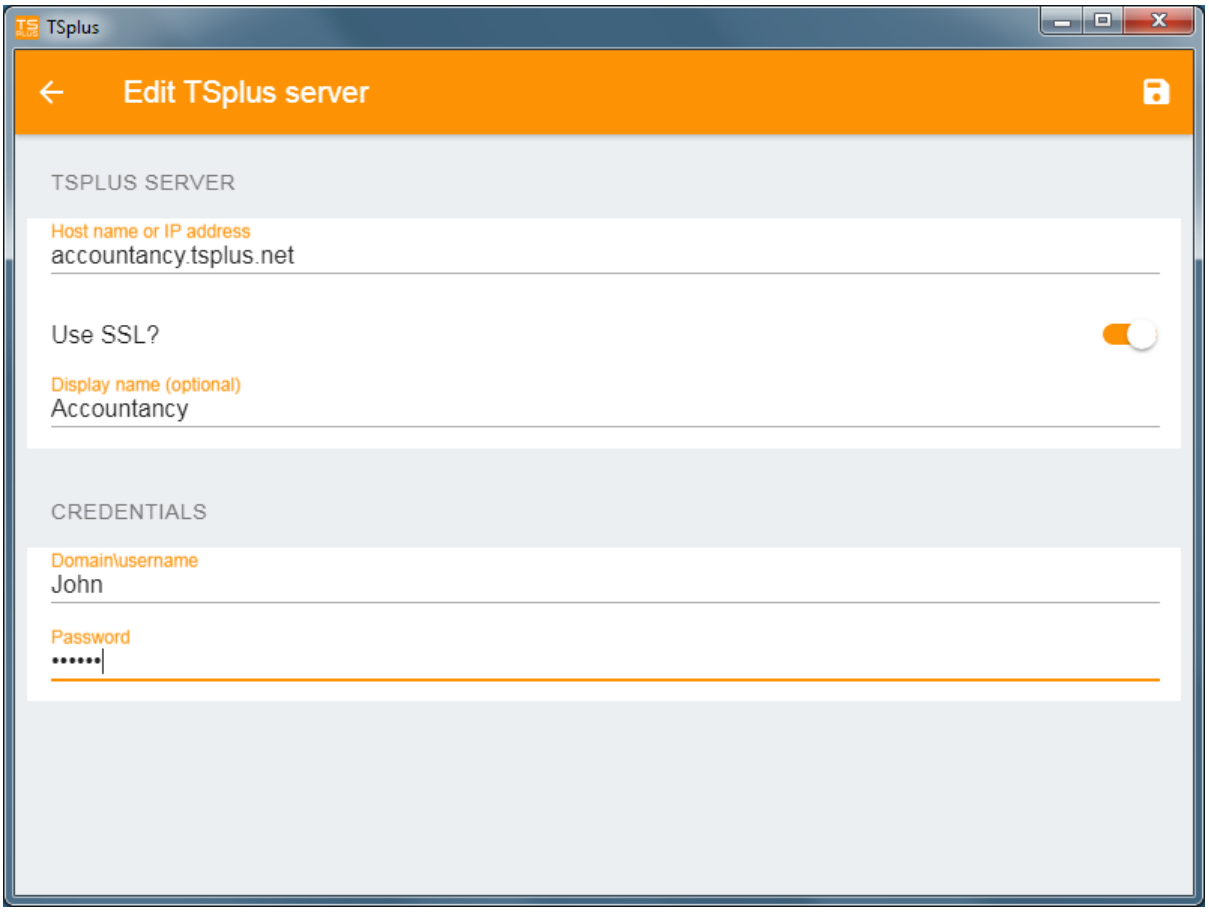


Luego, agrega la información de tu servidor y configúralo:

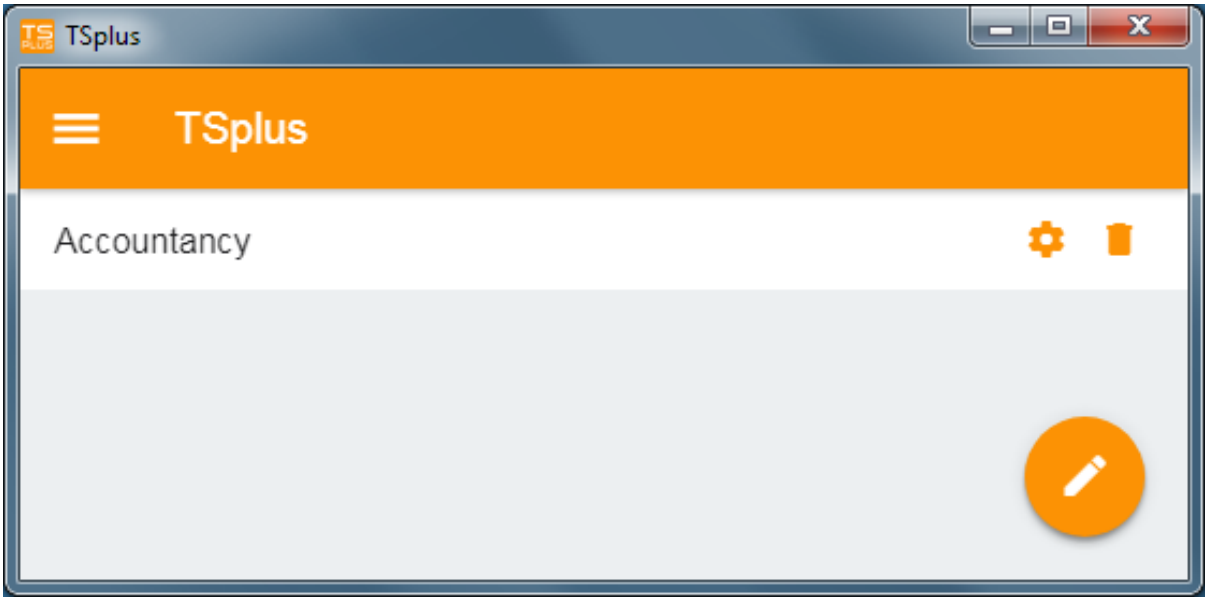
- Ingrese su nombre de host o dirección IP.
- SSL está deshabilitado por defecto, pero puedes optar por habilitarlo.

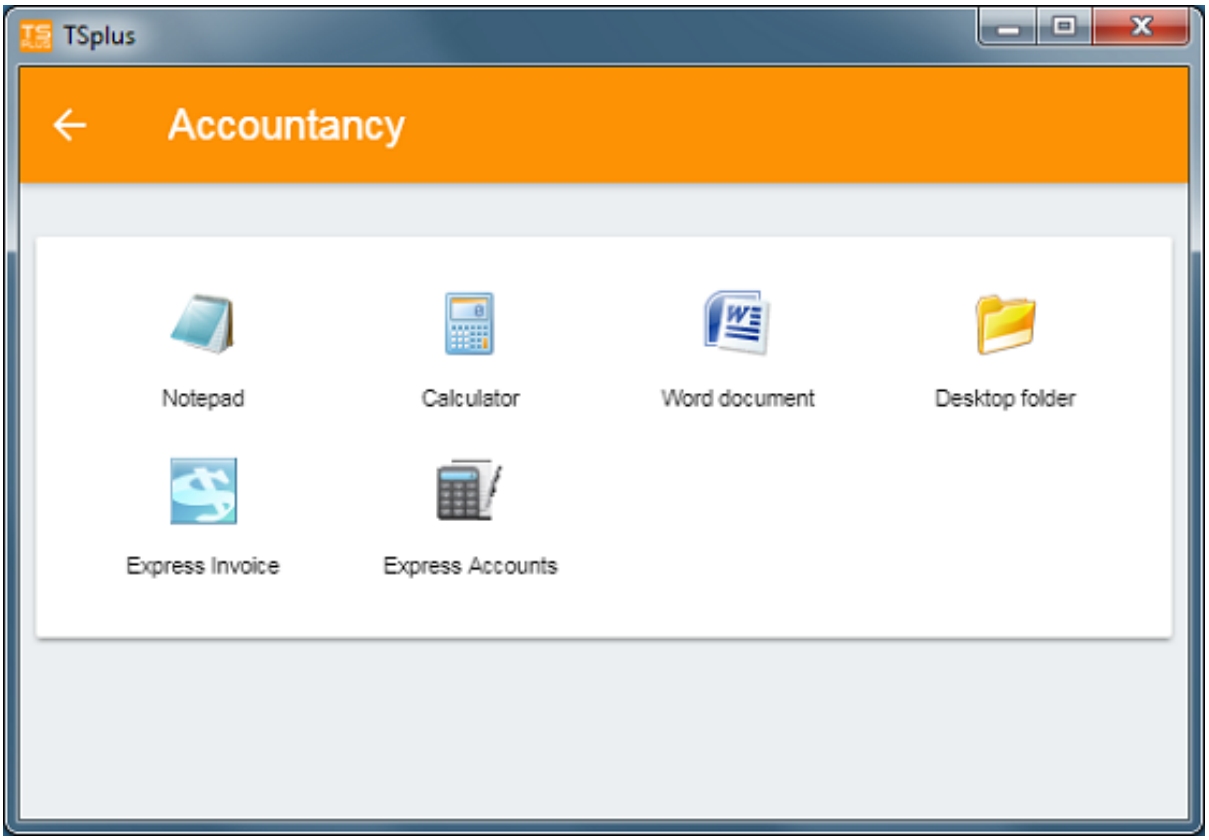
Advertencia: La activación de SSL solo funciona si instalaste un certificado SSL válido en tu servidor TSplus. Ver esta documentación para más información.

- Ingrese su nombre de visualización, que es opcional.
- Ingrese las credenciales de su usuario con el dominio o nombre de usuario y su contraseña.
- Si está utilizando el protocolo HTTPS, debe ingresar el puerto en la dirección configurada. appportal.mydomain.com:443



Luego, haga clic en el botón de la parte superior derecha para guardar. Ahora puede hacer clic en su servidor para acceder a sus aplicaciones:





Impresión

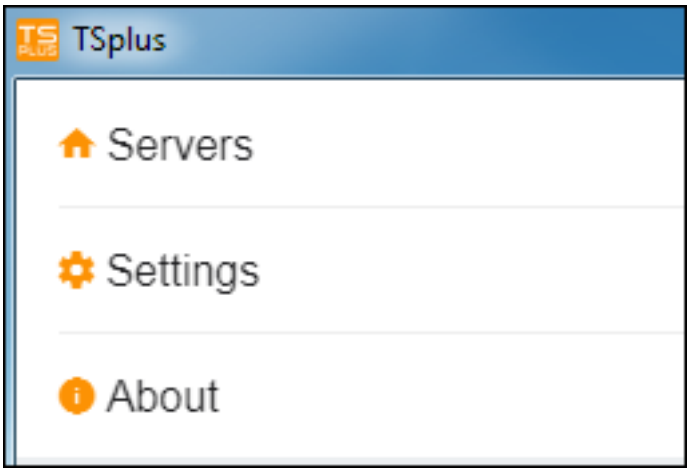
Imprima fácilmente en su impresora local utilizando el Impresora Universal .

Desde la versión 11.40 de TSplus App, los documentos impresos se abren con la aplicación de lector PDF predeterminada.

Configuraciones y Versión

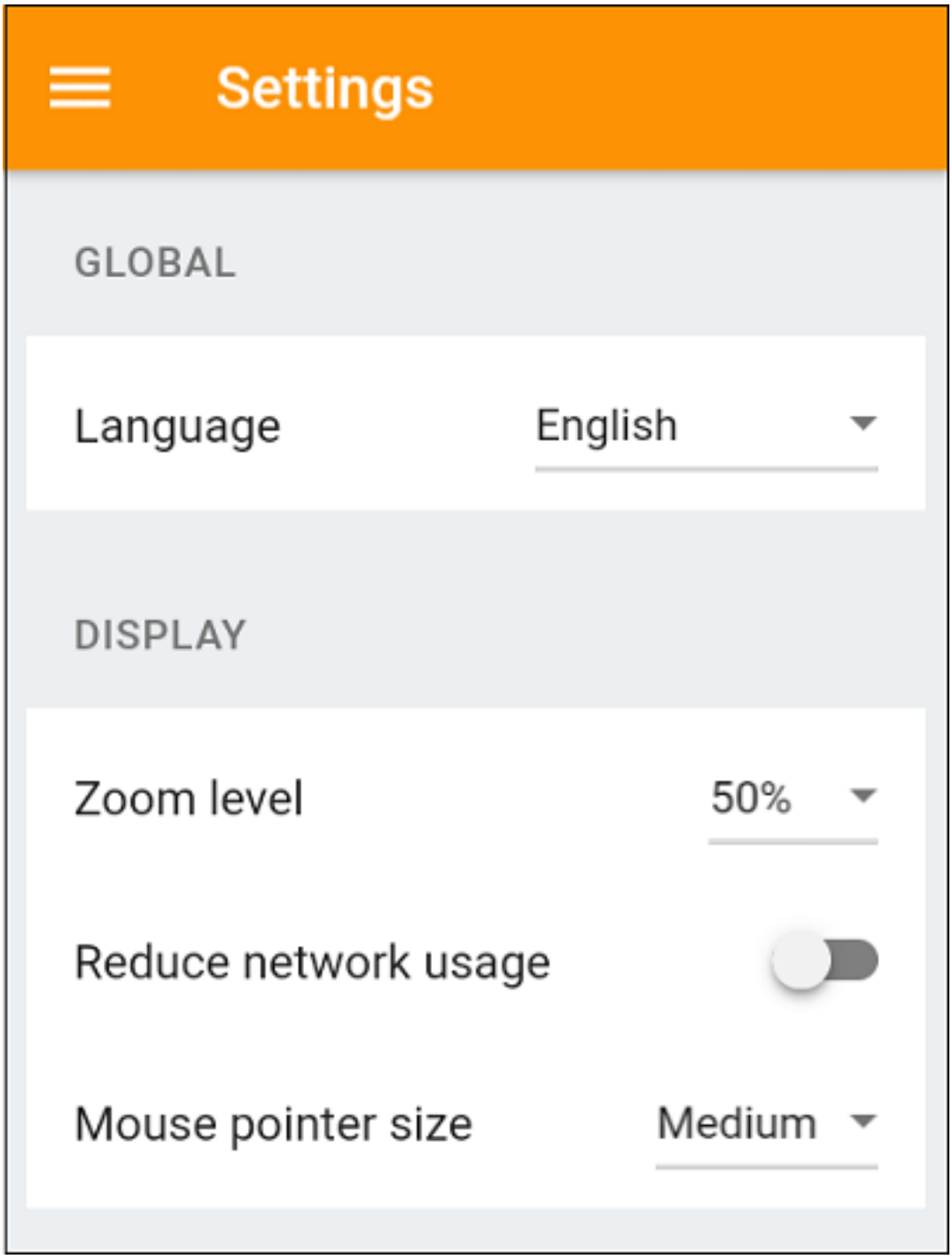
Bajo el menú superior izquierdo, puedes:

- Administra tus servidores
- Gestiona tus configuraciones
- Vea la información legal en la sección Acerca de y su versión de la aplicación TSplus.



Configuraciones

Se encuentran disponibles varias configuraciones en la ventana de Configuración:



- Puedes cambiar el idioma.
- Modifique la configuración de visualización cambiando el nivel de zoom a su conveniencia, reduzca el uso de la red o elija entre 3 tamaños de puntero de mouse: pequeño, mediano o grande.

Autenticación 2FA

La aplicación de Android es compatible con 2FA.

La aplicación solicita el código de 2FA si la cuenta de usuario ha sido configurada para usar 2FA.

La activación no se puede realizar desde la aplicación móvil, primero debe configurar 2FA desde el portal web.

Versión

En la pestaña Acerca de, puedes ver la información legal así como la versión actual de la aplicación TSplus:



TSplus App

La aplicación TSplus te permite conectarte a tu servidor TSplus desde cualquier dispositivo, en cualquier lugar.

Al igual que TSplus, proporciona conexiones remotas rápidas y estables desde tabletas y teléfonos inteligentes a escritorios de Windows y aplicaciones empresariales.

Acceda a sus aplicaciones y datos comerciales en tiempo real y imprima fácilmente cualquier documento y foto que necesite en la impresora local más cercana.

La aplicación TSplus es compatible con 2FA.



Para más información y enlaces de descarga, dirígete a la página de la aplicación en nuestro sitio web.

Requisitos de hardware y sistemas operativos

La aplicación TSplus está disponible en móviles y tabletas con los siguientes sistemas operativos: iOS, Android desde la versión 4.4 y Linux.

versión de Android

versión de iOS

Requisitos previos

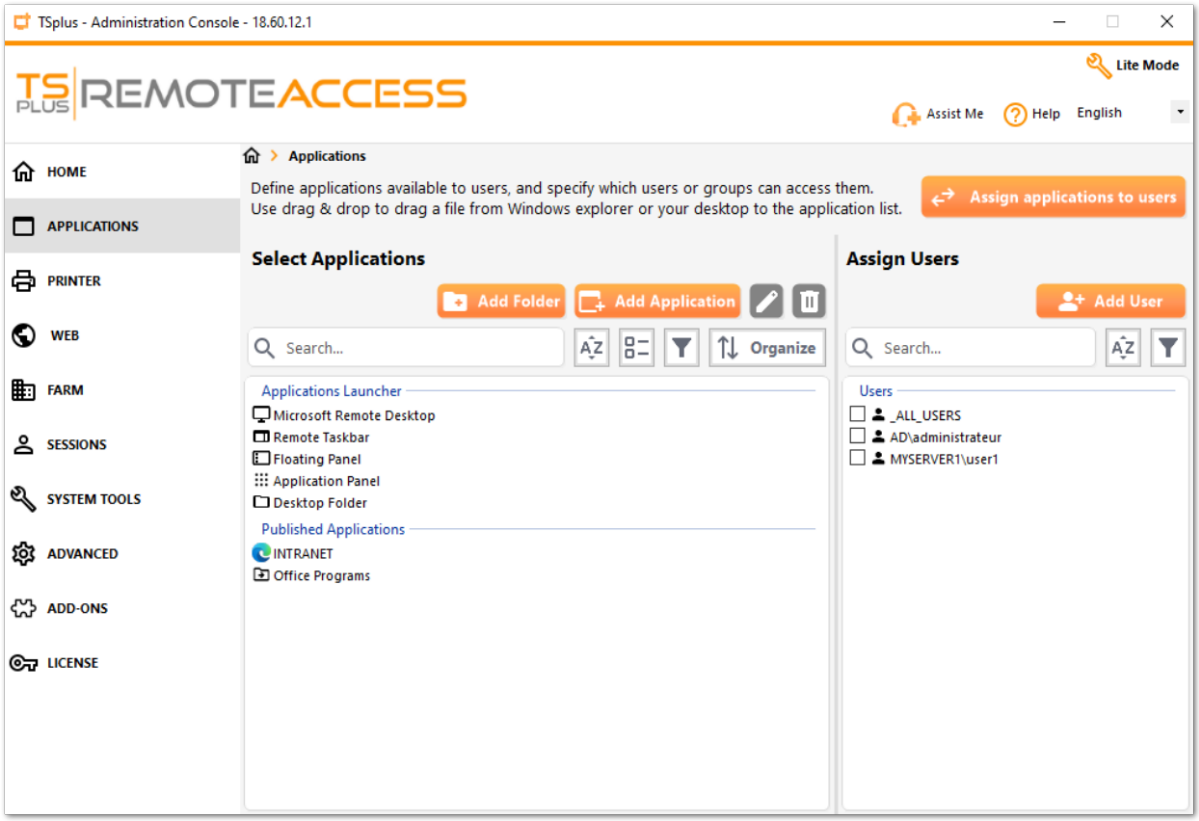
- El sitio host debe ser un sistema TSplus Mobile Web o Enterprise.
- La versión 11.30 (y superior) debe instalarse en este host.

Asignación de aplicaciones a usuarios o grupos

Una vez que tengas publicó algunas aplicaciones , puedes asignarlos a uno o más usuarios y/o grupos.

Asignar usuarios o grupos a aplicaciones

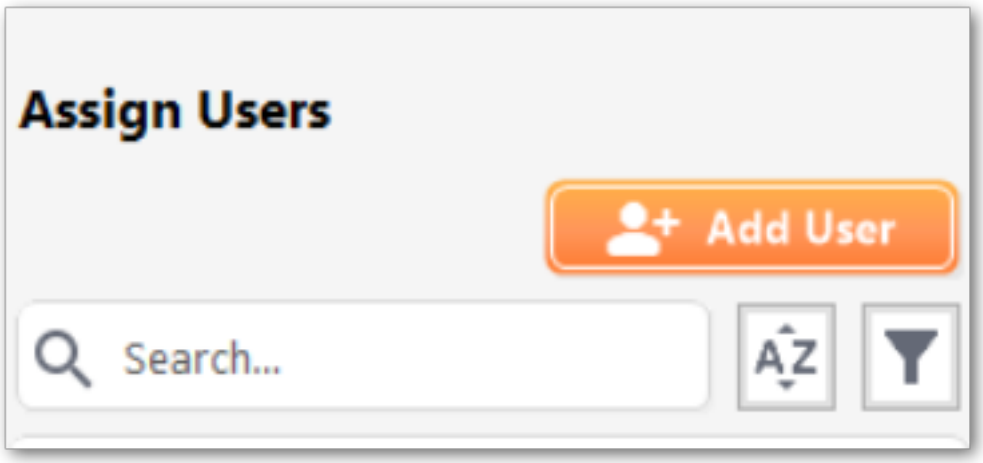
Cada tarea debe realizarse en el panel derecho de la sección "Aplicaciones" del AdminTool. Este panel derecho muestra todos los usuarios y grupos que actualmente tienen aplicaciones asignadas.



Para asignar usuarios o grupos, primero deberá agregar los usuarios/grupos para los que desea asignar la aplicación.

Agregar usuarios o grupos

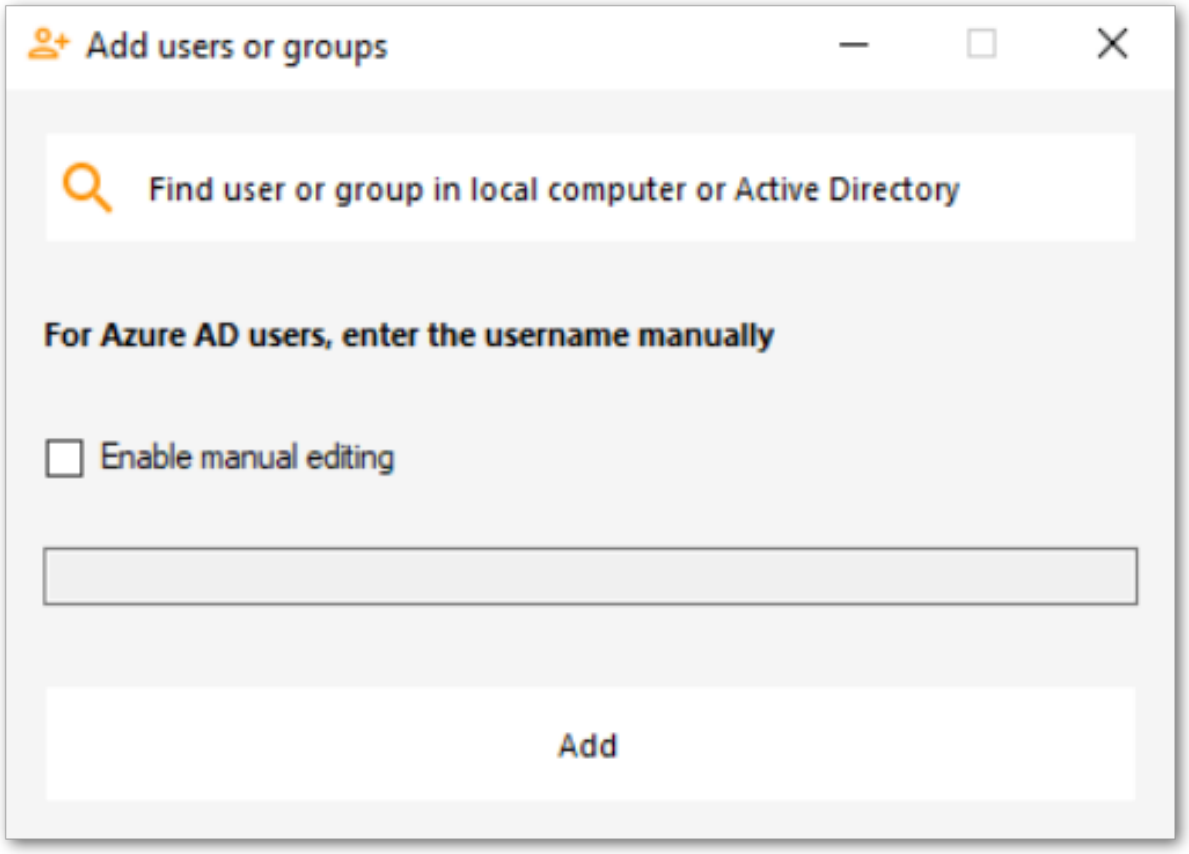
Para agregar usuarios o grupos, haga clic en los botones del ícono "Agregar usuario".



Se le recibirá con esta interfaz, que le permitirá encontrar un usuario o grupo a través del selector de usuario/grupo, o escribir directamente el nombre del usuario/grupo que desea agregar.

Los usuarios locales o de Active Directory deben ser seleccionados utilizando el botón Buscar usuarios o grupos locales o de Active Directory.

Solo los usuarios externos pueden ser ingresados directamente en el cuadro de texto.



El nombre de usuario especial _ALL_USERS

En la lista de usuarios, siempre encontrarás disponible el usuario “_ALL_USERS”. Este usuario no es un usuario de Windows, sino un usuario virtual. Si seleccionas una aplicación y marcas el nombre de usuario “_ALL_USERS”, entonces la aplicación estará disponible para todos los usuarios.

Asignar usuarios o grupos a aplicaciones

Una vez que se han agregado los usuarios, asígnales aplicaciones mediante:

1. seleccionando en el panel izquierdo las aplicaciones que desea asignar a su usuario
2. marcando en el panel derecho la casilla junto a su nombre de usuario para asignar las aplicaciones seleccionadas a ese usuario

Ej: si quiero asignar el bloc de notas al usuario "benjamin", simplemente selecciono la aplicación "bloc de notas" a la izquierda y marco la casilla junto al nombre de usuario "benjamin" a la derecha.

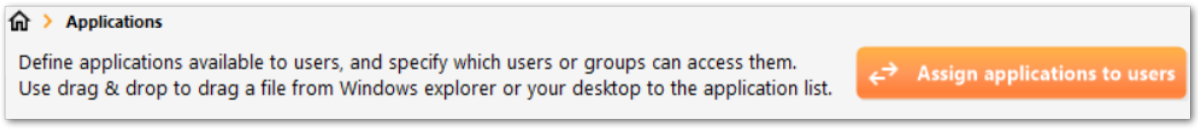
Para desasignar usuarios, simplemente desmarque la casilla junto al nombre del usuario.

Esta acción admite la selección múltiple
Esto significa que puedes seleccionar múltiples aplicaciones y no tienes que asignar una

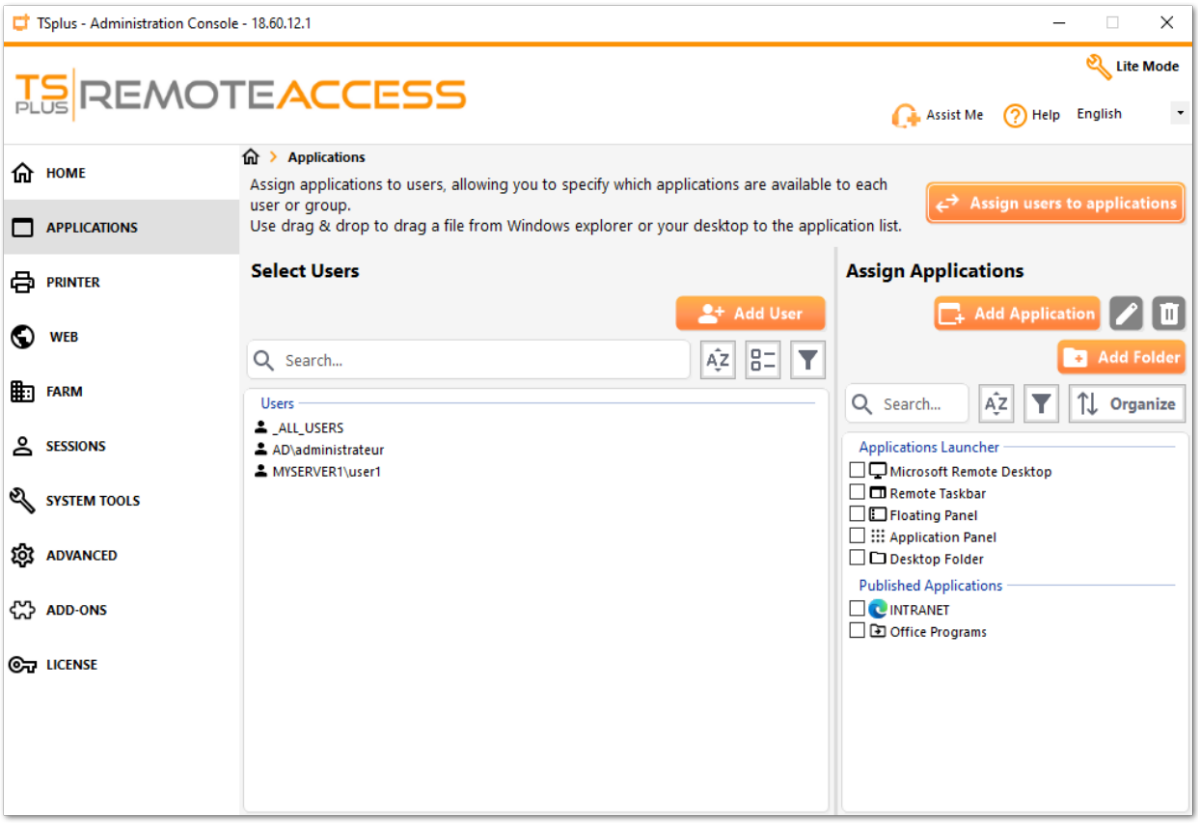
aplicación a la vez.

Asignar aplicaciones a usuarios o grupos

Si prefieres seleccionar usuarios o grupos y asignarles aplicaciones, puedes hacerlo haciendo clic en “Asignar aplicaciones a usuarios”.



Esto invertirá el panel lateral izquierdo y derecho.



Después de hacer clic en el botón, para asignar aplicaciones a los usuarios:

1. seleccionando en el panel izquierdo los usuarios o grupos que desea asignar a su aplicación
2. verificando en el panel derecho la casilla junto al nombre de su aplicación para asignar a los usuarios o grupos seleccionados a esa aplicación

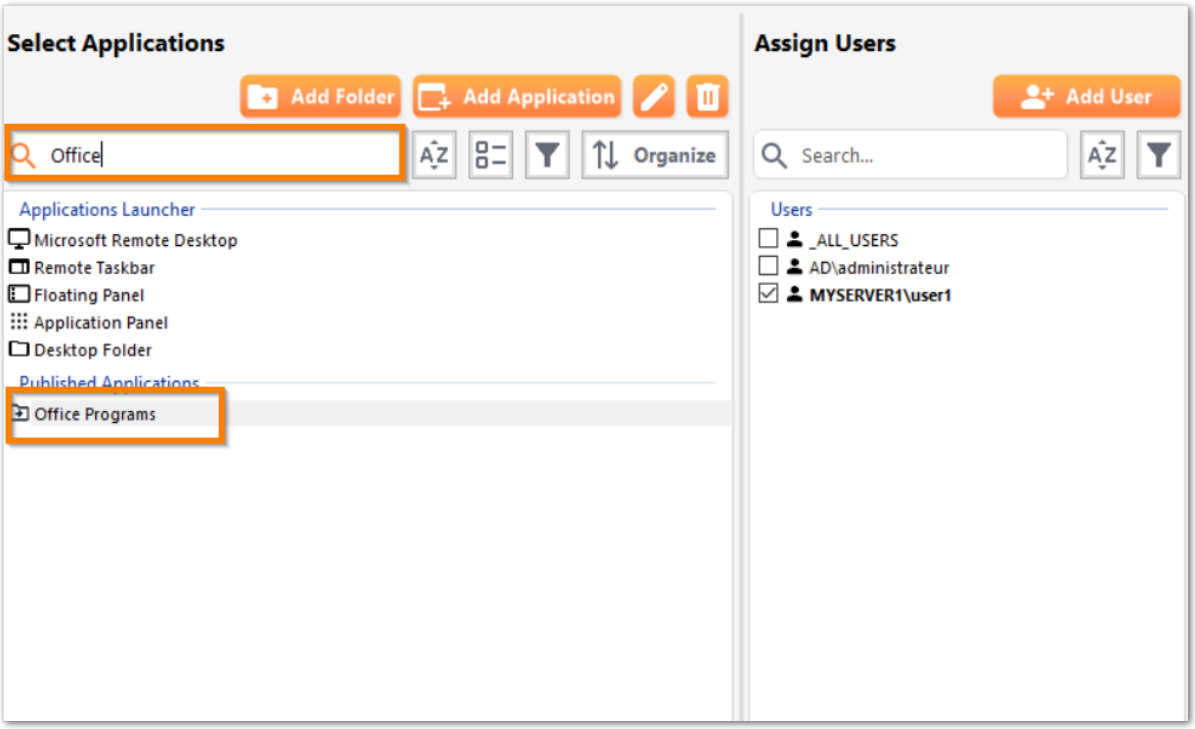
Ej: si quiero asignar el bloc de notas al usuario "benjamin", simplemente selecciono al usuario "benjamin" a la izquierda y marco la casilla junto al nombre de la aplicación "bloc de notas" a la derecha.

Para desasignar aplicaciones, simplemente desmarque la casilla junto al nombre de la aplicación.

Esta acción admite la selección múltiple
Esto significa que puedes seleccionar múltiples usuarios y no tienes que asignar usuarios uno a la vez.

Buscar y filtrar

Para facilitar la gestión de asignación de usuarios, hay disponible una barra de búsqueda así como un botón de filtrado, que permite mostrar solo usuarios o solo grupos.

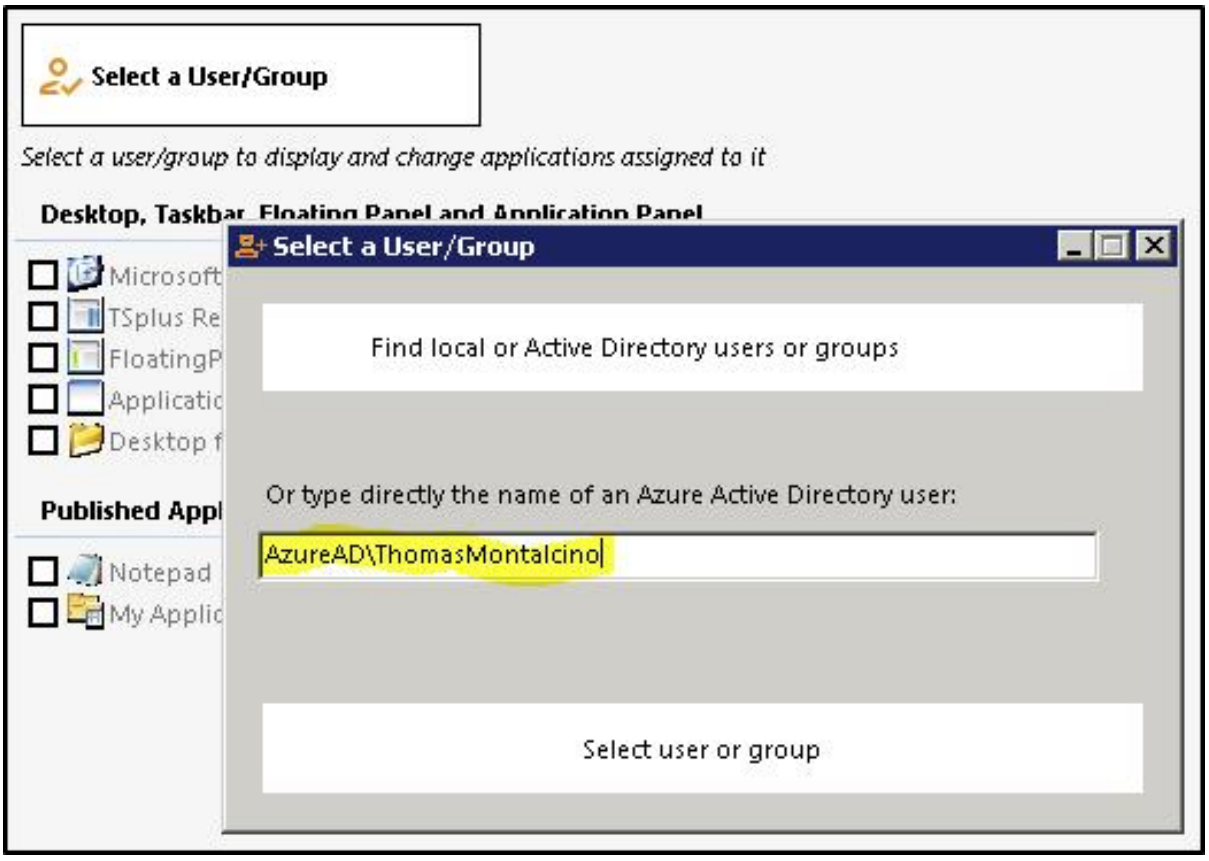


También puedes usar el botón de filtro para que solo se muestren las aplicaciones asignadas/no asignadas (o los usuarios asignados/no asignados si cambias la vista).
Esto te ayudará a gestionar tus asignaciones en caso de que tengas muchos usuarios con aplicaciones asignadas, o simplemente muchas aplicaciones publicadas.

Asignación de aplicaciones a usuarios con Azure Active Directory

Resumen

Para asignar un usuario de Azure Active Directory a una aplicación desde AdminTool > Aplicaciones > Usuarios :



Los usuarios locales o de Active Directory deben ser seleccionados utilizando el botón Buscar usuarios o grupos locales o de Active Directory. Solo se pueden ingresar usuarios externos directamente en el cuadro de texto.

Gestión del servidor web incorporado

Su servidor de escritorio remoto debe estar disponible, ser de fácil acceso y seguro. Por eso, TSplus utiliza un servidor web integrado que le ayuda a gestionar fácilmente su estado y operaciones.

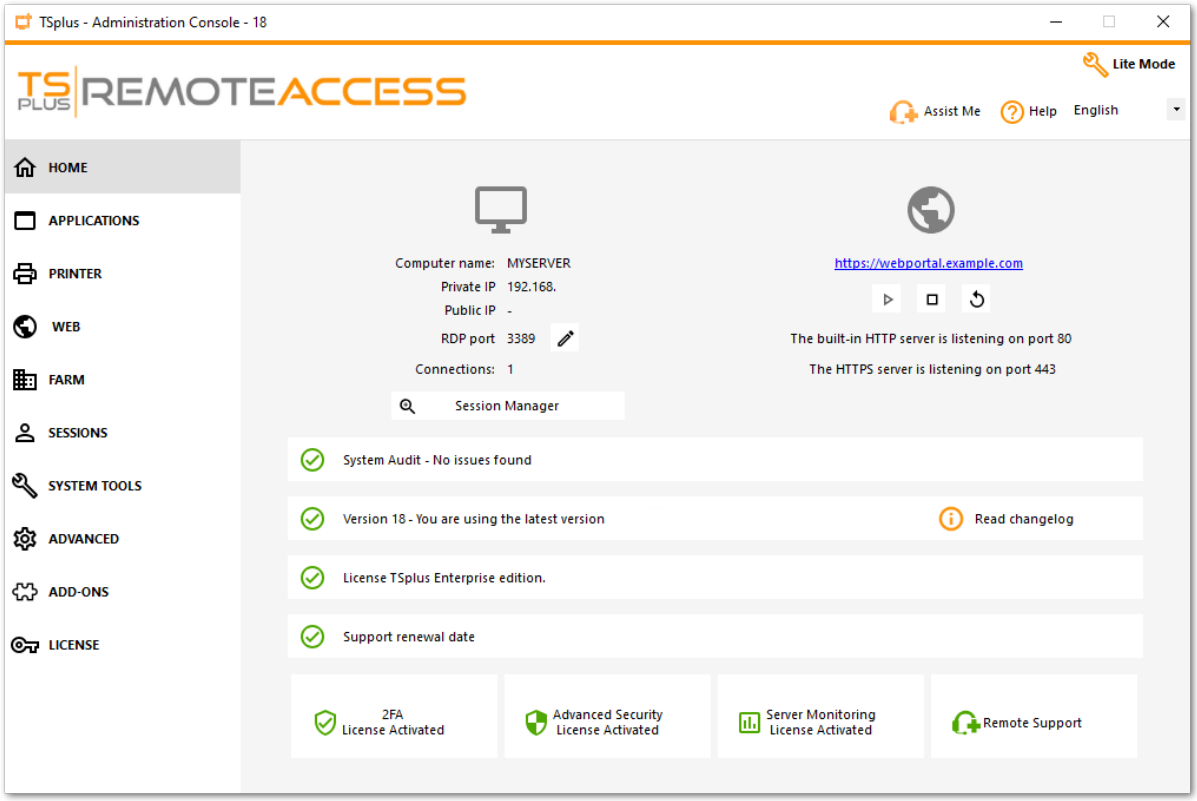
Una Consola de Gestión está disponible en la Herramienta de Administrador. Esta Consola de Gestión le permite ver y configurar el estado del Servidor Web integrado de Terminal Service Plus.

Cuando tú instalar TSplus Los servidores web están escuchando en los puertos 80 y 443 por defecto. Asegúrese de que los puertos definidos estén disponibles y de que Java esté instalado en el servidor.

Ver el video acerca de las características web.

Estado de los componentes del servidor web

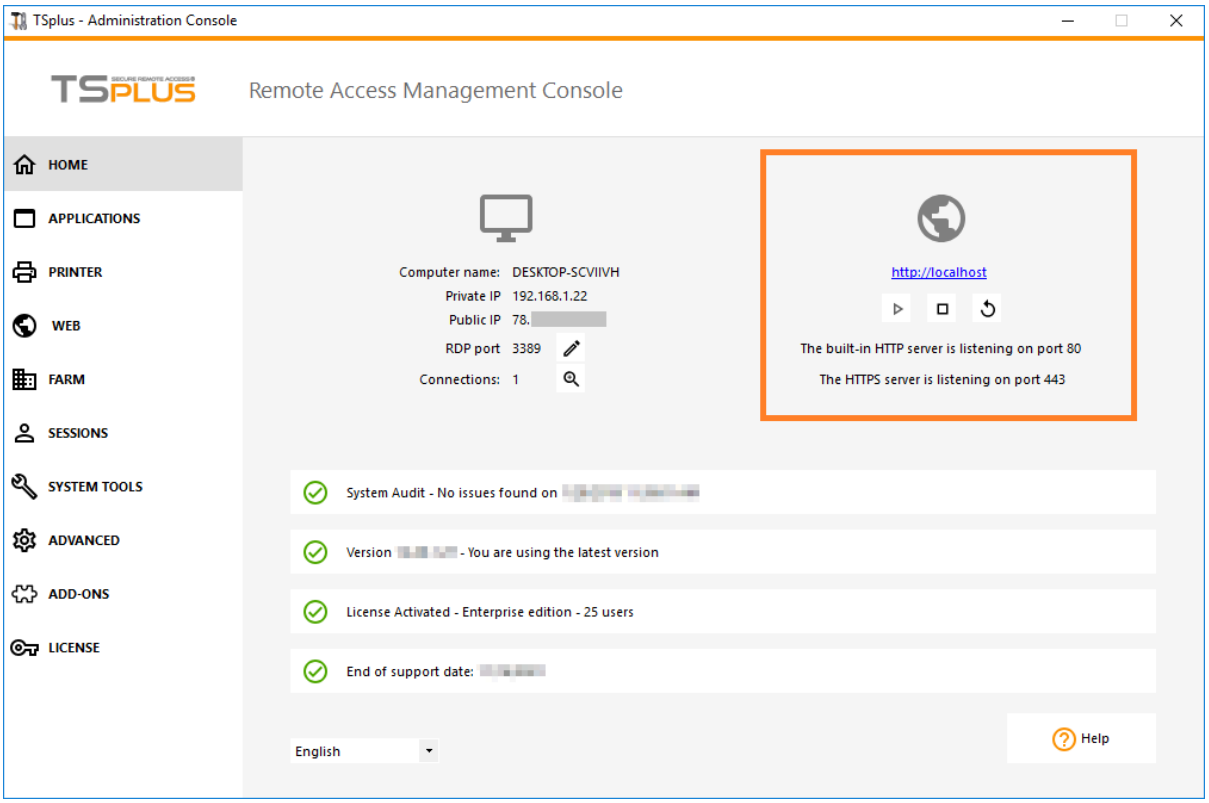
El estado de los componentes principales del servidor web se muestra en el panel de control de AdminTool Home.



Consideraciones de puertos (máquina local y firewall / enrutador)

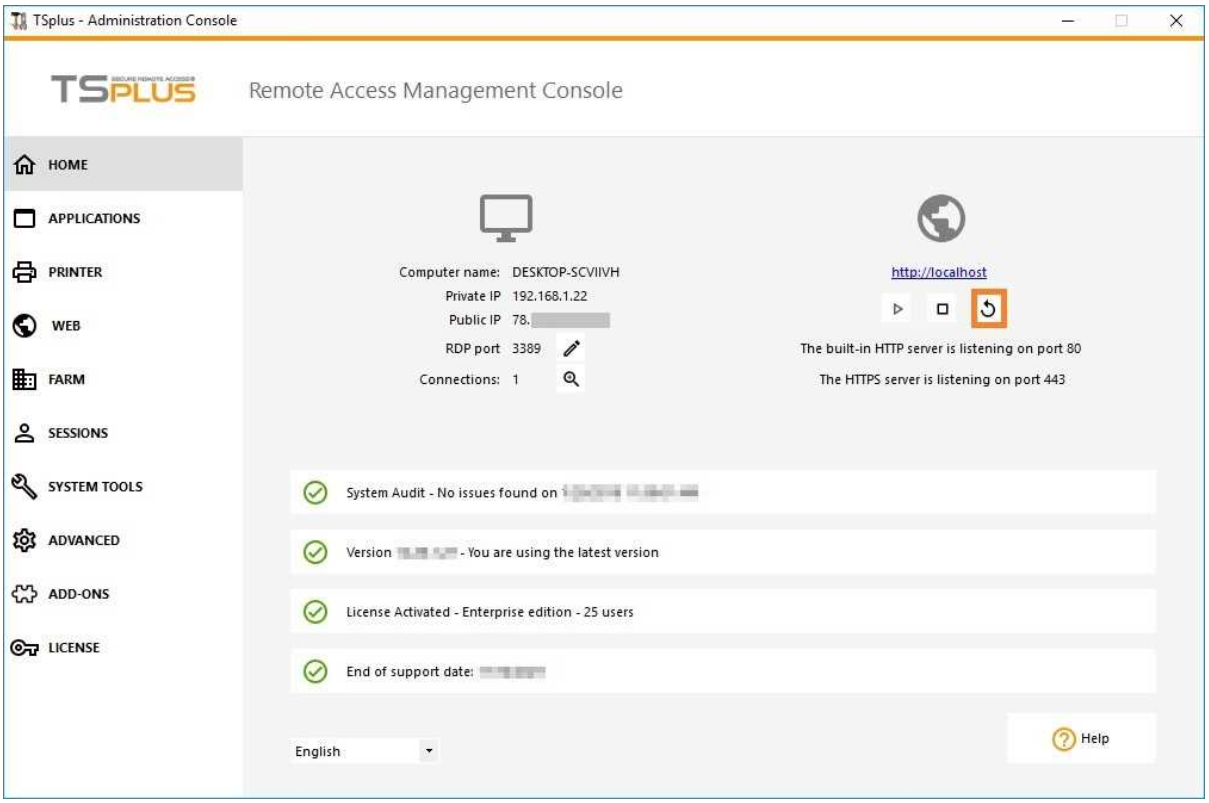
Terminal Service Plus solo requiere que se abra el Puerto 80 o el Puerto 443.

El puerto 3389 puede permanecer cerrado.

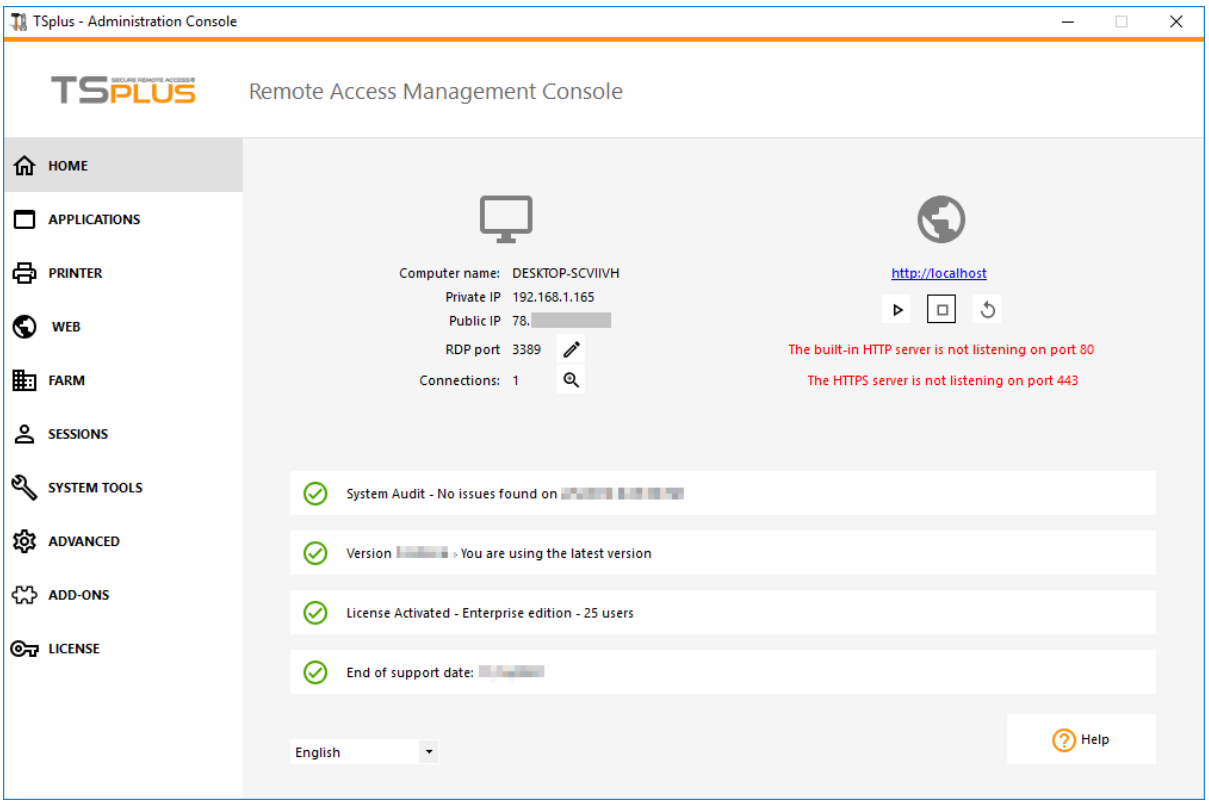


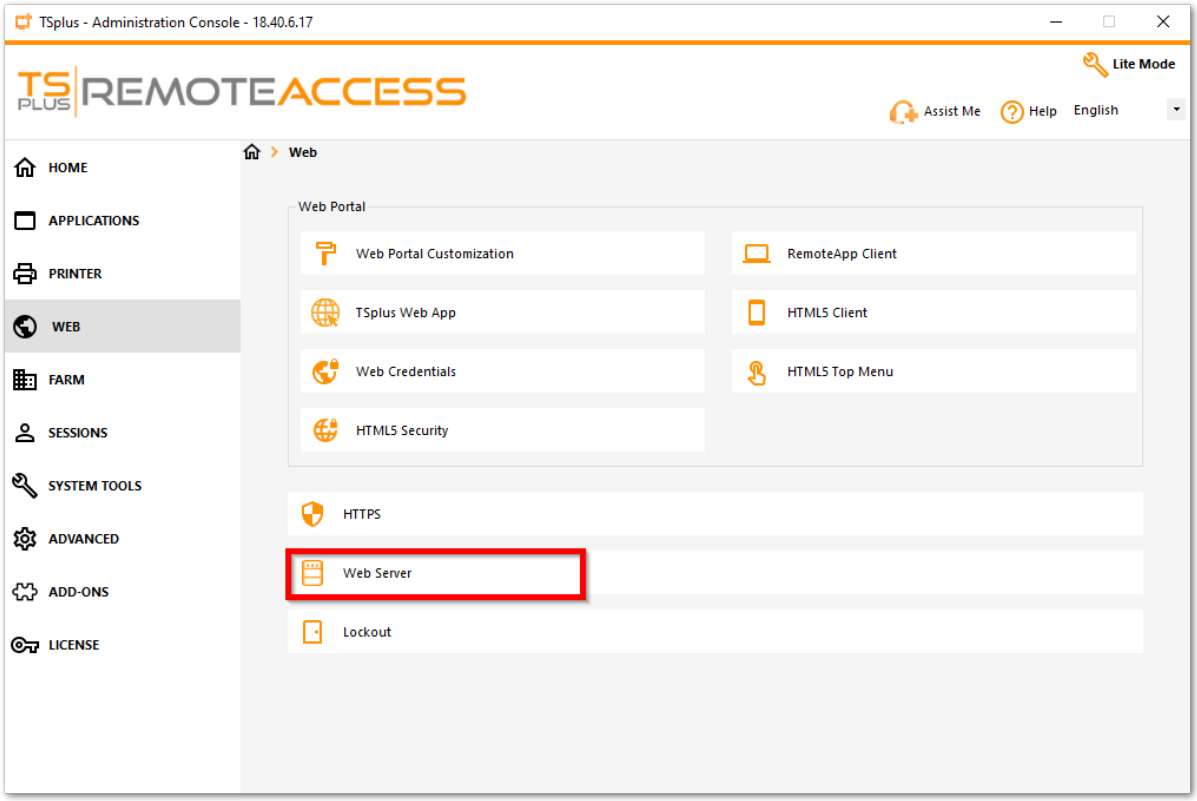
Reiniciar / Detener el Servicio del Servidor Web

Si ves que un servicio no está en funcionamiento, es posible que necesites reiniciar los servidores web haciendo clic en el botón "Reiniciar servidores web", que está representado por una flecha a la derecha; los servidores web se reiniciarán y el servicio debería estar funcionando nuevamente.



Si hace clic en el botón "Detener servidores web", ubicado en el medio, los servidores web se detendrán. El estado del servidor HTTP y HTTPS ahora se mostrará en rojo, indicando que los servicios HTTP / HTTPS están detenidos.





Puedes cambiar los puertos durante la instalación o en cualquier momento haciendo clic en la pestaña Web - Servidor Web. En esta pestaña, puedes elegir usar un servidor web HTTP diferente, modificar la ruta raíz del Servidor Web y los números de puerto HTTP/HTTPS. Asegúrate de que estos puertos estén disponibles antes de cambiarlos: si ocurre un conflicto, el servidor web de TSplus no funcionará. Aquí es una lista no exhaustiva de puertos TCP que podrían ser utilizados por una aplicación en su servidor. Una vez realizadas estas modificaciones, haga clic en guardar y el AdminTool se reiniciará.

###Deshabilitar solo http o http en https

Ver esta documentación para más información sobre este tema.

Para obtener información más detallada sobre **personalización de servidores** y **preferencias** , consulte estas páginas:

Personalización del Portal Web , Portal de Aplicaciones Web , Credenciales Web .

Elegir sus suites de cifrado para mejorar la seguridad

Resumen

TLS/SSL, la seguridad detrás de HTTPS, puede utilizar varios algoritmos diferentes para asegurar, cifrar y autenticar una conexión.

La elección del algoritmo a utilizar se decide mediante un acuerdo entre el servidor y el cliente, dependiendo de qué algoritmos están disponibles en cada lado.

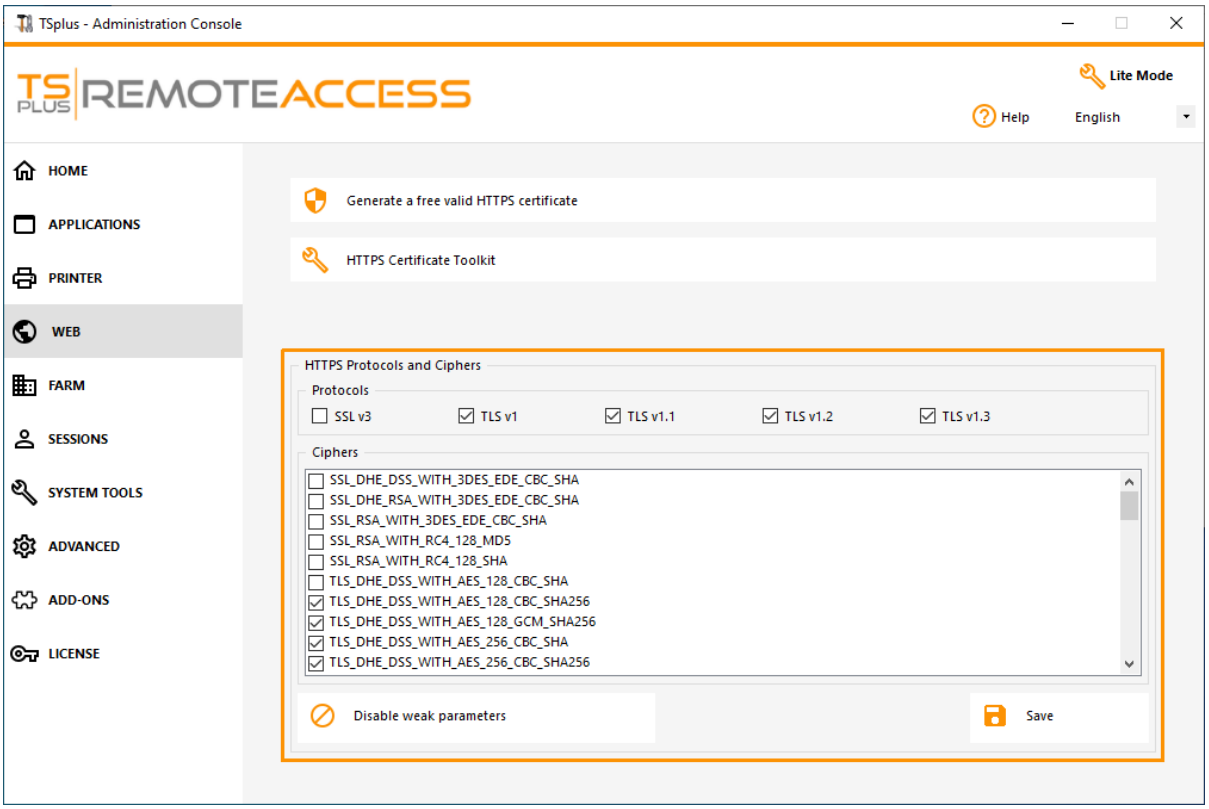
Una suite de cifrado es una combinación nombrada de algoritmos de autenticación, cifrado, autenticación de mensajes e intercambio de claves.

El servidor de Terminal Service Plus puede manejar una gran cantidad de diferentes suites de cifrado. Algunas de ellas son más seguras que otras, pero algunos navegadores antiguos/ legados pueden requerir algoritmos relativamente débiles para conectarse.

Esta es la razón por la que Terminal Service Plus te permite elegir los conjuntos de cifrado que deseas habilitar. Por supuesto, Terminal Service Plus también tiene una configuración fácil para deshabilitar los algoritmos más débiles, mejorando así la seguridad de tus conexiones.

Selección de protocolos y cifrados HTTPS

Para ver la selección de cifrados de Terminal Service Plus, abra Terminal Service Plus AdminTool, haga clic en la pestaña "Web - HTTPS", donde verá los protocolos y cifrados HTTPS:



Habilitar/Deshabilitar un conjunto de cifrado

Puedes habilitar fácilmente un conjunto de cifrado marcando su casilla de verificación y deshabilitar un conjunto de cifrado desmarcándola.

Cuando haya terminado de seleccionar, haga clic en "Guardar".

Esto guardará su selección y recargará la nueva configuración en el servidor web integrado de Terminal Service Plus. Su nueva selección de suites de cifrado se aplica instantáneamente a cada nueva conexión a su servidor.

Selección de suites de cifrado recomendadas

Recomendamos a la mayoría de los administradores que utilicen nuestra selección de suites de cifrado recomendadas, simplemente haciendo clic en el botón “Deshabilitar parámetros débiles” y luego en el botón “Guardar”.

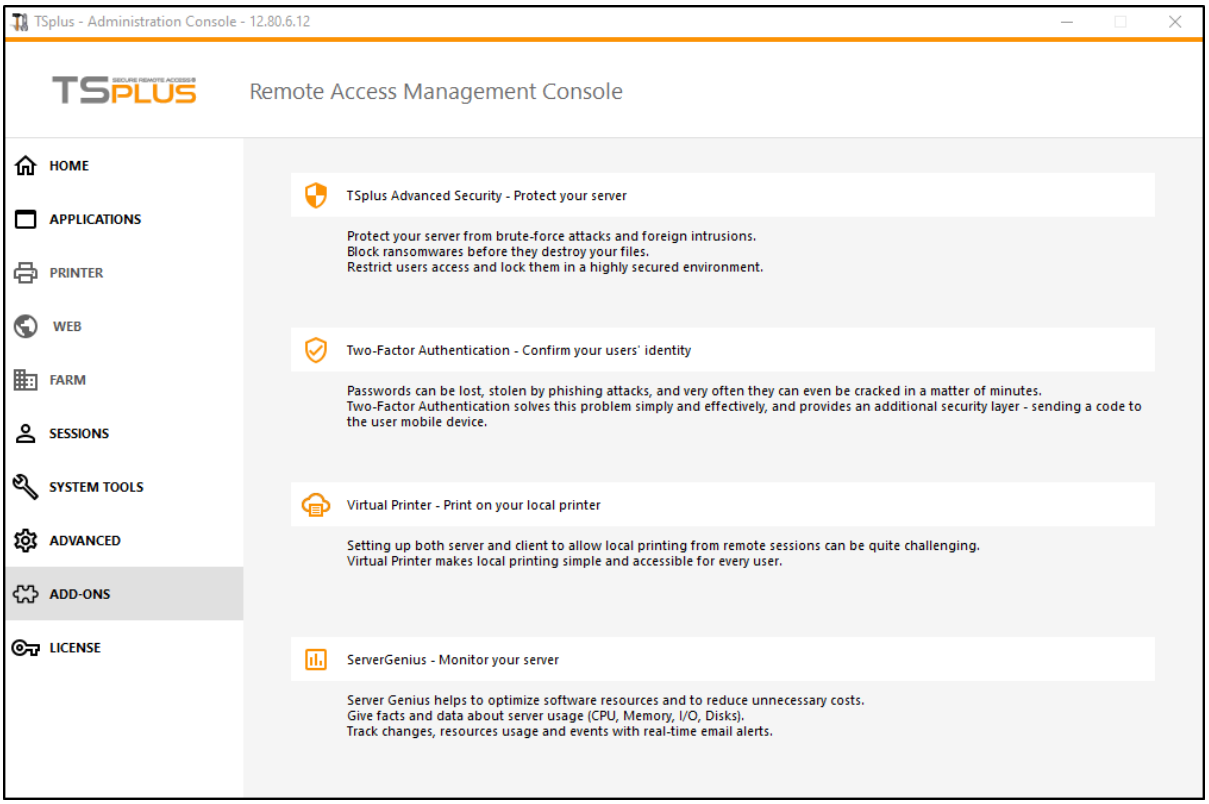
Esta acción deshabilitará todos los conjuntos de cifrado que actualmente se conocen como débiles.

Puedes verificar con Herramienta de Pruebas en Línea de SSL Labs sin esos conjuntos de cifrado débiles deberías obtener la calificación máxima: ¡A!

Clic para ayudar - Herramienta de administración - Complementos

¿Quieres obtener ayuda sobre una función de Terminal Service Plus Admin Tool rápidamente?

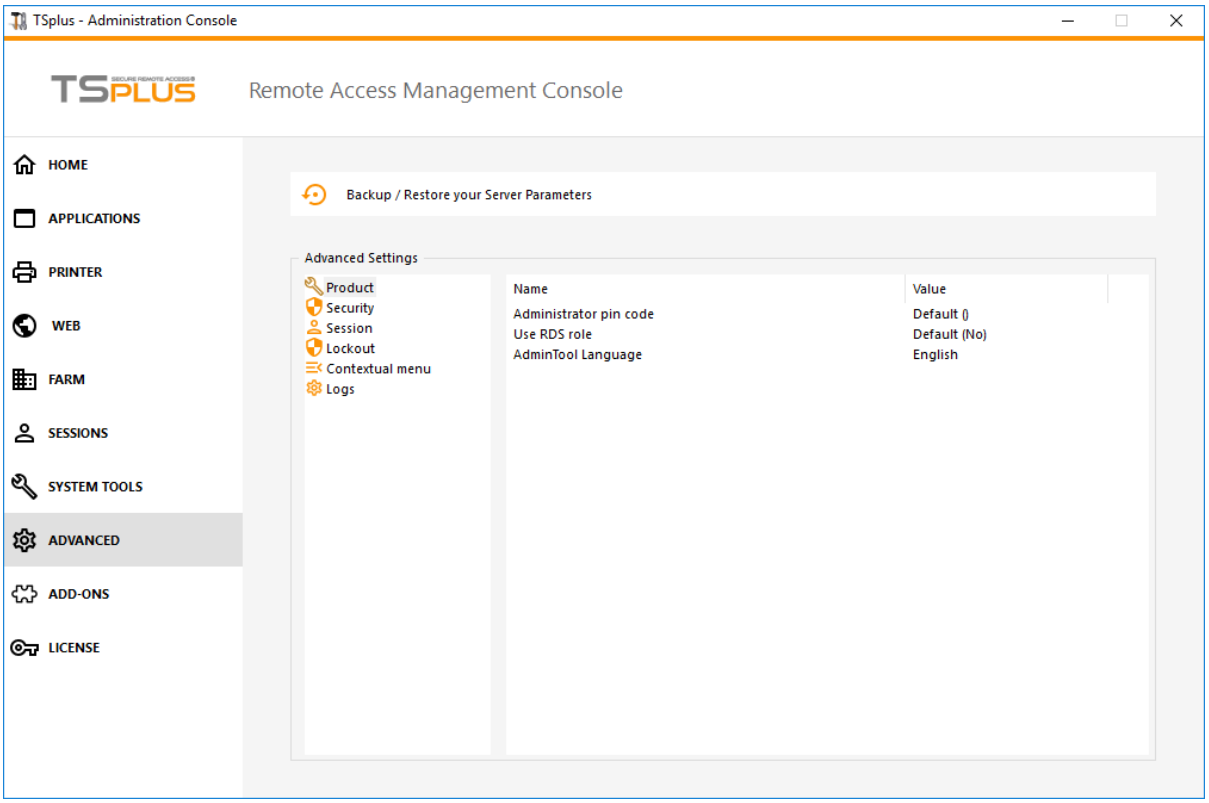
Solo **haga clic en un mosaico o en una pestaña** ¡Ir a la ayuda correspondiente!



Clic para ayudar - Herramienta de administración - Avanzado

¿Quieres obtener ayuda sobre una función de Terminal Service Plus Admin Tool rápidamente?

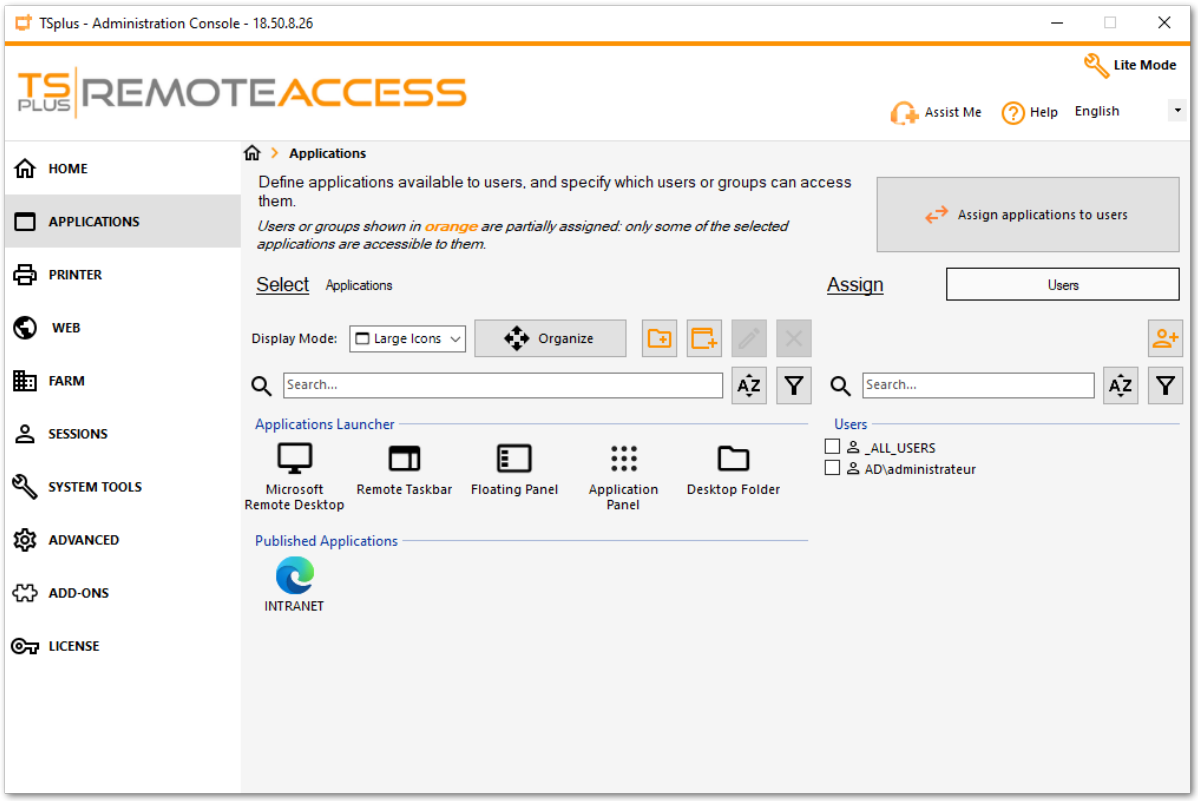
Solo **haga clic en un mosaico o en una pestaña** ¡Ir a la ayuda correspondiente!



Haga clic para ayudar - Herramienta de administración - Aplicaciones

¿Quieres obtener ayuda sobre una función de Terminal Service Plus Admin Tool rápidamente?

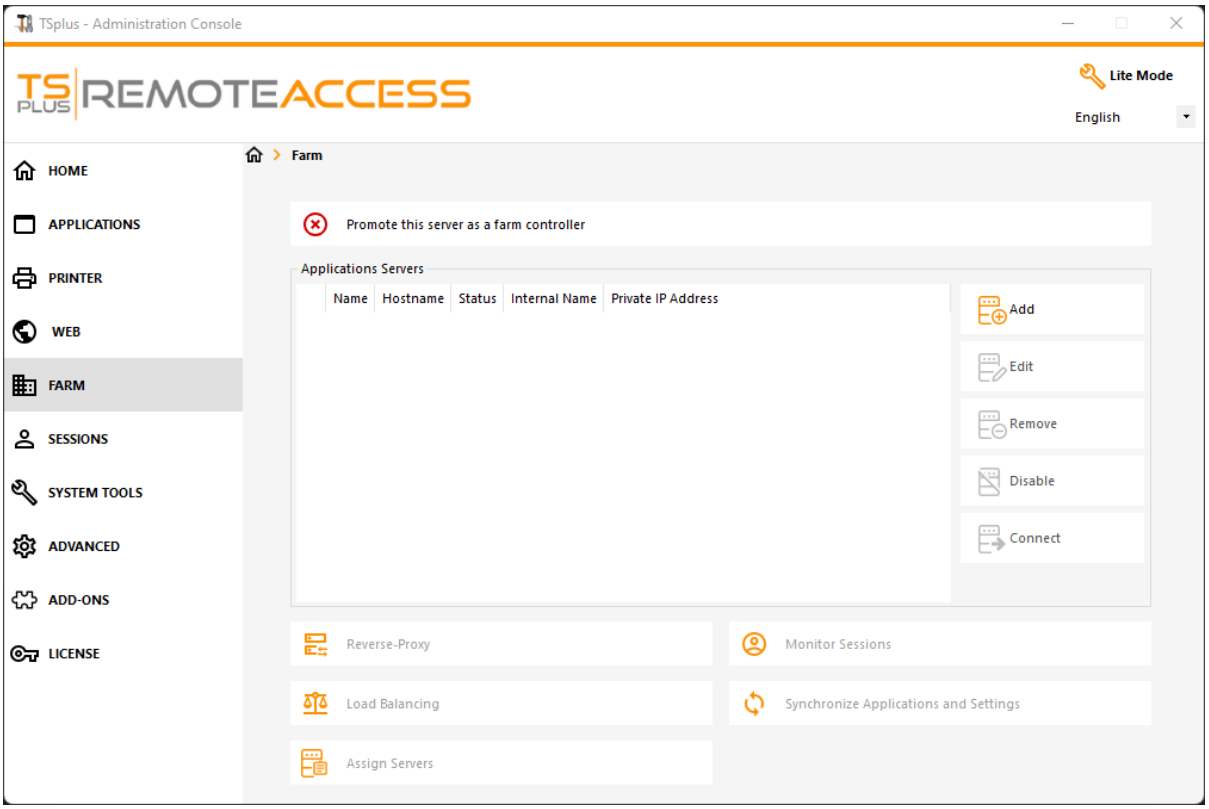
Solo **haga clic en un mosaico o en una pestaña** ¡Ir a la ayuda correspondiente!



Clic para ayudar - Herramienta de administración - Granja

¿Quieres obtener ayuda sobre una función de Terminal Service Plus Admin Tool rápidamente?

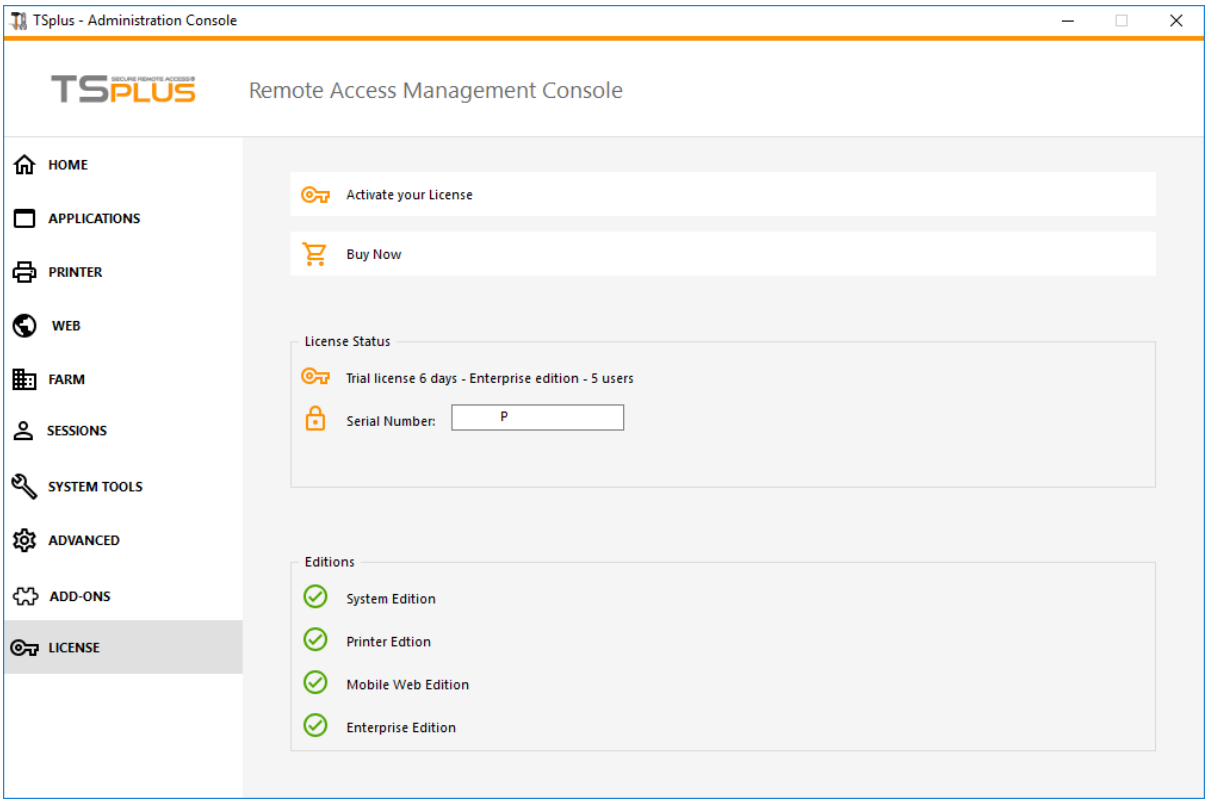
Solo **haga clic en un mosaico o en una pestaña** ¡Ir a la ayuda correspondiente!



Clic para ayudar - Herramienta de administración - Licencia

¿Quieres obtener ayuda sobre una función de Terminal Service Plus Admin Tool rápidamente?

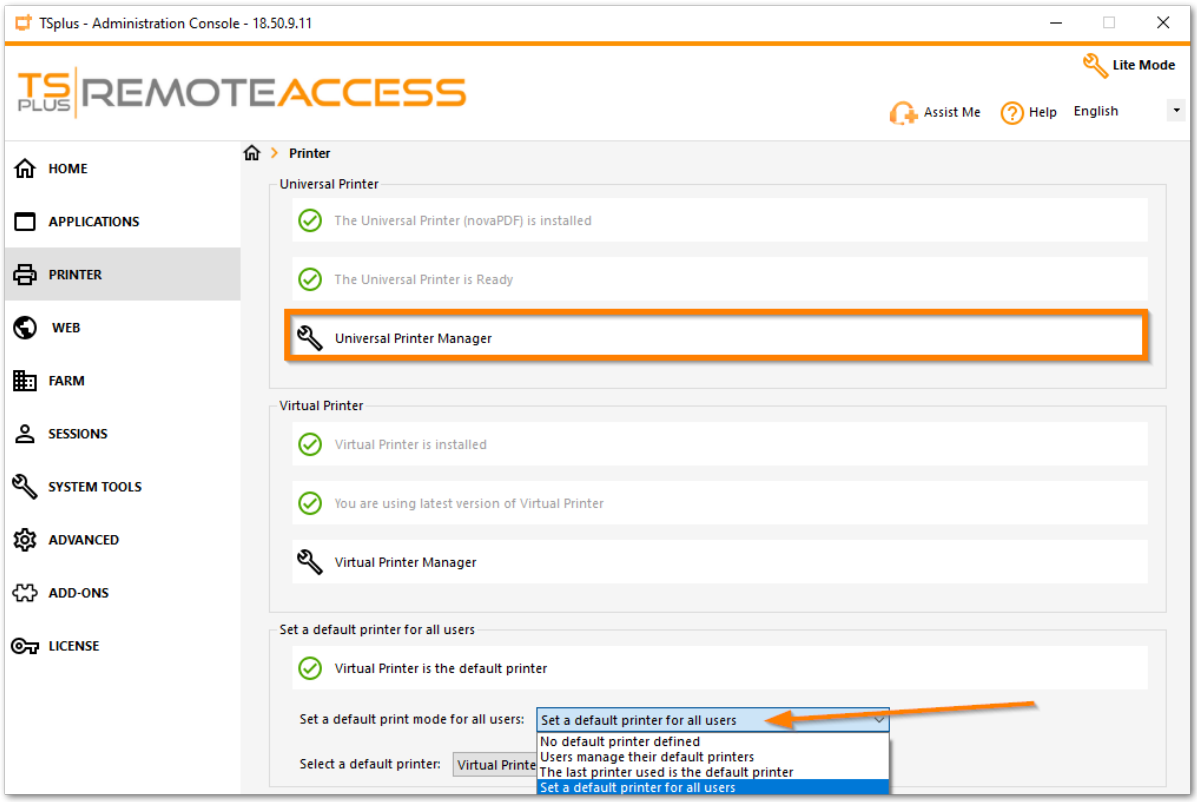
Solo **haga clic en un mosaico o en una pestaña** ¡Ir a la ayuda correspondiente!



Haga clic para ayudar - Herramienta de administración - Impresora

¿Quieres obtener ayuda sobre una función de Terminal Service Plus Admin Tool rápidamente?

Solo **haga clic en un mosaico o en una pestaña** ¡Ir a la ayuda correspondiente!



Clic para ayudar - Herramienta de administración - Seguridad

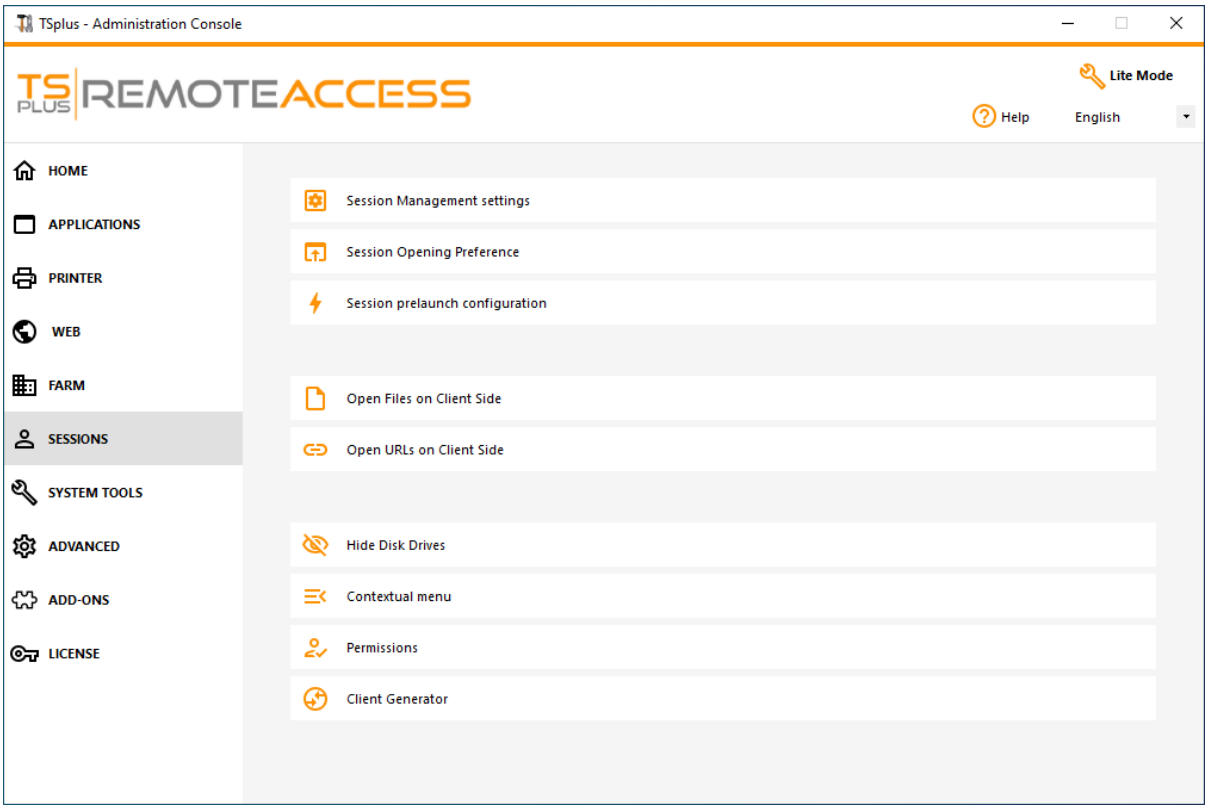
¿Quieres obtener ayuda sobre una función de Terminal Service Plus Admin Tool rápidamente?

Solo **haga clic en un mosaico o en una pestaña** ¡Ir a la ayuda correspondiente!

Clic para ayudar - Herramienta de administración - Sesiones

¿Quieres obtener ayuda sobre una función de Terminal Service Plus Admin Tool rápidamente?

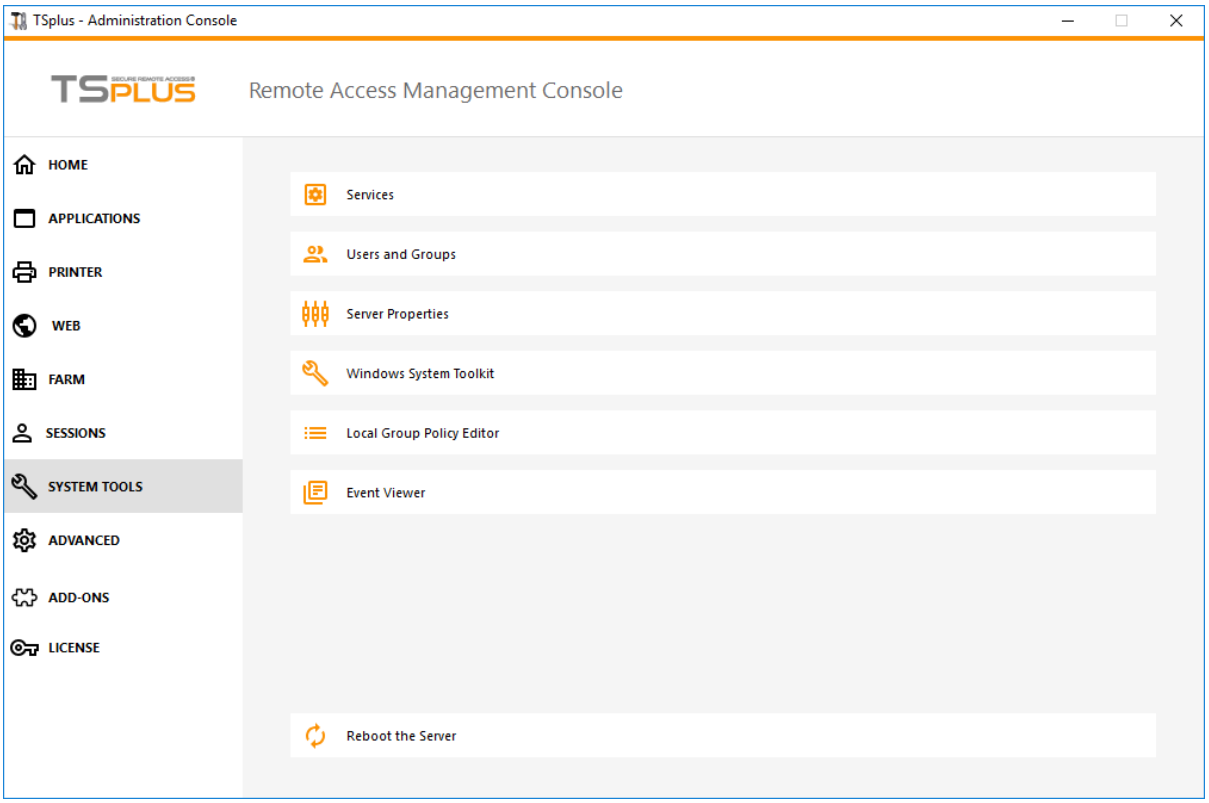
Solo **haga clic en un mosaico o en una pestaña** ¡Ir a la ayuda correspondiente!



Clic para ayudar - Herramienta de administración - Sistema

¿Quieres obtener ayuda sobre una función de Terminal Service Plus Admin Tool rápidamente?

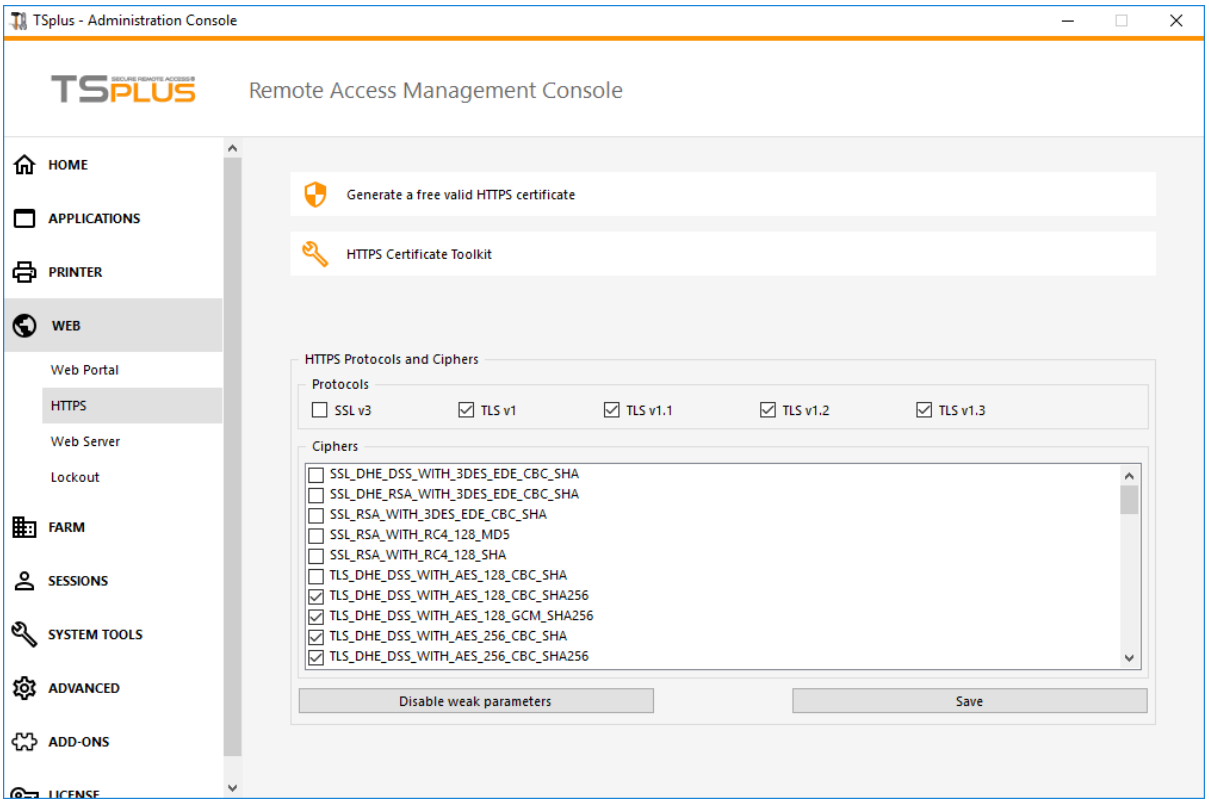
Solo **haga clic en un mosaico o en una pestaña** ¡Ir a la ayuda correspondiente!



Clic para ayudar - Herramienta de administración - Web

¿Quieres obtener ayuda sobre una función de Terminal Service Plus Admin Tool rápidamente?

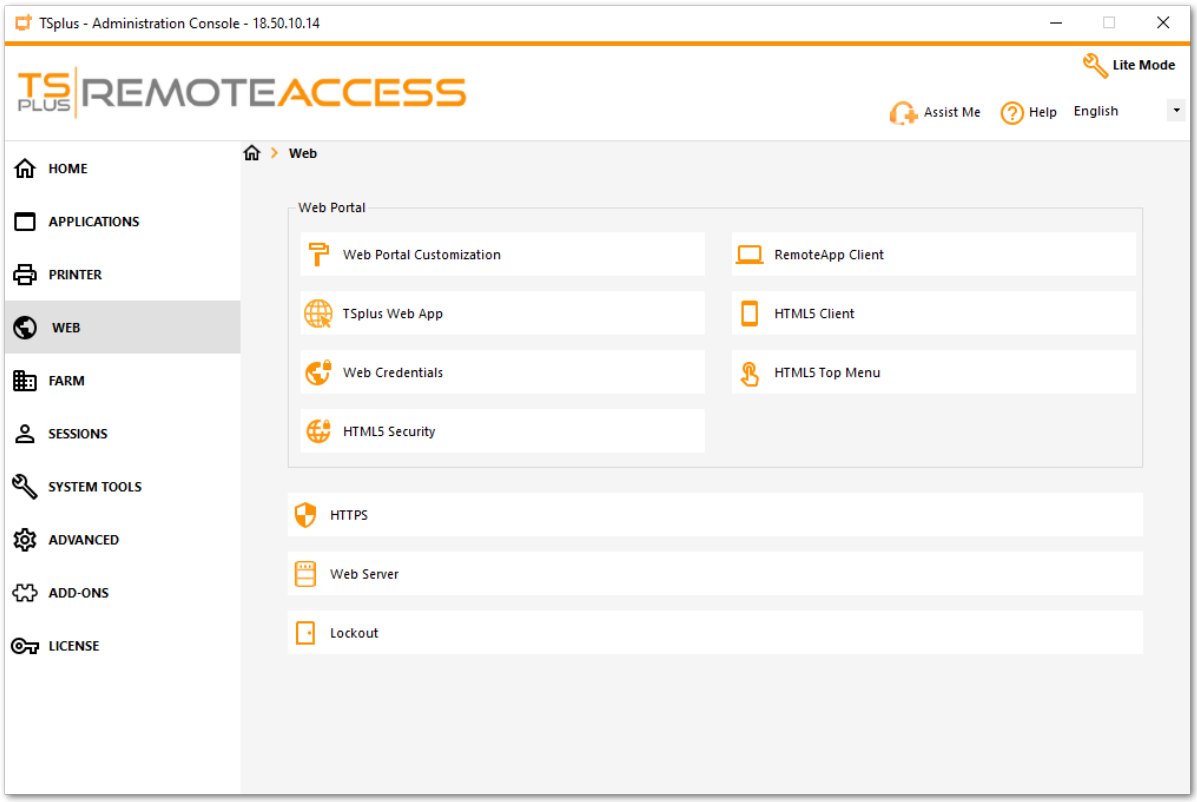
Solo **haga clic en un mosaico o en una pestaña** ¡Ir a la ayuda correspondiente!



Clic para ayudar - Herramienta de administración - Web

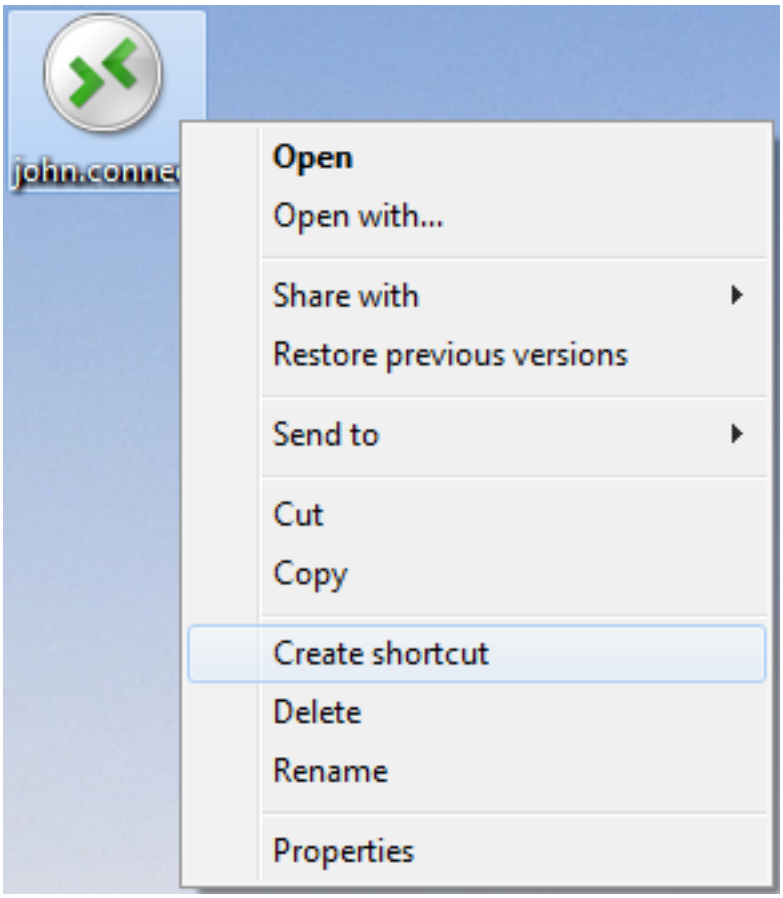
¿Quieres obtener ayuda sobre una función de Terminal Service Plus Admin Tool rápidamente?

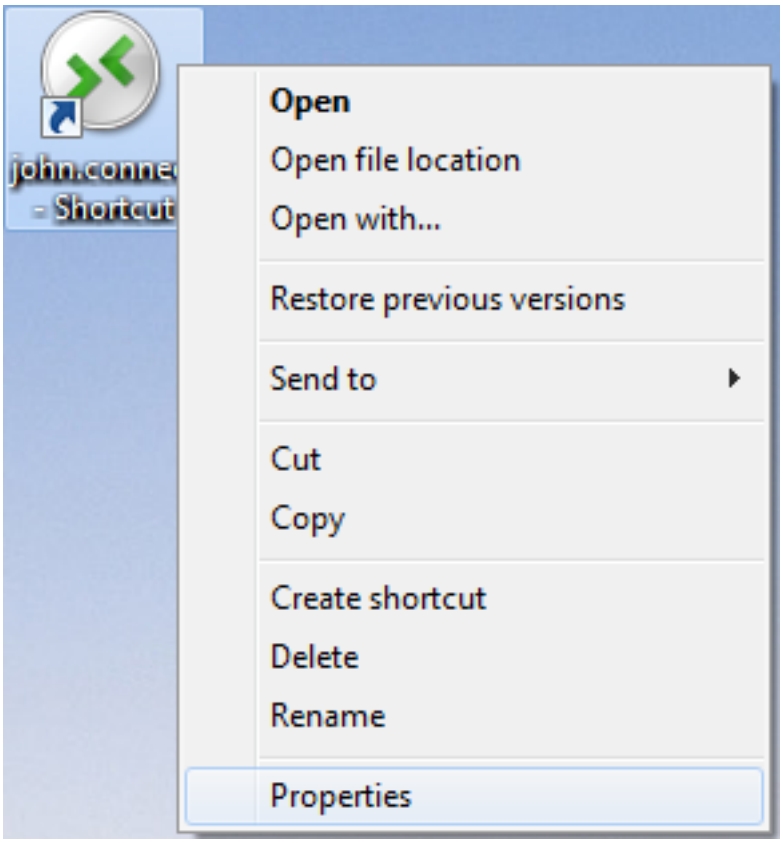
Solo **haga clic en un mosaico o en una pestaña** ¡Ir a la ayuda correspondiente!

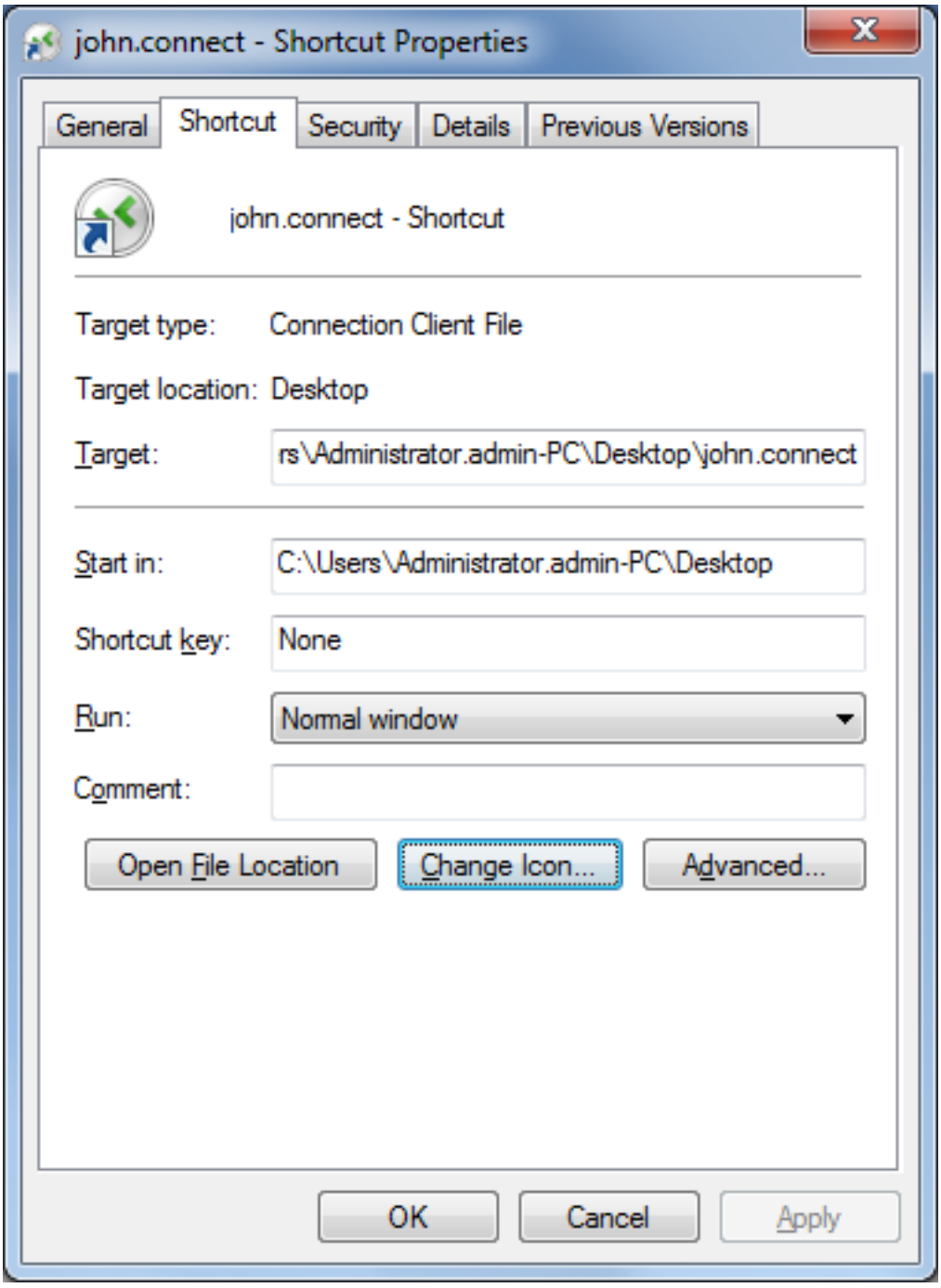


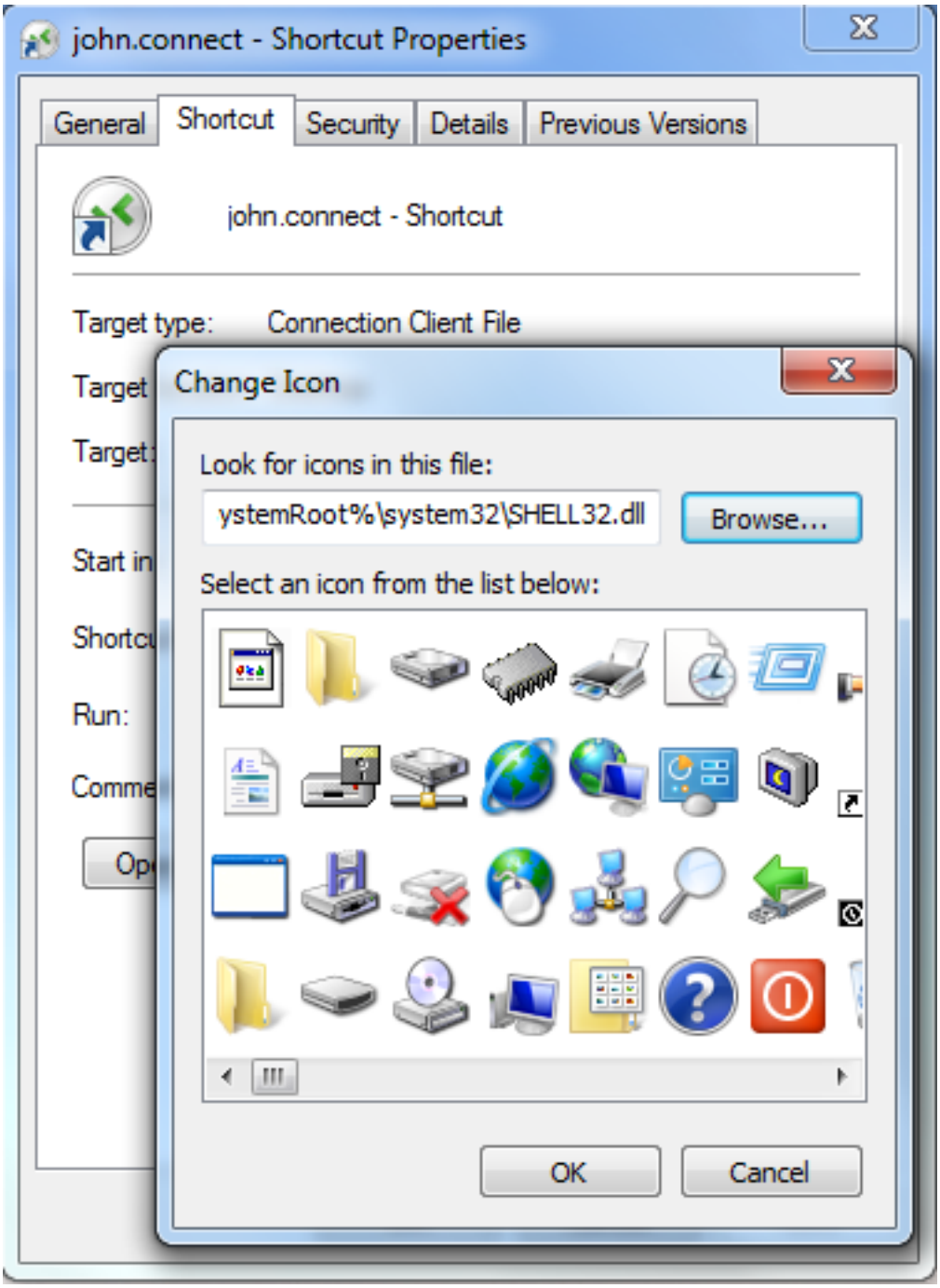
Cómo modificar el icono del cliente de TSplus

Para cambiar el ícono del cliente generado, simplemente crea un acceso directo del cliente y ve a las propiedades del acceso directo:




john.connec
- Shortcut
Open
Open file location
Open with...
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties


john.connect - Shortcut Properties
General
Shortcut
Security
Details
Previous Versions
john.connect - Shortcut
Target type: Connection Client File
Target location: Desktop
Target: rs\Administrator.admin-PC\Desktop\john.connect
Start in: C:\Users\Administrator.admin-PC\Desktop
Shortcut key: None
Run: Normal window
Comment:
Open File Location
Change Icon...
Advanced...
OK
Cancel
Apply

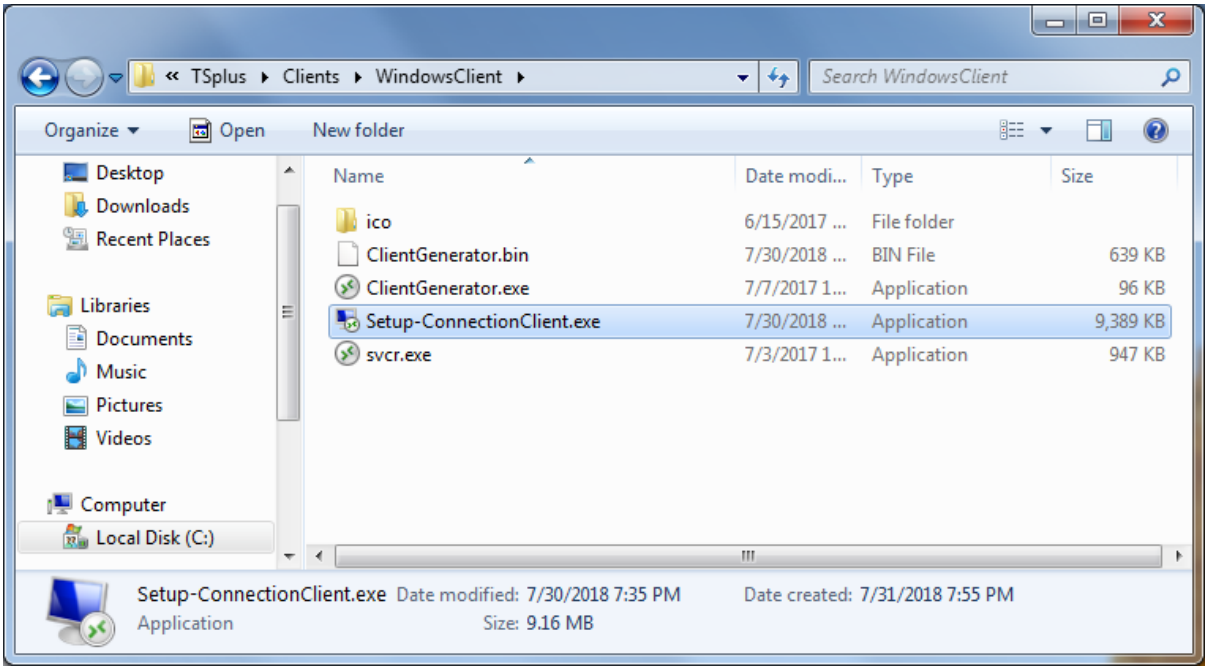

john.connect - Shortcut Properties
General
Shortcut
Security
Details
Previous Versions
john.connect - Shortcut
Target type:
Connection Client File
Target
Target:
Start in
Shortcu
Run:
Comme
Op
Change Icon
Look for icons in this file:
ystemRoot%\system32\SHELL32.dll
Browse...
Select an icon from the list below:
OK
Cancel

TSplus Client Setup program

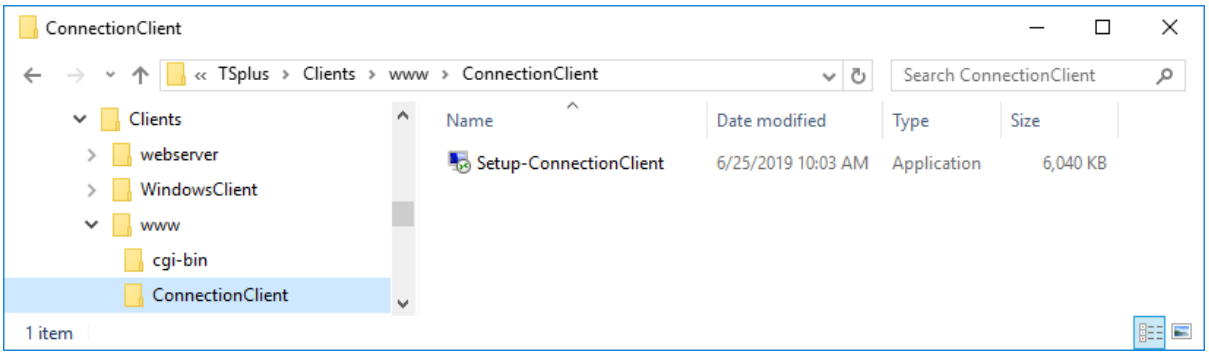
Instalar

En el lado del cliente, **cada usuario tendrá que ejecutar un programa firmado llamado "Setup-ConnectionClient.exe" como requisito previo** .

Este programa está disponible en su servidor, en la carpeta del programa TSplus: C:\Program Files (x86)\TSplus\Clients\WindowsClient:



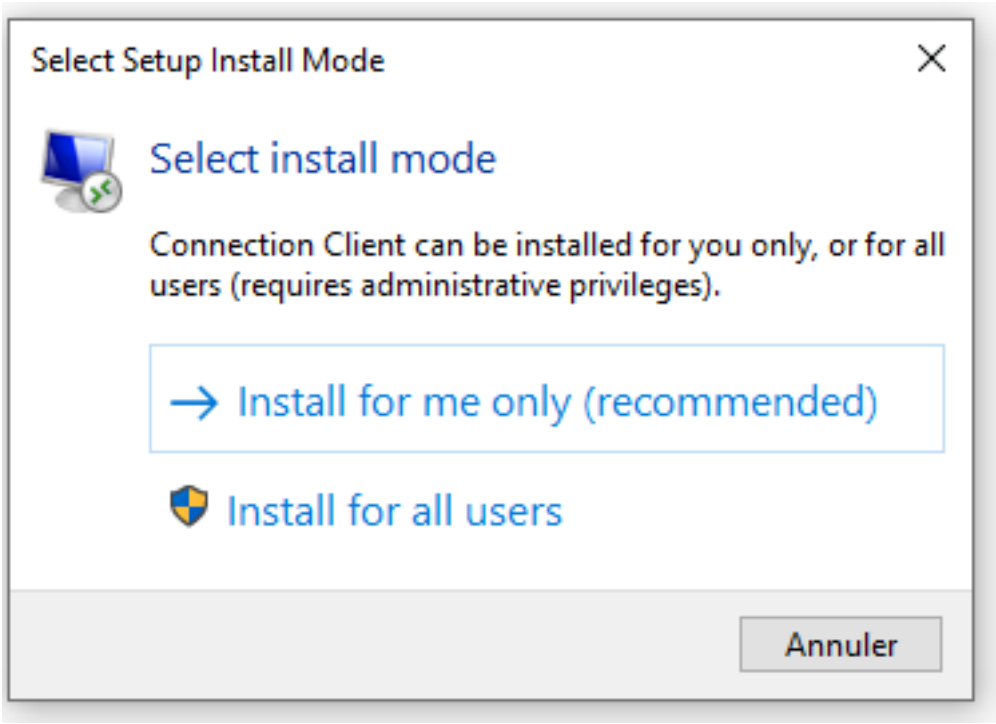
También está disponible en C:\Program Files (x86)\TSplus\Clients\www\ConnectionClient, por lo que sus usuarios pueden ejecutar el programa una vez en la dirección de su servidor web: http://xxxxxxxxxx/ConnectionClient/Setup-ConnectionClient.exe



o por descargándolo .

Instalar para todos los usuarios

Ahora puede instalar el Cliente de Conexión para todos los usuarios. Esto significa que, una vez instalado, cualquier usuario en la computadora se beneficiará de él y podrá conectarse en modo remoteApp desde el Portal Web, así como con un archivo de cliente .connect generado.



Nota: Para que este pop-up aparezca, no debe tener ya instalado el Cliente de Conexión. También puede, durante una instalación utilizando la línea de comandos, especificar qué modo desea usar con el argumento /ALLUSERS o /CURRENTUSER para instalar respectivamente para todos los usuarios o para el usuario actual.

Nota Desde TSplus 12.40, el Programa de Configuración del Cliente y el Configuración del cliente RemoteApp se han fusionado y se pueden implementar con una sola configuración, por lo que si descargas la configuración del cliente de conexión, no será necesario descargar la del

cliente de RemoteApp.

Identificador de hardware y servidor clonado

1- Cambio de identificador de hardware.

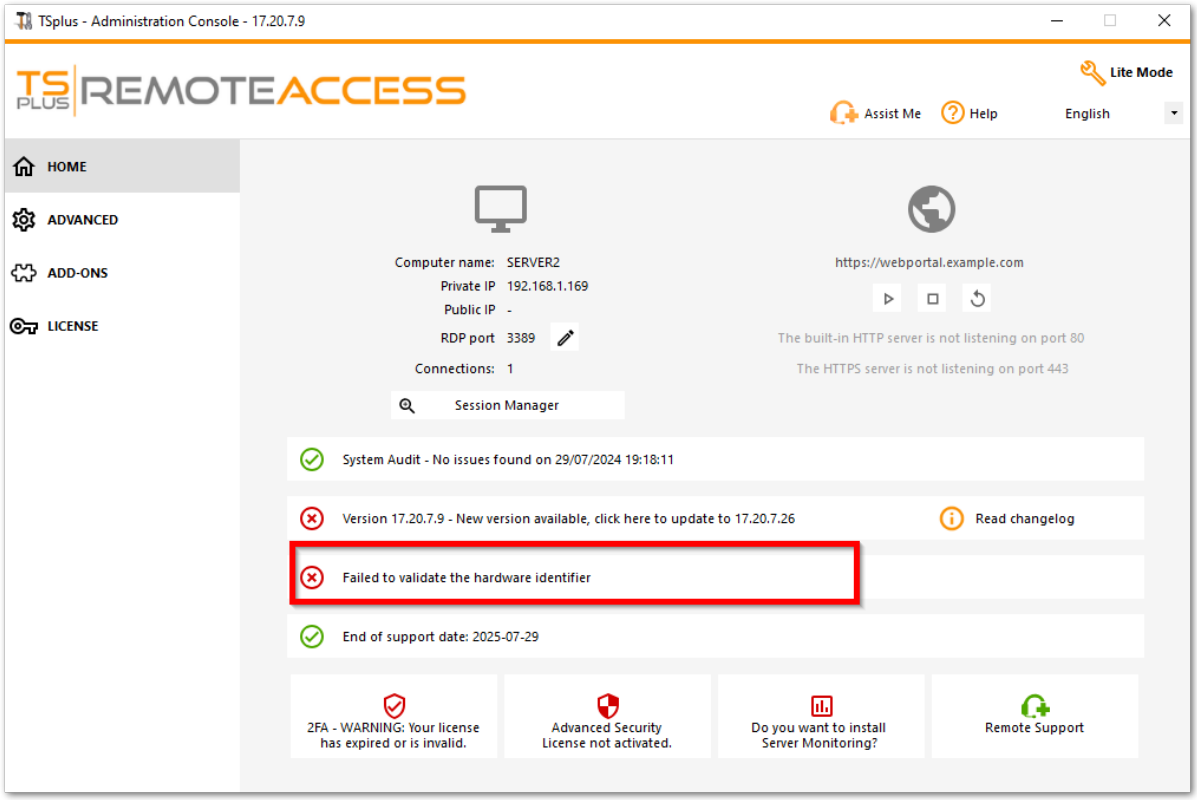
Reparar el identificador de hardware tras la clonación o una actualización.

Advertencia: No se pudo validar el identificador de hardware

Después de migrar un servidor físico a una máquina virtual o una actualización de Kernel de Microsoft, el estado de la licencia cambia a Fallido al validar el identificador de hardware en nuevo hardware.

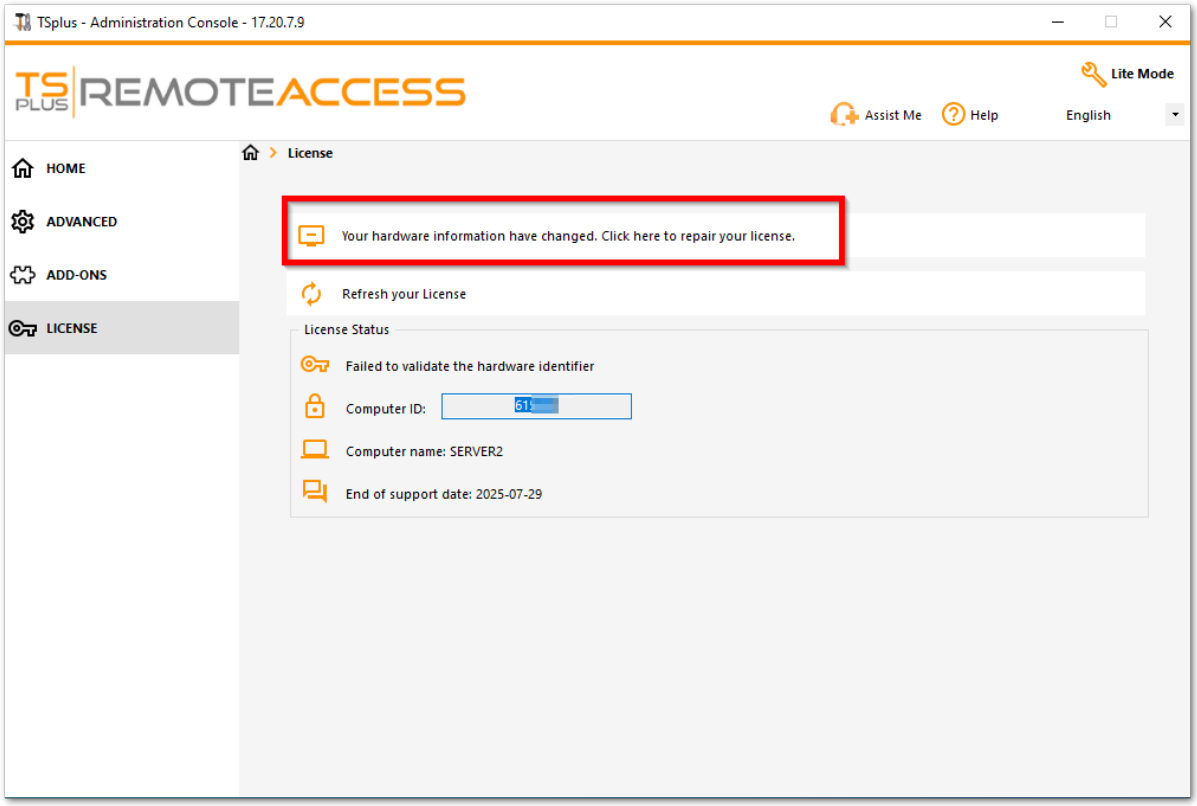
Este mensaje aparece porque TSplus ha detectado un conflicto de licencia copiado de un servidor a otro con el mismo ID de computadora y el mismo nombre.
Ya recomendamos renombrar su nuevo servidor (Ejemplo: SERVER1 > SERVER2)

- Reinicie su servidor



Haz clic en la ventana para llegar a la página de licencia.

Luego haga clic en la pestaña "Su información de hardware ha cambiado. Haga clic aquí para reparar su licencia.



Se abrirá una ventana emergente de "rehospedaje de licencia" para permitirle restaurar su licencia.

Caso 1: ¡No tienes soporte!
La rehosting, por lo tanto, no será posible; tendrás que suscribirte a una suscripción de soporte en el servidor original y comenzar nuevamente la acción de migración.
En caso de problemas, Contact Support y indique su ID de computadora y clave de activación.

Caso 2: ¡Ya has rehosted durante 6 meses!
El mensaje: Ya has reubicado esta computadora en los últimos 6 meses. Por favor, contacta con Soporte si necesitas ayuda para reubicar tu licencia.

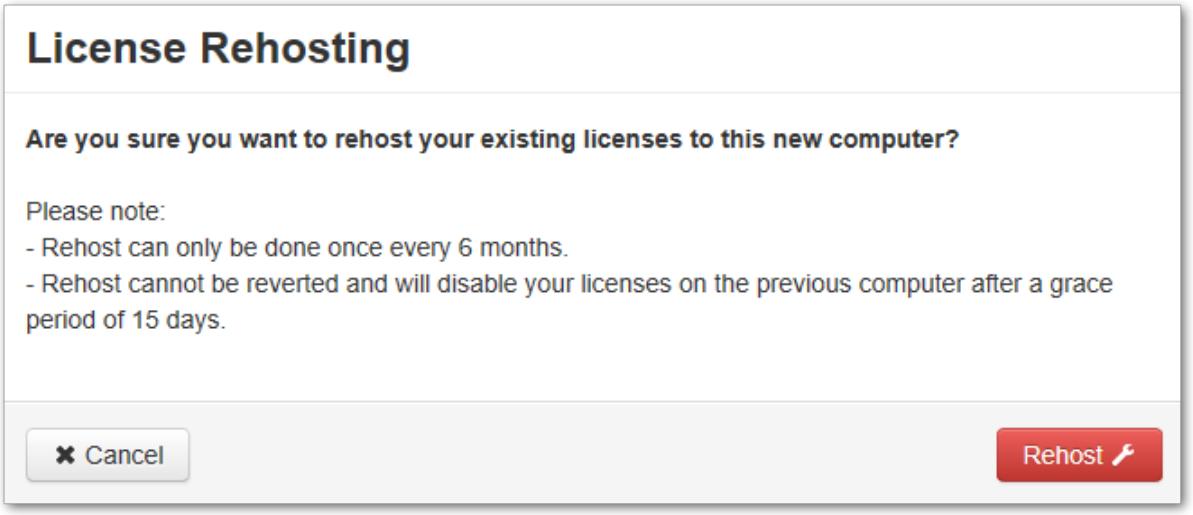
La reubicación, por lo tanto, no será posible, Contact Support y indique su ID de computadora y clave de activación.

Caso 3: ¡Tienes soporte!
El siguiente mensaje aparece: ¿Está seguro de que desea reubicar sus licencias existentes en esta nueva computadora?

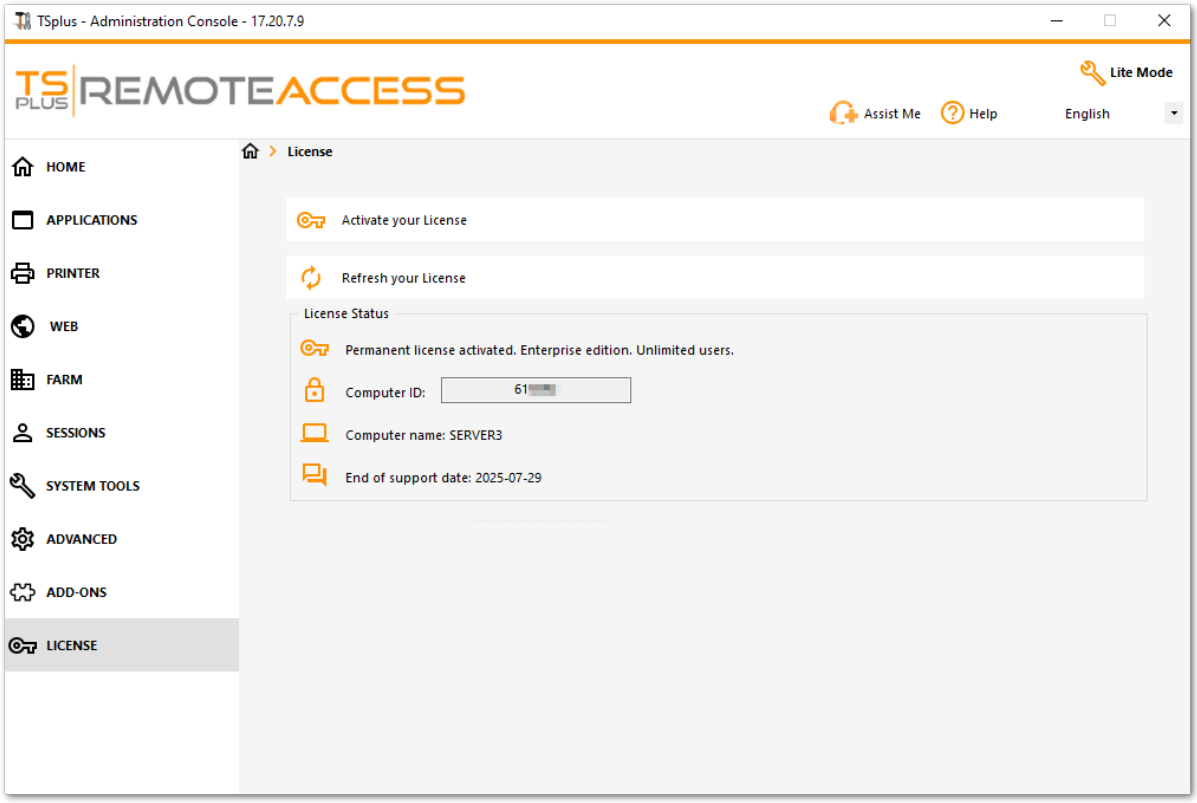
Por favor, tenga en cuenta:

- La reubicación solo se puede realizar una vez cada 6 meses.
- La reubicación no se puede cancelar y desactivará sus licencias en la computadora anterior después de un período de gracia de 15 días.

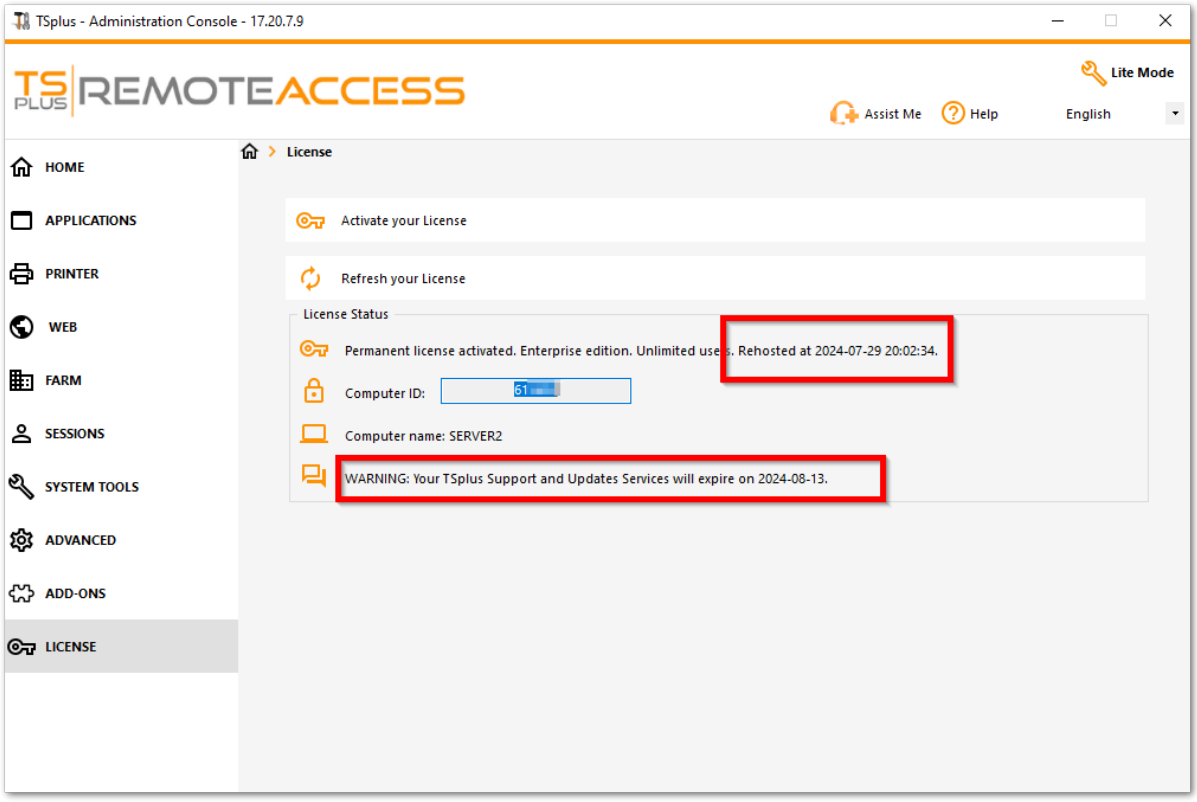
Haga clic en el **"REHOST"** botón



¡Su licencia está reubicada!



Nota: Aparecerá un mensaje en el servidor antiguo con la fecha de rehosting así como la fecha de finalización del período de uso del servidor antiguo (15 días).



Error de actualización:

Ejecute la actualización y verifique si esto ha resuelto su problema después de reiniciar su servidor.

- Descargar el Actualización de la versión

2- Clonar un servidor mientras se mantiene el servidor existente y se activa una nueva licencia.

Requisitos

Al trabajar con máquinas virtuales clonadas, es importante modificar el nombre del equipo y el ID del volumen del disco para garantizar una instalación única de TSplus Remote Access y evitar problemas de licencia.

Consideraciones sobre el nombre del ordenador

El nombre de la computadora se almacena en el registro de Windows dentro de la imagen misma. Si se modifica antes de aplicar la imagen, será sobrescrito por Sysprep cuando Windows se inicie. Sin embargo, puedes predefinir un nombre en un Unattended.xml Archivo de respuesta. Ver Documentación de Microsoft para más detalles.

Para establecer el nombre del equipo, agregue la siguiente sección dentro de Microsoft-Windows-Shell-Setup :

```
    <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
        <ComputerName>%COMPUTERNAME%ComputerName>
    component>
```

Consideraciones sobre el ID de volumen

El ID de volumen está asociado con la partición del disco, no con la imagen del sistema operativo. Se puede cambiar antes de aplicar la imagen, y persistirá. Utilice volumeid.exe de Sysinternals, disponible en Microsoft Sysinternals antes de que Windows se inicie.

Pasos de implementación

Al implementar una nueva máquina virtual a partir de una imagen preparada con sysprep, Windows ingresará a la Experiencia de Configuración Inicial (OOBE) en el primer arranque, solicitando la configuración de ajustes.

Pasos recomendados para la implementación:

1. **Arrancar en WinPE** – Prepare el sistema sin iniciar en Windows.
2. **Establecer el ID de volumen** – Cámbialo antes de aplicar la imagen para que persista.
3. **Desplegar la imagen sysprepped** – Utilice DISM para aplicar la imagen a C: .
4. **Establecer el nombre del equipo sin conexión** – Edite el registro dentro de la imagen montada.
5. **Copiar un Unattended.xml archivo** – Automatizar la configuración OOBE. Este archivo se puede modificar dinámicamente antes de la implementación utilizando un script.
6. **Crear un script de primer arranque** – Asegúrese de que las configuraciones finales se realicen con un solo reinicio.
7. **Reiniciar en Windows** – Windows se finaliza utilizando las configuraciones especificadas.
8. **Restablecer la licencia de acceso remoto** – Ejecute el siguiente comando:

Ventana de terminal

AdminTool.exe /license /reset

Esto restablece la licencia y aplica una nueva licencia.

Script de implementación

Por favor, encuentre a continuación el script de implementación de WinPE relacionado.

Ventana de terminal

```
<# Define variables #>
$ImagePath = "D:\Images\Windows.wim"   # Path to your sysprepped image
$ApplyDrive = "C:"                     # Target drive for deployment
$ComputerName = "REMOTE ACCESS-SERVER-" + (Get-Random -Minimum 1000 -
Maximum 9999)  # Generate a random name (naive implementation)
$VolumeID = "1234-ABCD"                # Desired Volume Serial Number
$UnattendFile = "D:\Unattended.xml"    # Path to the unattended answer file

Write-Host "=== Windows Deployment Automation ==="

<# 1. Set Volume ID before applying the image #>
Write-Host "Setting Volume ID..."
Start-Process -NoNewWindow -Wait -FilePath "volumeid.exe" -ArgumentList "$ApplyDrive
$VolumeID"

<# 2. Apply the Sysprepped Windows image #>
Write-Host "Applying Windows Image..."
dism /apply-image /imagefile:$ImagePath /index:1 /applydir:$ApplyDrive

<# 3. Load Registry Offline to Set Computer Name #>
Write-Host "Modifying Registry to Set Computer Name..."
reg load HKLM\TempSys $ApplyDrive\Windows\System32\Config\SYSTEM
reg add "HKLM\TempSys\ControlSet001\Control\ComputerName\ComputerName" /v
ComputerName /t REG_SZ /d "$ComputerName" /f
reg unload HKLM\TempSys

<# 4. Ensure Unattended Setup is Used #>
Write-Host "Copying Unattended File..."
Copy-Item -Path $UnattendFile -Destination "$ApplyDrive\Windows\Panther\Unattended.xml" -
Force

<# 5. Set the First Boot Script for Final Configurations #>
Write-Host "Creating First Boot Script..."
$FirstBootScript = @"
Write-Host "Finalizing Configuration..."
Rename-Computer -NewName "$ComputerName" -Force
```

```
    Restart-Computer -Force
    "@
    Set-Content -Path "$ApplyDrive\Windows\Setup\Scripts\SetupComplete.cmd" -Value
$FirstBootScript -Encoding ASCII

    Write-Host "Deployment Complete! Rebooting into Windows..."
    Write-Host "================================================"
    Write-Host "  Computer Name: $ComputerName"
    Write-Host "  Volume ID: $VolumeID"
    Write-Host "  Image Applied to: $ApplyDrive"
    Write-Host "================================================"

    <# Reboot into Windows #>
    wpeutil reboot
```

Activación de licencias

Después de la implementación, activar una licencia generará un nuevo ID de computadora para la máquina virtual. Este ID de computadora es creado por el portal de licencias cuando una máquina solicita una prueba o activación de licencia. Para las máquinas virtuales clonadas, la activación de la licencia es obligatoria. Utilice una clave de activación o una clave de licencia por volumen. **Las configuraciones fuera de línea no están permitidas** debido a preocupaciones de seguridad. Para obtener pasos de activación detallados, consulte Lista de comandos de TSplus .

Conclusión

Esta guía describe las consideraciones clave para implementar máquinas virtuales clonadas con TSplus Remote Access. Proporciona pasos esenciales para configurar y licenciar el sistema correctamente y debe adaptarse a sus necesidades y requisitos.

Clonación de servidores utilizando sysprep

Requisitos

Al trabajar con máquinas virtuales clonadas, es importante modificar el nombre del equipo y el ID del volumen del disco para garantizar una instalación única de TSplus Remote Access y evitar problemas de licencia.

Consideraciones sobre el nombre del ordenador

El nombre de la computadora se almacena en el registro de Windows dentro de la imagen misma. Si se modifica antes de aplicar la imagen, será sobrescrito por Sysprep cuando Windows se inicie. Sin embargo, puedes predefinir un nombre en un Unattended.xml Archivo de respuesta. Ver Documentación de Microsoft para más detalles.

Para establecer el nombre del equipo, agregue la siguiente sección dentro de Microsoft-Windows-Shell-Setup :

```
    <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
        <ComputerName>%COMPUTERNAME%ComputerName>
    component>
```

Consideraciones sobre el ID de volumen

El ID de volumen está asociado con la partición del disco, no con la imagen del sistema operativo. Se puede cambiar antes de aplicar la imagen, y persistirá. Utilice `volumeid.exe` de Sysinternals, disponible en Microsoft Sysinternals antes de que Windows se inicie.

Pasos de implementación

Al implementar una nueva máquina virtual a partir de una imagen preparada con sysprep, Windows ingresará a la Experiencia de Configuración Inicial (OOBE) en el primer arranque, solicitando la configuración de ajustes.

Pasos recomendados para la implementación:

1. **Arrancar en WinPE** – Prepare el sistema sin iniciar en Windows.
2. **Establecer el ID de volumen** – Cámbialo antes de aplicar la imagen para que persista.
3. **Desplegar la imagen sysprepped** – Utilice DISM para aplicar la imagen a `C:` .
4. **Establecer el nombre del equipo sin conexión** – Edite el registro dentro de la imagen montada.
5. **Copiar un `Unattended.xml` archivo** – Automatizar la configuración OOBE. Este archivo se puede modificar dinámicamente antes de la implementación utilizando un script.
6. **Crear un script de primer arranque** – Asegúrese de que las configuraciones finales se realicen con un solo reinicio.
7. **Reiniciar en Windows** – Windows se finaliza utilizando las configuraciones especificadas.
8. **Restablecer la licencia de acceso remoto** – Ejecute el siguiente comando:

Ventana de terminal

```
AdminTool.exe /license /reset
```

Esto restablece la licencia y aplica una nueva licencia.

Script de implementación

Por favor, encuentre a continuación el script de implementación de WinPE relacionado.

Ventana de terminal

```
<# Define variables #>
$ImagePath = "D:\Images\Windows.wim"   # Path to your sysprepped image
$ApplyDrive = "C:"                     # Target drive for deployment
$ComputerName = "REMOTE ACCESS-SERVER-" + (Get-Random -Minimum 1000 -
Maximum 9999)  # Generate a random name (naive implementation)
$VolumeID = "1234-ABCD"                # Desired Volume Serial Number
$UnattendFile = "D:\Unattended.xml"    # Path to the unattended answer file

Write-Host "=== Windows Deployment Automation ==="

<# 1. Set Volume ID before applying the image #>
Write-Host "Setting Volume ID..."
Start-Process -NoNewWindow -Wait -FilePath "volumeid.exe" -ArgumentList "$ApplyDrive
$VolumeID"

<# 2. Apply the Sysprepped Windows image #>
Write-Host "Applying Windows Image..."
dism /apply-image /imagefile:$ImagePath /index:1 /applydir:$ApplyDrive

<# 3. Load Registry Offline to Set Computer Name #>
Write-Host "Modifying Registry to Set Computer Name..."
reg load HKLM\TempSys $ApplyDrive\Windows\System32\Config\SYSTEM
reg add "HKLM\TempSys\ControlSet001\Control\ComputerName\ComputerName" /v
ComputerName /t REG_SZ /d "$ComputerName" /f
reg unload HKLM\TempSys

<# 4. Ensure Unattended Setup is Used #>
Write-Host "Copying Unattended File..."
Copy-Item -Path $UnattendFile -Destination "$ApplyDrive\Windows\Panther\Unattended.xml" -
Force

<# 5. Set the First Boot Script for Final Configurations #>
Write-Host "Creating First Boot Script..."
$FirstBootScript = @"
Write-Host "Finalizing Configuration..."
Rename-Computer -NewName "$ComputerName" -Force
```

```
    Restart-Computer -Force
    "@
    Set-Content -Path "$ApplyDrive\Windows\Setup\Scripts\SetupComplete.cmd" -Value
$FirstBootScript -Encoding ASCII

    Write-Host "Deployment Complete! Rebooting into Windows..."
    Write-Host "================================================"
    Write-Host "  Computer Name: $ComputerName"
    Write-Host "  Volume ID: $VolumeID"
    Write-Host "  Image Applied to: $ApplyDrive"
    Write-Host "================================================"

    <# Reboot into Windows #>
    wpeutil reboot
```

Activación de licencias

Después de la implementación, activar una licencia generará un nuevo ID de computadora para la máquina virtual. Este ID de computadora es creado por el portal de licencias cuando una máquina solicita una prueba o activación de licencia. Para las máquinas virtuales clonadas, la activación de la licencia es obligatoria. Utilice una clave de activación o una clave de licencia por volumen. **Las configuraciones fuera de línea no están permitidas** debido a preocupaciones de seguridad. Para obtener pasos de activación detallados, consulte Lista de comandos de TSplus .

Conclusión

Esta guía describe las consideraciones clave para implementar máquinas virtuales clonadas con TSplus Remote Access. Proporciona pasos esenciales para configurar y licenciar el sistema correctamente y debe adaptarse a sus necesidades y requisitos.

Líneas de comando

Estamos complacidos de proporcionarle un conjunto completo de herramientas de línea de comandos diseñadas para mejorar la flexibilidad y eficiencia de nuestro software. Estas herramientas permiten a los usuarios crear scripts y automatizar diversas funcionalidades, adaptando el software para satisfacer sus necesidades y flujos de trabajo específicos.

Explora las posibilidades y optimiza tu experiencia con nuestras opciones de línea de comandos.

Solo tienes que ejecutar las siguientes líneas de comando como un Administrador elevado. Como recordatorio, AdminTool.exe y TwoFactor.Admin.exe (complemento 2FA) deben estar ubicados aquí: **C:\Program Files (x86)\TSplus\UserDesktop\files**

Copia de seguridad de datos y configuraciones: /backup

Sintaxis:

AdminTool.exe /backup [rutaOpcional] [parámetros]

Descripción:

Comando /backup se utiliza para respaldar los datos y configuraciones de TSplus.

Por defecto, la copia de seguridad se creará en el directorio de archivos (C:\Backupparam)

Parámetros:

- rutaOpcional para hacer una copia de seguridad en otro directorio que no sea el predeterminado. Se permiten rutas relativas y absolutas.

- /silencio si se menciona este parámetro, la copia de seguridad se realiza en silencio

Ejemplos:

AdminTool.exe /backup AdminTool.exe /backup “c:/TSplus/CustomBackupFolder” /silent

Para más información, por favor visite TSplus - Configuración de Copia de Seguridad

Restaurar datos y configuraciones: /restaurar

Sintaxis:

AdminTool.exe /restore [rutaDeCopiaDeSeguridad] [parámetros]

Descripción:

Comando /restaurar se utiliza para restaurar los datos y configuraciones de TSplus.

El directorio de respaldo especificado debe contener una carpeta de datos y una carpeta de configuraciones, como se creó con el comando /backup.

Parámetros:

- rutaDeCopiaDeSeguridad la ruta donde se encuentra la carpeta de respaldo para restaurar.
- /silencio si se menciona este parámetro, la restauración se realiza en silencio

Ejemplos:

AdminTool.exe /restore “C:/Backupparam” /silent AdminTool.exe /restore “C:/TSplus/CustomBackupFolder” /silent

Para más información, por favor visite TSplus - Configuración de Copia de Seguridad

Servidor web: /webstop , /webstart y /

webrestart

Sintaxis:

AdminTool.exe /webstop

AdminTool.exe /webstart

AdminTool.exe /webrestart

Descripción:

Comando /webstop se utiliza para detener el servidor web.

Comando /webstart se utiliza para iniciar el servidor web.

Comando /webrestart se utiliza para reiniciar el servidor web.

Parámetros:

Ninguno

Actualización: /actualizar

Sintaxis:

AdminTool.exe /actualizar [opciones]

Descripción:

Comando actualizar se utiliza para actualizar TSplus Remote Access y potencialmente Advanced Security.

Parámetros:

-

opciones
:

- /añadidos si se utiliza esta opción, Advanced Security también se actualiza, si hay una nueva versión disponible.

Ejemplo:

AdminTool.exe /actualizar /complementos

Aplicar actualizaciones de compatibilidad de Windows: /actualizarkernel

Sintaxis:

svcac.exe /updatekernel [/silencioso]

svcac.exe debe estar ubicado aquí: **C:\Program Files (x86)\TSplus**

Descripción:

Comando /actualizarkernel se utiliza para aplicar actualizaciones de compatibilidad de Windows.

Estas actualizaciones automáticas garantizan que TSplus Remote Access siga siendo compatible con las nuevas actualizaciones de Windows y evitan la necesidad de descargar e reinstalar una versión más nueva de TSplus Remote Access.

Las actualizaciones de compatibilidad de Windows pueden ocurrir a diario. TSplus Remote Access permite actualizaciones forzadas. Esto es útil cuando la compatibilidad parece estar rota y necesitas recuperar el último parche de TSplus Remote Access fuera del horario regular de actualizaciones.

Tenga en cuenta que se requiere una licencia válida para obtener actualizaciones de compatibilidad. Si su licencia de prueba ha expirado o si su licencia es inválida, se mostrará un cuadro de mensaje de error. Comuníquese con nuestro equipo de soporte con una captura de pantalla de este mensaje de error si el problema es inesperado.

Parámetros:

- /silencio Actualice silenciosamente proporcionando este parámetro. No se mostrará ningún cuadro de mensaje.

Instalar Impresora Universal: Instalar Impresora Universal

Sintaxis:

universalprintermanagement.exe /InstallUniversalPrinter

universalprintermanagement.exe se encuentra aquí: **C:\Program Files (x86)\TSplus\UserDesktop\files**

Descripción:

Comando Instalar Impresora Universal se utiliza para instalar Universal Printer.

Esta es una instalación limpia ya que elimina la impresora universal existente si se había instalado anteriormente.

Parámetros:

Ninguno

También puede realizar esta acción manualmente, por favor mire en Impresora Universal

---

Eliminar UniversalPrinter: EliminarImpresoraUniversal

Sintaxis:

universalprintermanagement.exe /RemoveUniversalPrinter

universalprintermanagement.exe se encuentra aquí: **C:\Program Files (x86)\TSplus\UserDesktop\files**

Descripción:

Comando EliminarImpresoraUniversal se utiliza para desinstalar Universal Printer.

Parámetros:

Ninguno

También puede realizar esta acción manualmente, por favor mire en Impresora Universal

---

Configurar servidor proxy: /proxy /set

Sintaxis:

AdminTool.exe /proxy /set [parámetros]

Descripción:

Comando /proxy /set se utiliza para configurar un servidor proxy para el acceso a Internet.

Parámetros:

- /host el host de destino puede ser un valor predefinido (“ie” o “none”) o un valor definido por el usuario (por ejemplo: 127.0.0.1 o proxy.company.org). Este parámetro es obligatorio
- /puerto el número de puerto utilizado para conectarse al servidor proxy. Requerido si el valor del nombre de host es un valor definido por el usuario personalizado.
- /usuario el nombre de usuario para conectarse al servidor proxy. Esta configuración es opcional
- /contraseña la contraseña del usuario debe ser proporcionada si se ha definido un nombre de usuario. Sin embargo, su valor puede estar vacío

Ejemplos:

AdminTool.exe /proxy /set /host proxy.company.org /port 80 /username dummy /password

pass@word1

AdminTool.exe /proxy /set /host ie

Para más información, por favor visite ¿Cómo configurar un servidor proxy para el acceso a Internet?

Abrir formulario de credenciales web: /webcredentials

Sintaxis:

AdminTool.exe /webcredentials

Descripción:

Comando /webcredentials lanza en una sola ventana la interfaz de Credenciales Web (como lo harías en AdminTool > Web > Credenciales Web).

Parámetros:

Ninguno

Crear credenciales web: /webcredentials-agregar

Sintaxis:

AdminTool.exe /webcredentials-add [webLogin] [webPassword] [windowsLogin] [windowsPassword] [maximumConcurrentSessions]

Descripción:

Comando /webcredentials-agregar se utiliza para crear Credenciales Web (como harías en AdminTool > Web > Credenciales Web).

Parámetros:

- inicio de sesión web el inicio de sesión web que desea crear.
- contraseñaWeb la contraseña web asociada. Puede ser una credencial en blanco. Para eso, use comillas dobles "" para indicar una contraseña en blanco.
- inicio de sesión de Windows el inicio de sesión de Windows del usuario correspondiente.
- contraseñaDeWindows la contraseña de Windows.
- sesionesConcurrentesMáximas (opcional): el número máximo de sesiones concurrentes para este usuario.

Ejemplo:

AdminTool.exe /webcredentials-add johndoe passwordABCD johnWinuser johnWinpassword 4

Para más información, por favor visite Credenciales Web

Eliminar credenciales web: /webcredentials-remove

Sintaxis:

AdminTool.exe /webcredentials-remove [webLogin]

Descripción:

Comando /webcredentials-remove se utiliza para eliminar una Credencial Web existente (como harías en AdminTool > Web > Credenciales Web).

Parámetros:

- inicio de sesión web el inicio de sesión web que desea eliminar.

Ejemplo:

AdminTool.exe /webcredentials-remove johndoe

Para más información, por favor visite Credenciales Web

Administrador de Sesiones Abiertas: /sessionmanager

Sintaxis:

AdminTool.exe /sessionmanager

Descripción:

Comando /sessionmanager lanza en una única ventana de tamaño considerable el administrador de sesiones (como harías en AdminTool > Inicio > Administrador de Sesiones).

Parámetros:

Ninguno

Monitor de sesiones abiertas: /farm-sessions-monitor

Sintaxis:

AdminTool.exe /monitor de sesiones de granja

Descripción:

Comando /farm-sessions-monitor lanza en una única ventana de tamaño considerable el monitor de sesiones del administrador de la granja (como harías en AdminTool > Granja > Monitor de Sesiones).

Parámetros:

Ninguno

Abrir el administrador de balanceo de carga: /carga-balanceo-de-granja

Sintaxis:

AdminTool.exe /carga-balanceo-farm

Descripción:

Comando /carga-balanceo-de-granja lanza en una única ventana de tamaño considerable el administrador de balanceo de carga del administrador de granja (como harías en AdminTool > Granja > Balanceo de Carga).

Parámetros:

Ninguno

Ejecutar auditoría del sistema: /sistema de auditoría

Sintaxis:

AdminTool.exe /systemaudit

Descripción:

Comando /sistema de auditoría realiza una auditoría del sistema (como lo harías manualmente en AdminTool > Inicio > Auditoría del sistema > Ejecutar auditoría del sistema).

Parámetros:

Ninguno

Activación de licencia: /activar

Sintaxis:

AdminTool.exe /activar [licensePath]

Descripción:

Comando activar se utiliza para activar la licencia de Remote Access, utilizando un archivo de licencia.

Parámetros:

- licenciaRuta la ruta del archivo de licencia

Ejemplo:

AdminTool.exe /activate “C:\Program Files (x86)\TSplus\license.lic”

Restablecimiento de licencia tras la clonación de una máquina virtual: /restablecer

Sintaxis:

AdminTool.exe /license /reset

Descripción:

Al clonar un servidor, la pestaña 'Licencia' en AdminTool puede no mostrar un ID de computadora o puede mostrar el mensaje de error: “Identificador de hardware no válido.” El comando /restablecer apunta a inicializar la licencia en el servidor clonado para que se puedan asignar nuevas licencias a los productos TSplus instalados.

Notas Importantes:

1. Se debe activar una nueva licencia de TSplus utilizando una nueva clave de activación.
2. No utilice el comando /license /reset en una máquina que no ha sido clonada, ya que impide permanentemente la asignación de licencias. Siempre confirme el estado de la máquina antes de continuar.

Pasos para restablecer la licencia en un servidor clonado:

1. Abra una sesión de Administrador en el servidor clonado.

2. Cambiar el número de serie del volumen del HDD.

- Ejecutar el volumen comando para mostrar el número de serie de volumen actual (VSN). El resultado debería parecerse a: 74F8-9C08 .

- Descargue e instale la utilidad VolumeID, disponible aquí .

- Ejecuta el comando: volumeid C: 84F8-9C08 como administrador para cambiar el VSN de la unidad. En este ejemplo, cambiamos el VSN del disco C: y solo he cambiado un carácter (el primero) del VSN antiguo para especificar el nuevo.

- Nota: este paso es crítico porque ciertas versiones de Windows Server no generan un nuevo Número de Serie de Volumen durante la clonación, incluso al usar SysPrep.

3. Renombre el servidor clonado y reinícielo.

4.

Restablecer la licencia en AdminTool:

- Abre un símbolo del sistema con privilegios de administrador.
- Navegue al directorio que contiene el ejecutable AdminTool utilizando este comando: cd "C:\Program Files (x86)\TSplus\UserDesktop\files"
- Ejecute el siguiente comando: AdminTool.exe /license /reset

5. Verifique el restablecimiento.

- Después de ejecutar el comando, la pestaña 'Licencia' debería mostrar el siguiente error: Fallo al leer el archivo de licencia (formato de archivo inesperado).

6. Activar la nueva licencia.

- En la pestaña 'Licencia', haz clic en 'Activar tu licencia' e ingresa la nueva Clave de Activación para activar las licencias y soportes requeridos.

Ejemplo:

AdminTool.exe /license /reset TSplus-Security.exe /license /reset ServerMonitoring.exe /license /reset

---

Activación de licencia por volumen: /vl /activar

Sintaxis:

AdminTool.exe /vl /activate [licensekey] [parameters]

Comando vl /activar se utiliza para activar una licencia por volumen.

Parámetros:

- clave de licencia clave de licencia para activar, en este formato: AAAA-BBBB-CCCC-DDDD

- /usuarios cualquier número del 1 al 50, o "ilimitado"
- /edición “Escritorio”, “Web Móvil” o “Empresa”
- soporte años Cualquier número de 0 a 3.
- /comentarios/ Especifica los comentarios que se adjuntarán a la licencia en el portal de licencias

Ejemplo:

AdminTool.exe /vl /activate VOLU-MELI-CENS-EKEY /users unlimited /edition Enterprise / supportyears 3 /comments “Este es un comentario”

Para más información, por favor visite Documentación de licencia por volumen

---

Habilitar y deshabilitar la licencia por volumen: /vl /habilitar y /vl /desactivar

Sintaxis:

AdminTool.exe /vl /enable [licensekey]

AdminTool.exe /vl /disable [licensekey]

Descripción:

Comando vl /habilitar se utiliza para habilitar una licencia por volumen.

Comando vl /desactivar se utiliza para deshabilitar una licencia por volumen.

Parámetros:

- clave de licencia clave de licencia para habilitar/deshabilitar, en este formato: AAAA-BBBB-CCCC-DDDD

Ejemplos:

AdminTool.exe /vl /enable VOLU-MELI-CENS-EKEY

AdminTool.exe /vl /disable VOLU-MELI-CENS-EKEY

Para más información, por favor visite ¿Cómo habilitar/deshabilitar una licencia desde el servidor?

Actualización de licencia por volumen: /vl / actualizar

Sintaxis:

AdminTool.exe /vl /update [licensekey] [parameters]

Descripción:

Comando vl /actualizar se utiliza para actualizar a los usuarios de una licencia por volumen.

Parámetros:

- clave de licencia clave de licencia para actualizar, en este formato: AAAA-BBBB-CCCC-DDDD
- /usuarios cualquier número del 1 al 50, o "ilimitado"

Ejemplos:

AdminTool.exe /vl /update /users 2 AdminTool.exe /vl /update /users ilimitado

Para más información, por favor visite ¿Cómo actualizar los usuarios de una licencia por volumen desde el servidor?

Mostrar los créditos de licencia restantes para una clave de Licencia por Volumen: /vl / créditos-licencia

Sintaxis:

AdminTool.exe /vl /credits-license [licensekey] [parameters]

Descripción:

Comando vl /créditos-licencia se utiliza para mostrar los créditos de licencia restantes asociados con una clave de licencia por volumen.

Parámetros:

- clave de licencia Clave de licencia por volumen, en este formato: AAAA-BBBB-CCCC-DDDD
- /iniciar sesión proporcione el inicio de sesión del socio asociado con la clave de licencia por volumen
- /edición proporcione el parámetro de edición opcional para los productos de Advanced Security y Server Monitoring
- /silencio : ejecuta el comando en silencio

La salida se almacenará en la variable de entorno a nivel de usuario llamada CREDITOS_DE_LICENCIA_DE_VOLUMEN Puede ser necesario leer el valor de CREDITOS_DE_LICENCIA_DE_VOLUMEN desde un proceso diferente, utilizando el comando echo %VOLUME_LICENSE_CREDITS% .

Ejemplos:

AdminTool.exe /vl /credits-license VOLU-MELI-CENS-EKEY /login JOHNDOE TSplus-Security.exe /vl /credits-license VOLU-MELI-CENS-EKEY /login JOHNDOE /edition Essentials / silent

Para más información, por favor visite ¿Cómo mostrar los créditos de licencia restantes para una clave de Licencia por Volumen?

Mostrar créditos de soporte restantes para una clave de licencia por volumen: /vl /soporte-de-créditos

Sintaxis:

AdminTool.exe /vl /credits-support [licensekey] [parameters]

Descripción:

Comando vl /créditos-soporte se utiliza para mostrar los créditos de soporte restantes asociados con una clave de licencia por volumen.

Parámetros:

- clave de licencia Clave de licencia por volumen, en este formato: AAAA-BBBB-CCCC-DDDD
- /iniciar sesión proporcione el inicio de sesión del socio asociado con la clave de licencia por volumen
- /edición proporcione el parámetro de edición opcional para los productos de Advanced Security y Server Monitoring
- /silencio : ejecuta el comando en silencio

La salida se almacenará en la variable de entorno a nivel de usuario llamada CREDITOS_DE_LICENCIA_DE_VOLUMEN Puede ser necesario leer el valor de CREDITOS_DE_LICENCIA_DE_VOLUMEN desde un proceso diferente, utilizando el comando echo %VOLUME_LICENSE_CREDITS% .

Ejemplos:

AdminTool.exe /vl /credits-support VOLU-MELI-CENS-EKEY /login JOHNDOE TSplus-Security.exe /vl /credits-support VOLU-MELI-CENS-EKEY /login JOHNDOE /edition Essentials

Para más información, por favor visite ¿Cómo mostrar los créditos de soporte restantes para una clave de Licencia por Volumen?

2FA - restablecer: /resetear usuario

Sintaxis:

TwoFactor..Admin.exe /resetuser [user1] [user2] … [userN]

Descripción:

Comando /resetear usuario se utiliza para restablecer usuarios de 2FA, en lugar de hacerlo a través de la interfaz de usuario (esto se puede hacer aquí en la interfaz: TwoFactor.Admin >

Administrar usuarios > Restablecer)

Parámetros:

- usuario1 usuario2 ... usuarioN los nombres de dominio de los usuarios que desea restablecer (separados por un espacio simple)

Ejemplos:

TwoFactor.Admin.exe /resetuser johndoe jackrussell chuckbartowski

Para más información, por favor visite Restablecer configuración para usuarios

---

2FA - agregar usuarios: /agregarusuarios

Sintaxis:

TwoFactor.Admin.exe /addusers [userInfos1] [userInfos2] … [userInfosN]

Descripción:

Comando /agregarusuarios se utiliza para agregar varios usuarios de 2FA, en lugar de hacerlo a través de la interfaz de usuario, usuario por usuario (esto se puede hacer aquí en la interfaz: TwoFactor.Admin > Administrar usuarios > Agregar usuario)

Parámetros:

- userInfos1 userInfos2 ... userInfosN
  los datos del usuario de los usuarios que desea agregar. Esta información consiste en los siguientes campos, separados por un punto y coma.
  - nombreDeDominio (mandatorio): el nombre de dominio del usuario a agregar
  - métodoRecibido (opcional): el método para recibir códigos de confirmación. Debe ser uno de estos valores: SMS, App, Correo electrónico o DejarQueElUsuarioElija. App es el valor predeterminado.
  - teléfono móvil (opcional): el teléfono del usuario a agregar
  - correo electrónico (opcional): el correo electrónico del usuario a agregar

Ejemplos:

TwoFactor.Admin.exe /addusers johndoe jackrussell;DejarQueElUsuarioElija chuckbartowski;Teléfono;+33101010101; abcd@efgh.com samanthacarter;Correo electrónico;;

Para más información, por favor visite Agregar usuarios y grupos

---

2FA - agregar grupos: /agregargrupos/

Sintaxis:

TwoFactor.Admin.exe /addgroups [grupo1] [grupo2] … [grupoN]

Descripción:

Comando /agregargrupos/ se utiliza para agregar varios grupos de 2FA, en lugar de hacerlo a través de la interfaz de usuario, grupo por grupo (esto se puede hacer aquí en la interfaz: TwoFactor.Admin > Administrar Usuarios > Agregar Grupo)

Parámetros:

- grupo1 grupo2 ... grupoN los nombres de los grupos que deseas agregar.

Ejemplos:

TwoFactor.Admin.exe /addgroups grupo1 grupo2 grupo3

Para más información, por favor visite Agregar usuarios y grupos

---

2FA - lista de usuarios: /getusers

Sintaxis:

TwoFactor.Admin.exe /getusers

Descripción:

Comando /getusers se utiliza para obtener una lista de todos los usuarios/grupos configurados en la consola de administración de 2FA. Se devuelve una representación json de esta lista de usuarios/grupos, y se puede utilizar, por ejemplo, en un script de Powershell.

Esta lista se puede ver aquí en la interfaz: TwoFactor.Admin > Administrar usuarios.

Parámetros:

Ninguno

2FA - agregar grupos: /eliminarusuario

Sintaxis:

TwoFactor.Admin.exe /deleteuser [domainName] [userType]

Descripción:

Comando /eliminarusuario se utiliza para eliminar un usuario de la configuración de 2FA (esto se puede hacer aquí en la interfaz: TwoFactor.Admin > Administrar usuarios > Eliminar)

Parámetros:

- nombreDeDominio el nombre del usuario o del grupo a eliminar.
- tipoDeUsuario el tipo de objeto a eliminar. Su valor debe ser "usuario" o "grupo"

Ejemplos:

TwoFactor.Admin.exe /deleteuser “Este es un nombre de grupo” grupo TwoFactor.Admin.exe /deleteuser administrador usuario

Para más información, por favor visite Eliminar usuarios y grupos

---

Agregar o actualizar credenciales en el Administrador de Credenciales de Windows: / windowscredential-agregarouactualizar

Sintaxis:

AdminTool.exe /windowscredential-addorupdate

o

AdminTool.exe /windowscredential-addorupdate csvFilePath

Descripción:

Comando /windowscredential-agregarouactualizar se utiliza para agregar nuevas credenciales de Windows al Administrador de Credenciales de Windows o actualizar las existentes. Puede proporcionar credenciales individualmente especificando el dominio, el nombre de usuario y la contraseña, o procesar múltiples entradas en bloque desde un archivo CSV.

Este comando es útil para configurar la autenticación externa a través de SAML para el Portal Web con SSO.

Parámetros:

- **Modo de credencial única**

  - dominio (obligatorio): el nombre de dominio del usuario si forma parte de un Active Directory, o el nombre de la máquina si el usuario es un usuario local
  - nombre de usuario (mandatorio): el nombre de usuario de la cuenta de Windows
  - contraseña la contraseña de la cuenta de Windows

- **Modo masivo (archivo CSV)**

  - csvFilePath (mandatorio): la ruta a un archivo CSV que contiene una o más credenciales para agregar o actualizar

Ejemplos

Para un usuario de Active Directory:

AdminTool.exe /windowscredential-addorupdate COMPANY johndoe SecurePassword123

Para un usuario local:

AdminTool.exe /windowscredential-addorupdate MACHINE-NAME janedoe SecurePassword123

Para agregar o actualizar credenciales en masa desde un archivo CSV:

AdminTool.exe /windowscredential-addorupdate C:\\credentials\\users.csv

---

Eliminar credenciales del Administrador de Credenciales de Windows: /windowscredential-remove

Sintaxis:

AdminTool.exe /windowscredential-remove nombredeusuario

o

AdminTool.exe /windowscredential-remove csvFilePath

Descripción:

Comando /windowscredential-remove se utiliza para eliminar credenciales de Windows. Puede eliminar una sola credencial especificando el objetivo, o eliminar múltiples credenciales en bloque utilizando un archivo CSV.

Parámetros:

- **Modo de credencial única:**
- objetivo (obligatorio): el nombre de destino para la credencial, típicamente un nombre de dominio o servidor
- **Modo masivo (archivo CSV):**
  - csvFilePath (mandatorio): la ruta a un archivo CSV que contiene los nombres de usuario a eliminar. El archivo debe existir

Ejemplos:

AdminTool.exe /windowscredential-remove COMPANY

AdminTool.exe /windowscredential-remove C:\credentials\remove_users.csv

¿Cómo personalizar completamente la página de acceso web más allá de las capacidades del portal web?

Resumen

Al utilizar el Portal Web puedes personalizar las páginas de acceso web de Terminal Service Plus de manera extensa.

Sin embargo, en algunos casos, esto no es suficiente. En estos casos, puedes personalizar completamente la Página de Acceso Web, más allá de las capacidades del Portal Web, modificando tú mismo la Página de Acceso Web generada por el Webmaster Toolkit.

Advertencia, esta documentación está destinada únicamente a desarrolladores web experimentados.

Generando configuraciones obligatorias

Para incluir la configuración obligatoria en su página de Acceso Web, le recomendamos que comience generando su Página de Acceso Web utilizando el Portal Web .

Ubicación de archivos

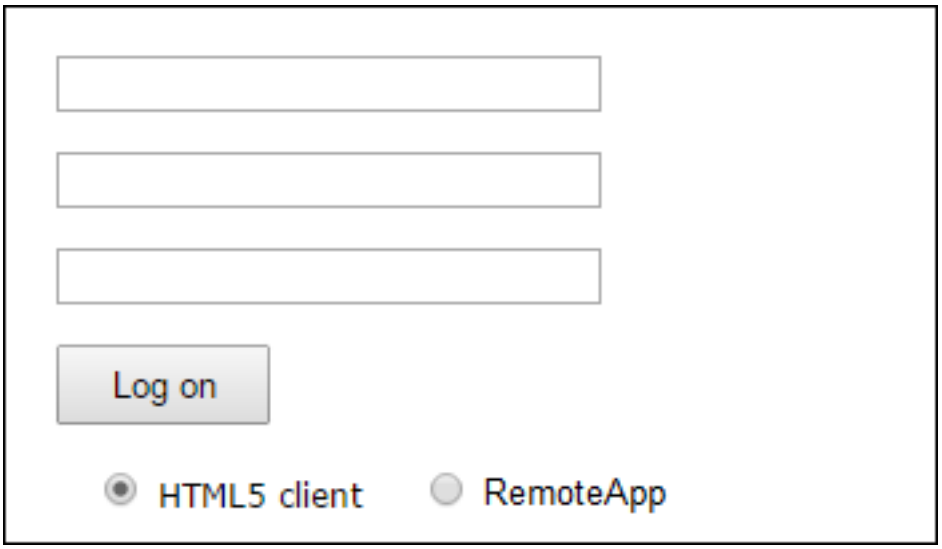
La página de acceso web se generará en la carpeta “C:\Program Files (x86)\TSplus\Clients\www”; por ejemplo, si eliges “index” como el nombre de la página, será el archivo llamado “index.html” en esta carpeta. Es un archivo HTML estándar, por lo que puedes utilizar todo tu conocimiento de los lenguajes de programación HTML, JavaScript y CSS para desarrollar tu página personalizada.

Todos los archivos de inclusión están escritos en relación con la carpeta “C:\Program Files (x86)\TSplus\Clients\www”. Por ejemplo, el archivo principal de estilos CSS se encuentra en “C:\Program Files (x86)\TSplus\Clients\www\software\common.css”, por lo que se incluye en el archivo de la página de acceso web HTML mediante la siguiente línea:

Página de Acceso Web Mínima

A partir de un archivo HTML generado por las Preferencias del Portal Web, lo reduciremos a una Página de Acceso Web mínima. Le aconsejamos que utilice un editor de texto como Notepad o Notepad++. no usa Word).

Después de nuestro trabajo, se verá como la captura de pantalla a continuación:



Primero, debes mantener todo lo que está entre los
y etiquetas HTML:

- meta etiquetas para forzar a los navegadores a limpiar su caché
- inclusiones de archivos .js
- Declaraciones de configuración de JavaScript

Luego, puedes reducir el contenido entre las etiquetas HTML 'body' y '/body' a estas pocas líneas:

cliente HTML5 Aplicación Remota

Actualiza la página web en tu navegador, y deberías obtener la página mínima de la captura de

pantalla anterior.

Recomendamos que limpie la caché de su navegador después de guardar cualquier archivo modificado.

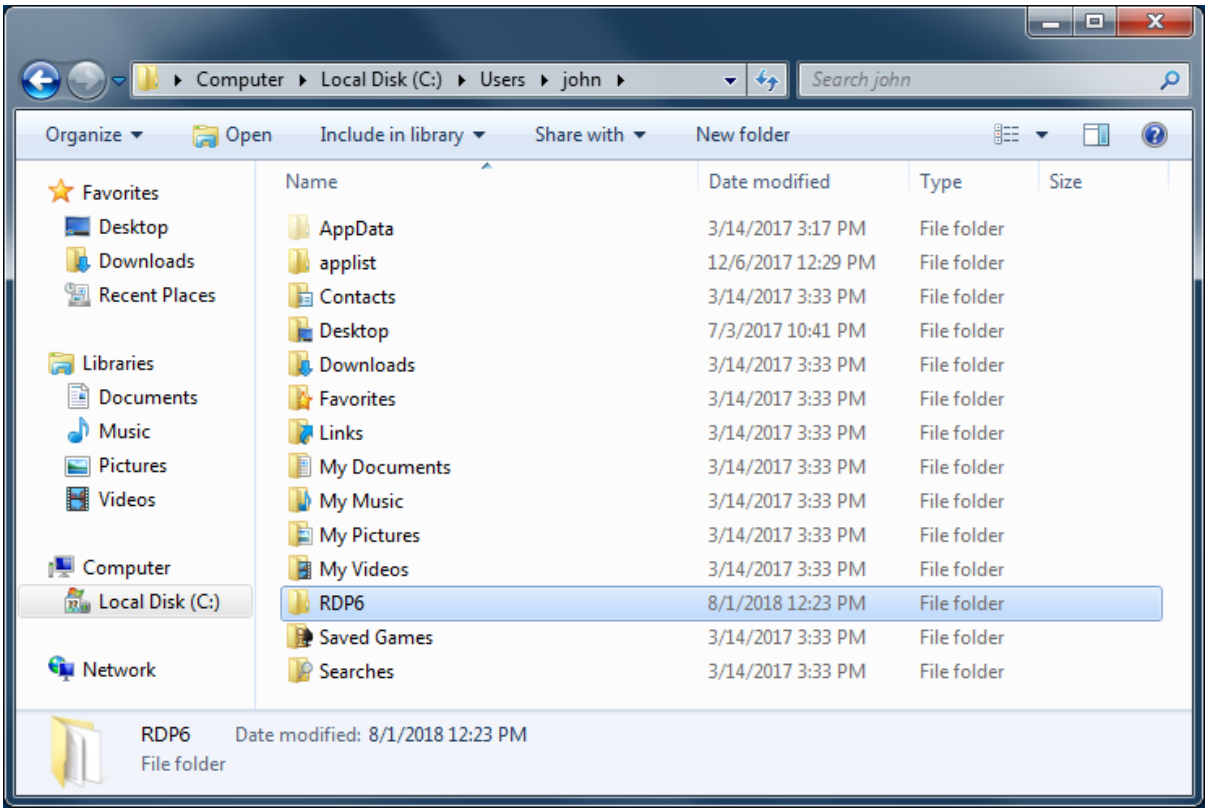
¡Finalmente, ahora depende de ti!

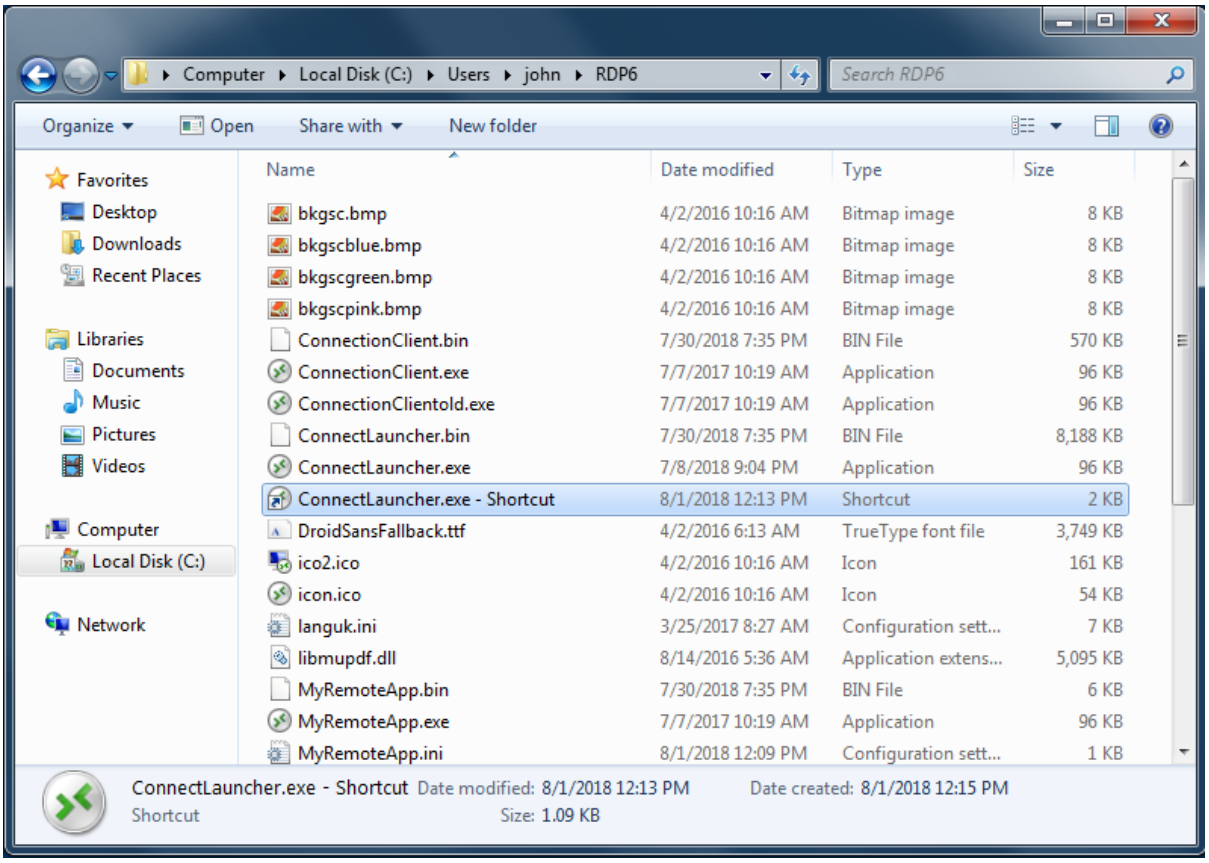
Mientras mantengas las llamadas a las funciones de JavaScript en eventos específicos y los identificadores dados (id="..."), tu Página de Acceso Web completamente personalizada funcionará bien.

Editar o eliminar los parámetros de un cliente generado

Hay muchas razones por las que querrías cambiar los parámetros de tu cliente de conexión: la dirección IP de tu servidor TSplus cambió, necesitas agregar la redirección de impresoras, cambiar la configuración de la impresora universal o algo así...

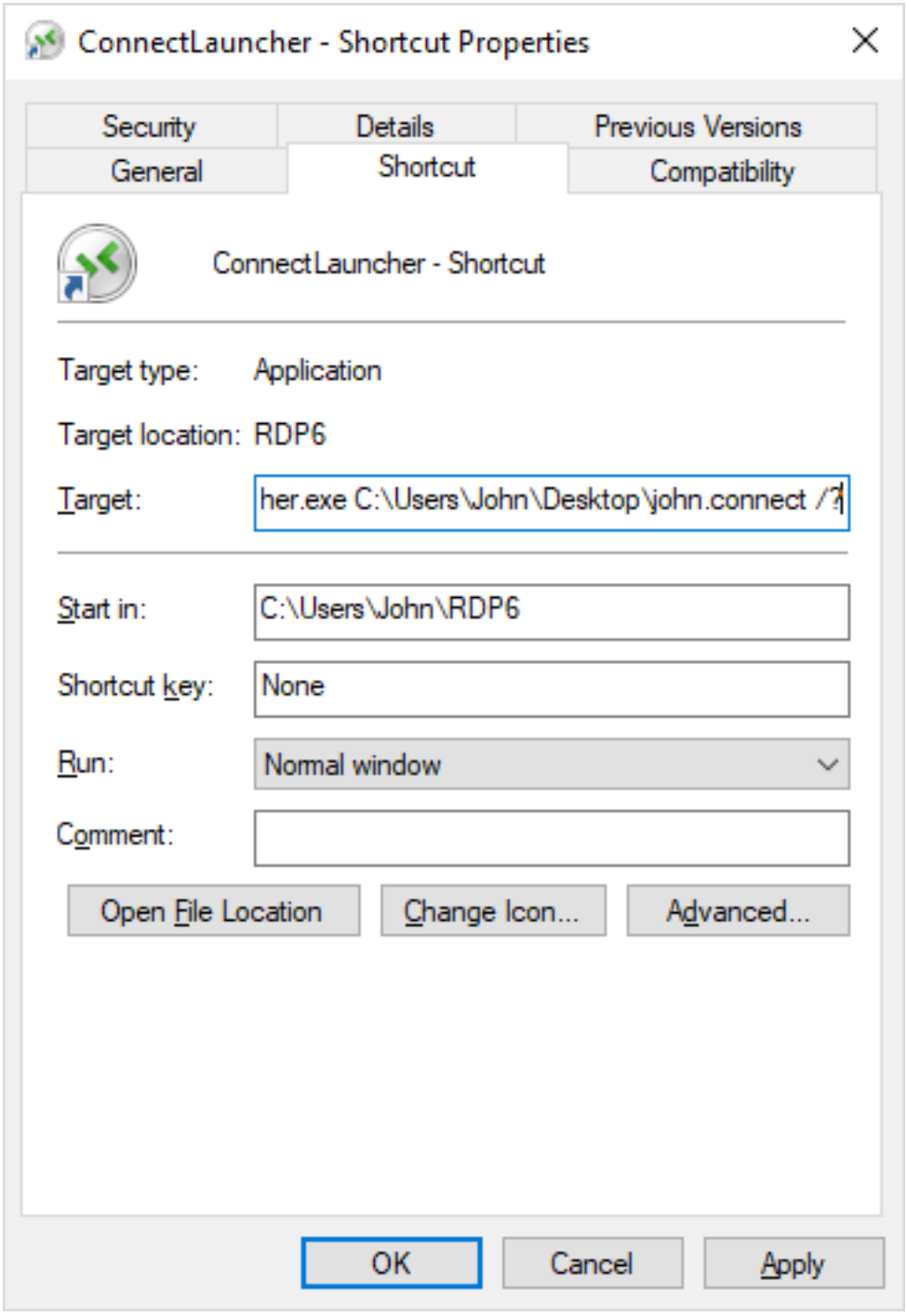
- Primero necesitas crear un acceso directo del archivo ConnectLauncher.exe, ubicado en la carpeta RDP6 del perfil del usuario:



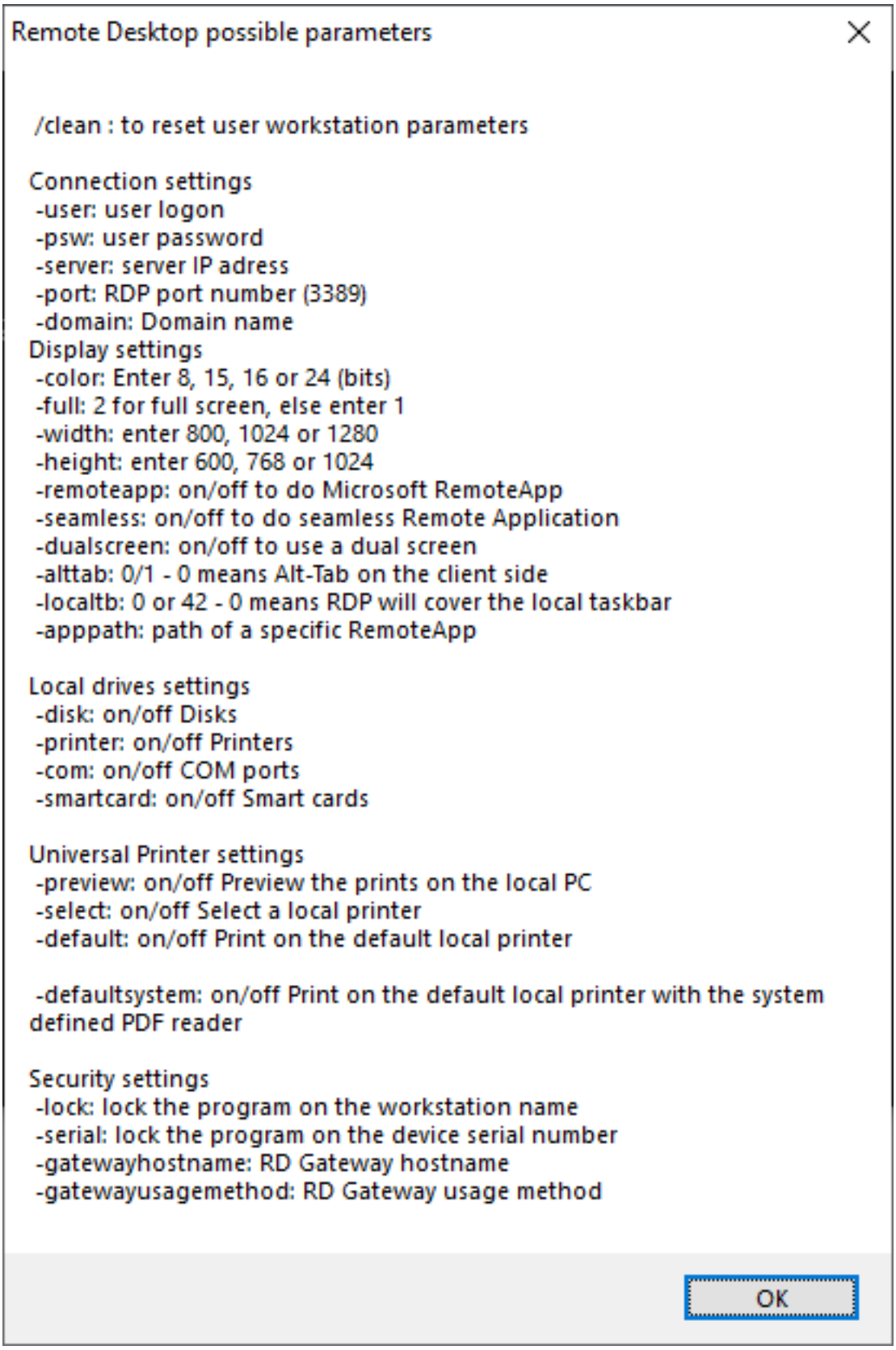


.

- Luego, haz clic derecho sobre él y selecciona propiedades. Coloca el mouse al final del campo "destino" y escribe la ruta del cliente seguida de "/?", por ejemplo: C: \Users\John\Desktop\clientname.connect /?":

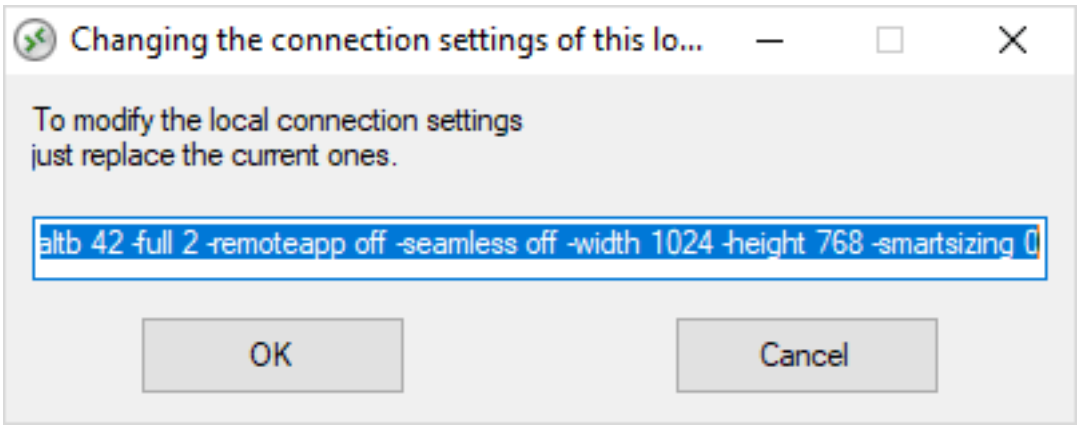


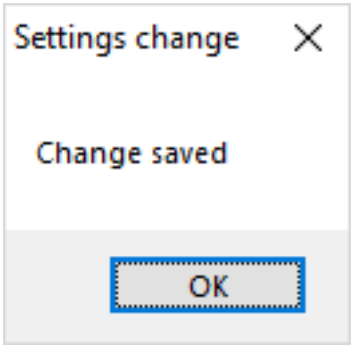
Ahora haga clic en Aceptar y haga doble clic en el acceso directo. Aparece una lista de conmutadores:



Haga clic en Aceptar, la lista de todos los parámetros aparece en una ventana pequeña.

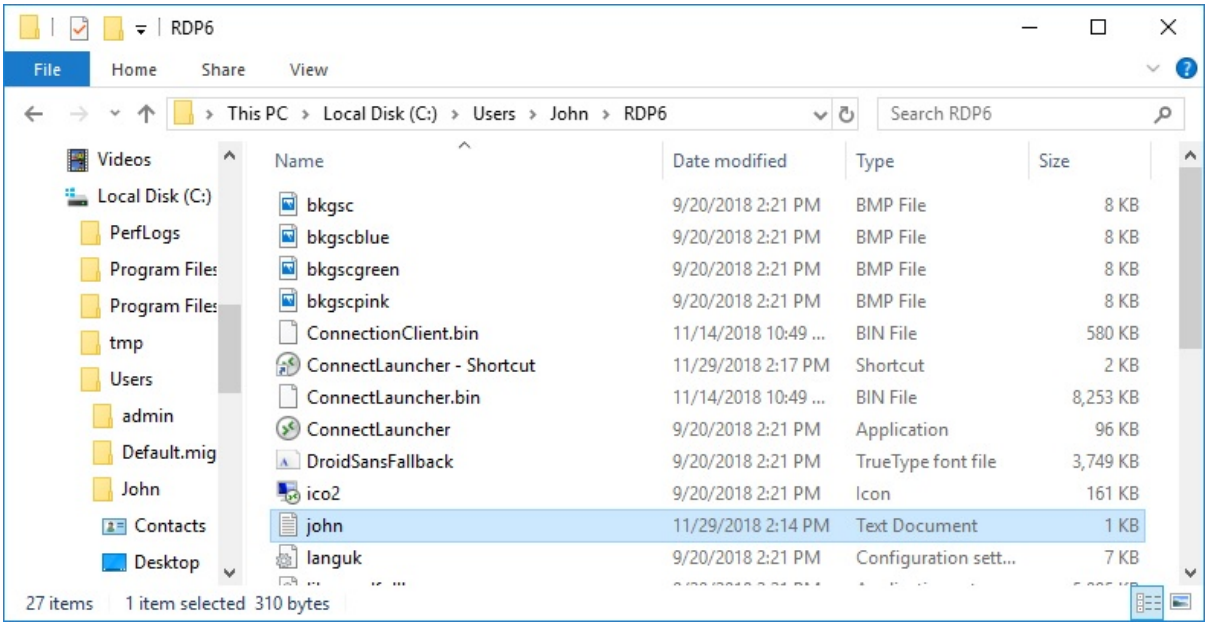
Ahora puedes editarlos para que coincidan con tus preferencias, necesitarás cerrar sesión y volver a iniciar sesión para aplicar los cambios.





Limpie los parámetros de un cliente generado

Después de haber lanzado el cliente al menos una vez, puedes limpiar los parámetros eliminando el archivo client.txt ubicado en la carpeta RDP6:



Habilitar la autenticación integrada de Windows en un dominio de Active Directory

Esta guía se proporciona para configurar la Autenticación Integrada de Windows (Kerberos/ NTLM) con una Cuenta de Servicio Administrada por Grupo (gMSA) en el Portal Web.

Debido a la naturaleza única de la red y la arquitectura de cada empresa, no podemos proporcionar soporte para problemas que surjan de seguir esta documentación. Cumple con los requisitos técnicos para el Portal Web con Autenticación Integrada de Windows, pero la implementación es bajo su propia responsabilidad.

Configuración de dominio

El entorno de Active Directory debe soportar la autenticación Kerberos o NTLM.

Configurar una Cuenta de Servicio Administrado (gMSA)

Instale el servicio del Portal Web y ejecútelo con un **cuenta de servicio administrada de dominio** en lugar de una cuenta de administrador de dominio.

Requisitos

- Nivel del esquema de Active Directory: **Windows Server 2012** o más tarde (requerido para gMSA)
- Al menos un controlador de dominio en ejecución **Windows Server 2012** o más tarde
- Clave raíz de KDS creada (configuración única)
- Membresía en **Administradores de dominio** o **Operadores de cuenta** crear la cuenta

Cree la clave raíz KDS (si aún no se ha creado)

Ejecutar en un controlador de dominio en una sesión de PowerShell elevada:

Ventana de terminal

```
Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10))
```

Esto hace que la clave raíz esté disponible de inmediato.

Crear el gMSA

Usar Nuevo-ADServiceAccount :

Ventana de terminal

```
New-ADServiceAccount `
  -Name "WebPortalSvc" `
  -DNSHostName "WebPortalSvc.domain.local" `
  -PrincipalsAllowedToRetrieveManagedPassword "YourServerGroup" `
  -Enabled $true
```

- Nombre nombre de cuenta gMSA
- NombreDelHostDNS FQDN para la cuenta
- Principales autorizados para recuperar la contraseña gestionada computadoras/grupo permitido para usar este gMSA

Conceder derechos administrativos (opcional / según sea necesario)

Por defecto, un gMSA no tiene privilegios especiales.

Para otorgar acceso a nivel de dominio (opcional):

Ventana de terminal

```
Add-ADGroupMember -Identity "Domain Admins" -Members "WebPortalSvc$"
```

Para otorgar capacidad de administrador local/inicio de sesión (si es necesario):

Ventana de terminal

```
Add-ADGroupMember -Identity "Administrateurs" -Members "WebPortalSvc$"
```

Importante: el final `$` es necesario para las referencias de cuenta gMSA en AD.

Requisito de reinicio

Se requiere un reinicio antes de continuar e instalar/utilizar la cuenta de servicio. También actualice las políticas.

Instalar el gMSA en los servidores de destino

Ejecutar en cada servidor que utilizará el gMSA:

Ventana de terminal

```
Install-ADServiceAccount -Identity "WebPortalSvc"
```

Instalación de prueba:

Ventana de terminal

```
Test-ADServiceAccount -Identity "WebPortalSvc"
```

Configurar servicios para usar el gMSA

1. Conceder **Iniciar sesión como un servicio** a la cuenta:

   - Abrir el Editor de directivas de grupo
   - Ir a: Configuración del ordenador > Configuración de Windows > Configuración de seguridad > Políticas locales > Asignación de derechos de usuario
   - Abrir Iniciar sesión como un servicio
   - Agregar DOMINIO\WebPortalSvc$

2. Asegure los permisos NTFS en los archivos/carpetas del Portal Web:

   - Haga clic derecho en la carpeta de la aplicación/ejecutable > Propiedades > Seguridad
   - Agregar DOMINIO\WebPortalSvc$
   - Conceder al menos **Leer y ejecutar** o **Control total** si es necesario para su implementación

3. Configurar la identidad del servicio:

   - Cuenta: DOMINIO\WebPortalSvc$
   - Contraseña: **dejar en blanco**

Configurar el nombre principal del servicio (SPN)

El servicio web debe estar registrado en Kerberos.

Ejecutar en un controlador de dominio:

Ventana de terminal

```
setspn -A HTTP/webserver.domain.com DOMAIN\WebPortalSvc
```

Reemplace con su FQDN de servidor y cuenta.

Si el servidor de alojamiento del Portal Web utiliza HTTP.sys, registre SPN contra la cuenta de la máquina:

Ventana de terminal

```
setspn -S HTTP/portal.hiyoko.com:8008 WIN-HLBO0AGABB7
```

setspn -S HTTP/portal.hiyoko.com:8009 WIN-HLBO0AGABB7

Configurar la red en la máquina cliente

Para colocar un cliente unido a un dominio en la subred correcta:

1. Identificar la interfaz de red correcta
2. Eliminar IP estática existente (si es incorrecta)
3. Asignar IP estática, máscara de subred y puerta de enlace predeterminada que coincida con la subred DNS/DC
4. Establecer direcciones del servidor DNS

Importante: asigne direcciones IP estáticas al controlador de dominio y a los clientes. La sincronización de políticas de seguridad requiere que las máquinas estén en la misma subred en este contexto.

Permitir la conectividad del cliente requerida

UDP/TCP 53 puede ser bloqueado, lo que impide las consultas DNS.

Pasos de solución de problemas

Verificar el estado del servidor DNS

En el controlador de dominio:

Ventana de terminal

net start DNS

Verifique que el servicio DNS esté en funcionamiento.

Verificar la IP del servidor DNS

En cliente:

Ventana de terminal

```
ipconfig /all
```

Confirme que la IP del servidor DNS coincide con la IP del controlador de dominio.

Prueba de conectividad básica

En cliente:

Ventana de terminal

```
ping <DC_IP_Address>
```

Si el ping falla, soluciona problemas de enrutamiento de red/firewall.

Verificar reglas del firewall

Asegúrese de que se permita UDP/TCP 53 entrante/saliente en el cliente y el servidor.

Prueba con nslookup

Ventana de terminal

nslookup domain.com <DC_IP_Address>

Si esto funciona, el servidor DNS predeterminado puede estar mal configurado o ser inalcanzable.

Revisar el Visor de Eventos

En el controlador de dominio, verifica los errores relacionados con DNS.

Configurar Mozilla Firefox para la autenticación integrada de Windows

Firefox no utiliza WIA de forma predeterminada.

Paso 1: negociar URIs de confianza

1. Abrir Firefox
2. Ir a sobre:config
3. Aceptar advertencia
4. Conjunto

network.negotiate-auth.trusted-uris
a tus dominios, por ejemplo:

- intranet.dominio.com, dominio.com

Paso 2: URIs NTLM de confianza

Conjunto red.automatic-ntlm-auth.uris-de-confianza a la misma lista de dominios.

Paso 3: URIs de delegación de Kerberos (si es necesario)

Conjunto network.negotiate-auth.delegation-uris por ejemplo:

- domain.com

Paso 4: reiniciar el navegador

Reinicie Firefox para aplicar los cambios.

Configurar Google Chrome para la Autenticación Integrada de Windows

Chrome utiliza la configuración de autenticación del sistema de Windows.

A través de la Directiva de Grupo (recomendado)

1. Descargar plantillas ADMX de Chrome:
   - https://chromeenterprise.google/policies/

2. Copiar
   chrome.admx
   y
   chrome.adml
   a:
   - C:\Windows\PolicyDefinitions
   - C:\Windows\PolicyDefinitions\es-ES

3. Abrir gpedit.msc
4. Ir a:
   - Configuración del ordenador > Plantillas administrativas > Google > Google Chrome

5. Habilitar la autenticación integrada para sitios de intranet y configurar sitios de confianza:

- intranet.dominio.com, dominio.com

6. Aplicar política:

Ventana de terminal

gpupdate /force

Otros métodos

Otros métodos (conmutadores y banderas de la línea de comandos de Chrome) no tuvieron éxito en este contexto.

Configurar Microsoft Edge para la autenticación integrada de Windows

Edge utiliza las políticas de Microsoft Edge y la configuración de zonas de seguridad de Windows.

Habilitar inicio de sesión automático en la zona de intranet

1. Abrir Opciones de Internet
2. Seguridad tab > Intranet local > Nivel Personalizado
3. Debajo
   Autenticación de usuario
   , conjunto:
   - Inicio de sesión automático solo en la zona de Intranet

Configurar políticas de Edge a través de GPO

Paso 1: instalar plantillas ADMX de Edge

1. Descargar:
   - https://www.microsoft.com/en-us/edge/business/download

2. Copiar
   msedge.admx
   y
   msedge.adml
   a:
   - C:\Windows\PolicyDefinitions
   - C:\Windows\PolicyDefinitions\es-ES

Paso 2: editar la configuración de la política

1. Abrir gpedit.msc
2. Ir a:
   - Configuración del ordenador > Plantillas administrativas > Microsoft Edge

3. Habilitar:
   - Configurar la lista de servidores a los que Microsoft Edge puede delegar credenciales

4. Configurar servidores de confianza:
   - intranet.dominio.com, dominio.com

Paso 3: aplicar políticas

Ventana de terminal

gpupdate /force

Otros métodos

Otros métodos (conmutadores y banderas de línea de comandos de Edge) no tuvieron éxito en

este contexto.

Solución de problemas de autenticación integrada

Verificar tickets de Kerberos

En el cliente de Windows:

Ventana de terminal

klist

Deberías ver un ticket para HTTP/webserver.domain.com .

Borrar credenciales/tickets en caché

Ventana de terminal

klist purge

Verificar el registro de SPN

En el controlador de dominio:

Ventana de terminal

```
setspn -L serviceaccount
```

Asegúrate HTTP/webserver.domain.com está listado.

Depurar Kerberos en Firefox

Iniciar Firefox con registro:

Ventana de terminal

```
set NSPR_LOG_MODULES=negotiateauth:5
set NSPR_LOG_FILE=%USERPROFILE%\Desktop\firefox.log
start firefox.exe
```

Revisión firefox.log por errores de autenticación.

Verificar políticas de Chrome

En Chrome, abre:

chrome://policy

Asegúrate AuthServerWhitelist y AuthNegotiateDelegateWhitelist se aplican.

Verificar políticas de Edge

En Edge, abre:

edge://policy

Asegúrate AuthServerWhitelist y AuthNegotiateDelegateWhitelist se aplican.

Fin de vida versión 1-12

Remote Access v12 (y todas las versiones anteriores) dejarán de funcionar en todas las computadoras con Windows.
Las interrupciones del servicio comenzarán en enero de 2026 y se extenderán gradualmente hasta el cierre completo en abril.

Actualizar a una versión LTS o a la última versión requiere un **suscripción de soporte activo** por su licencia. Si este no es el caso, le invitamos a suscribirse a una suscripción de soporte desde su portal de licencia y actualizar su licencia desde su Admintool con su archivo .LIC para beneficiarse de la actualización.

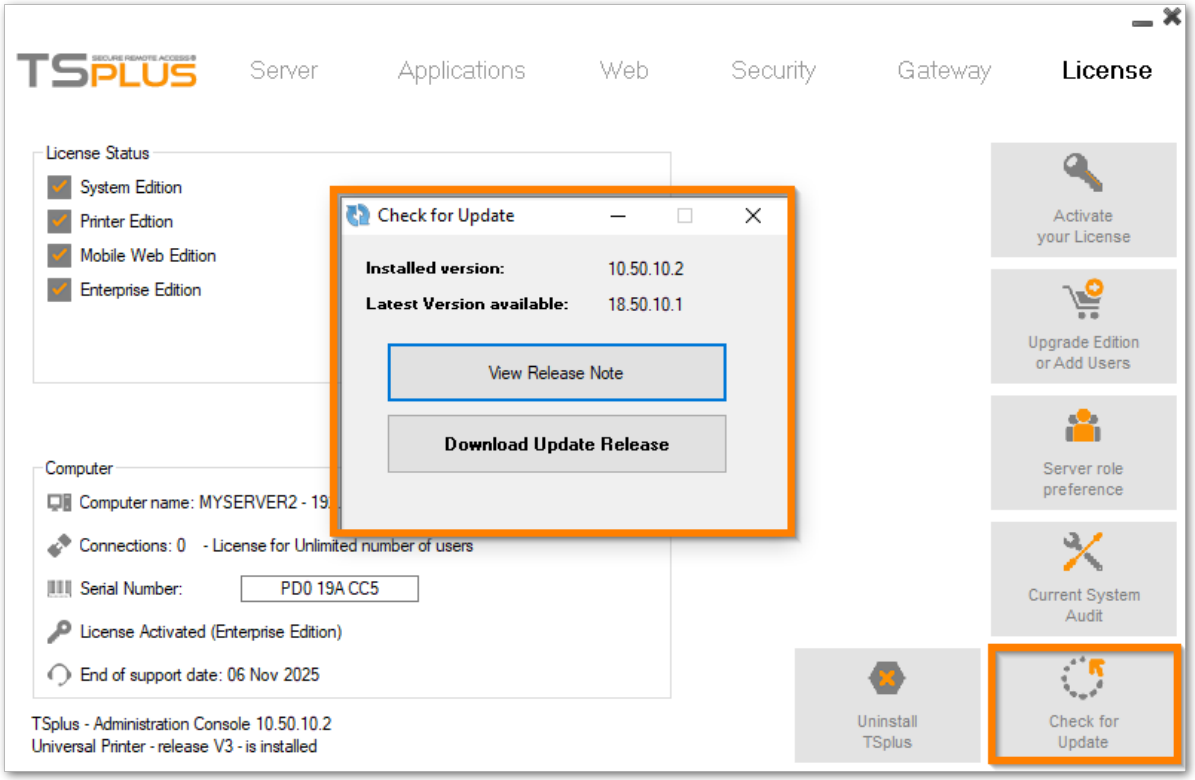
Si no puedes añadir una suscripción de soporte o recibes un mensaje de error, contáctenos utilizando nuestro Contact Support , proporcionando:

- Su número de licencia en el formato PXX XXX XXX Visible en la pestaña de licencia de Admintool
- Su factura de compra de licencia
- Tu factura de suscripción de soporte

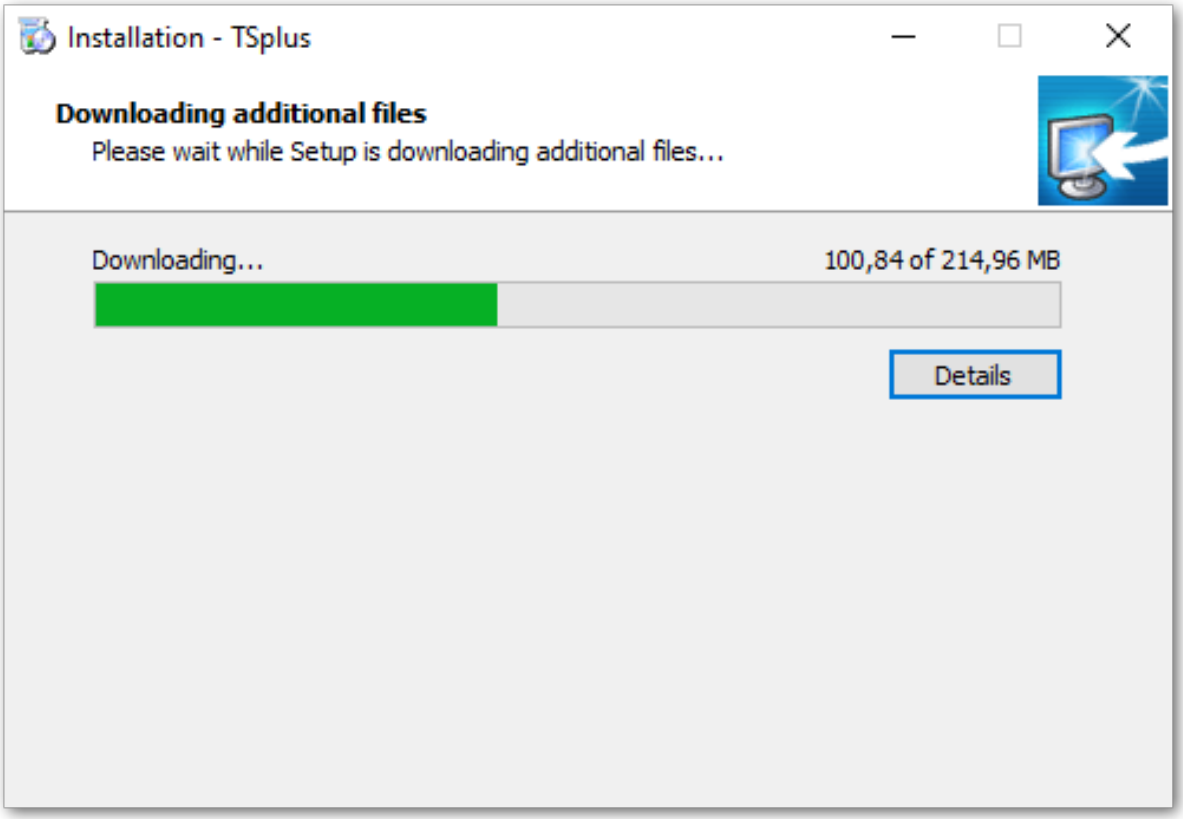
Actualizando su versión v10

Si deseas instalar una LTS en lugar de la última versión, ve a la página LTS)

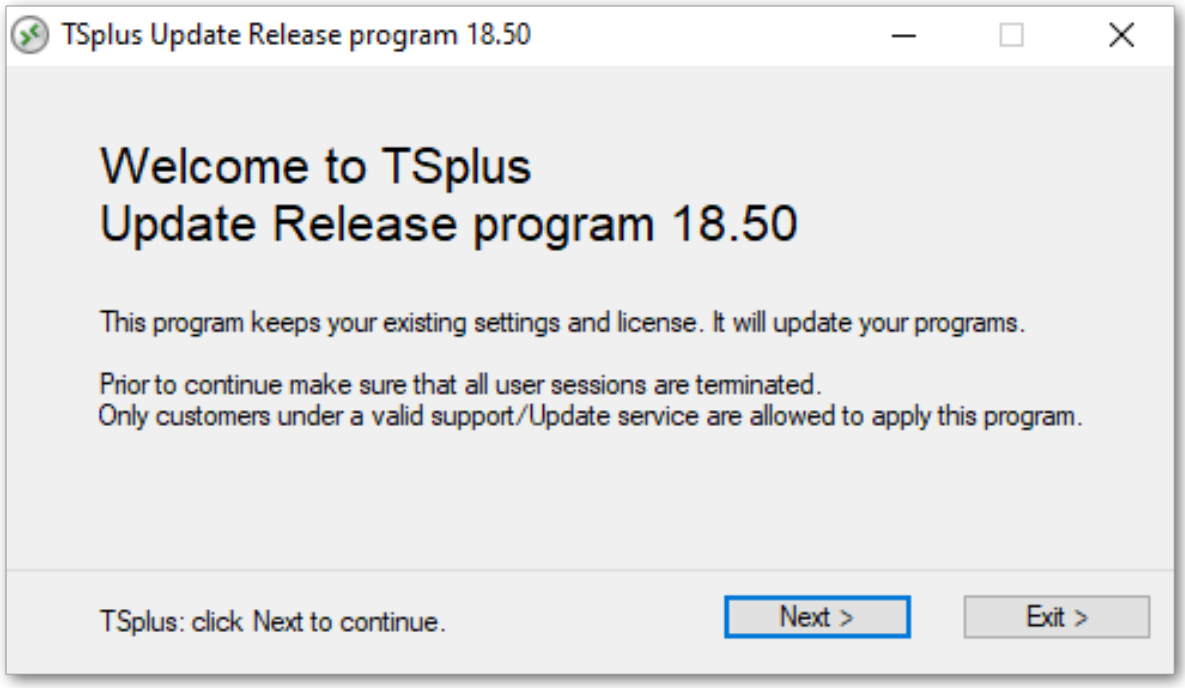
Desde tu versión en línea 10, haz clic en el siguiente campo para descargar el **UpdateRelease.exe**
También puedes descargar el UpdateRelease.exe para iniciar el procedimiento de actualización.



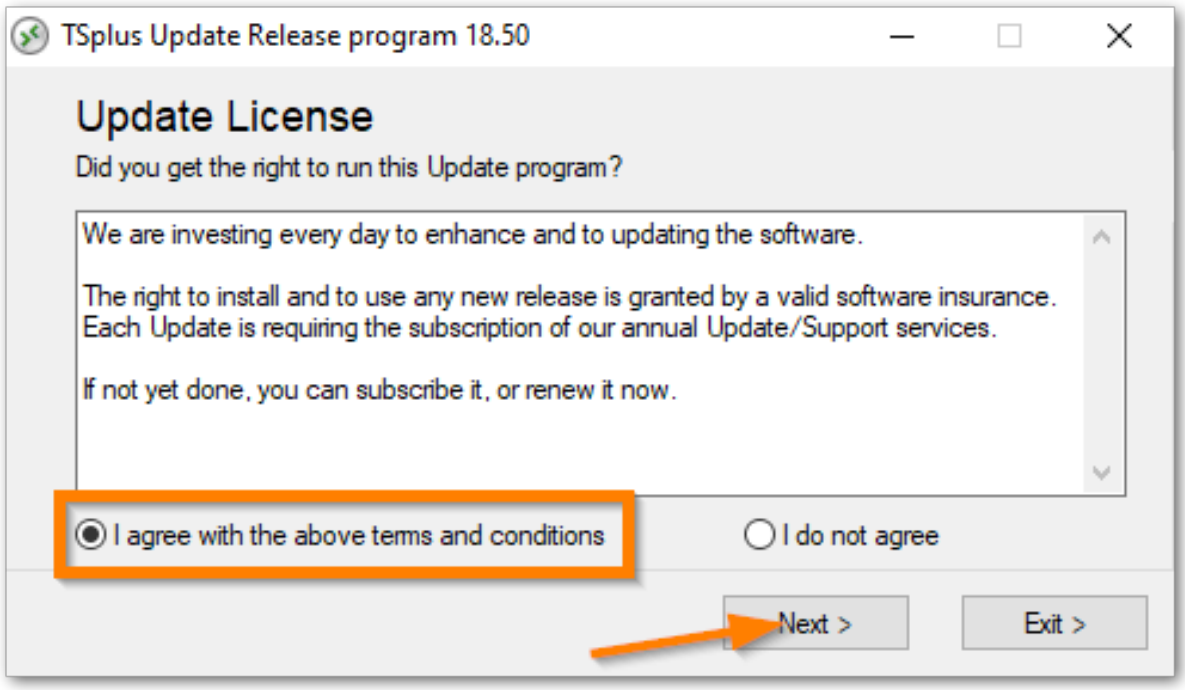
Descargue el updaterelease.exe y ejecute el ejecutable.



El programa de actualización aparecerá.



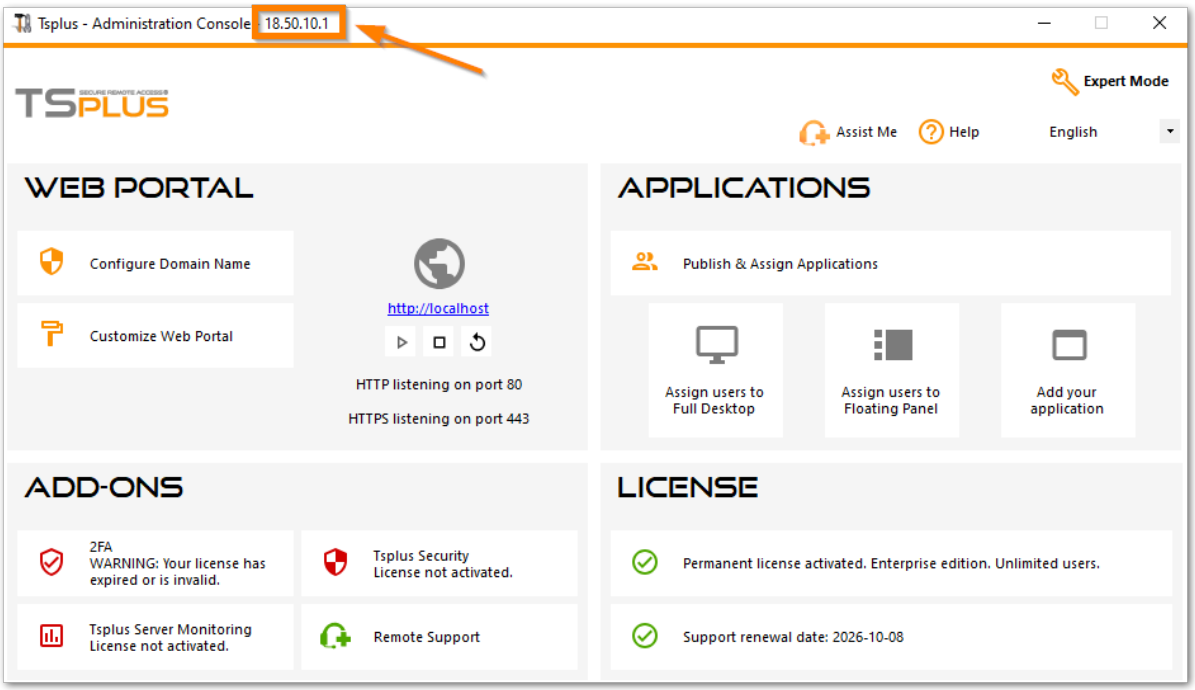
Acepta los términos y haz clic
SIGUIENTE



Sigue todos los pasos y luego reinicia tu servidor al final de la migración.

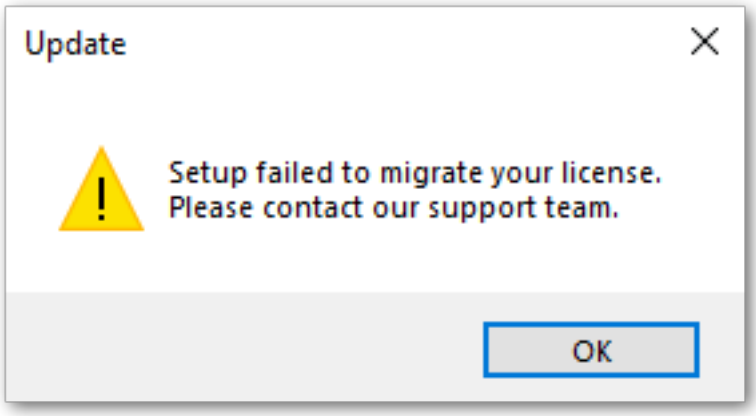
- Cuando haya terminado, **Reinicie su servidor** para completar la actualización.

Lanza el AdminTool. Felicitaciones, ahora estás en la versión 19.



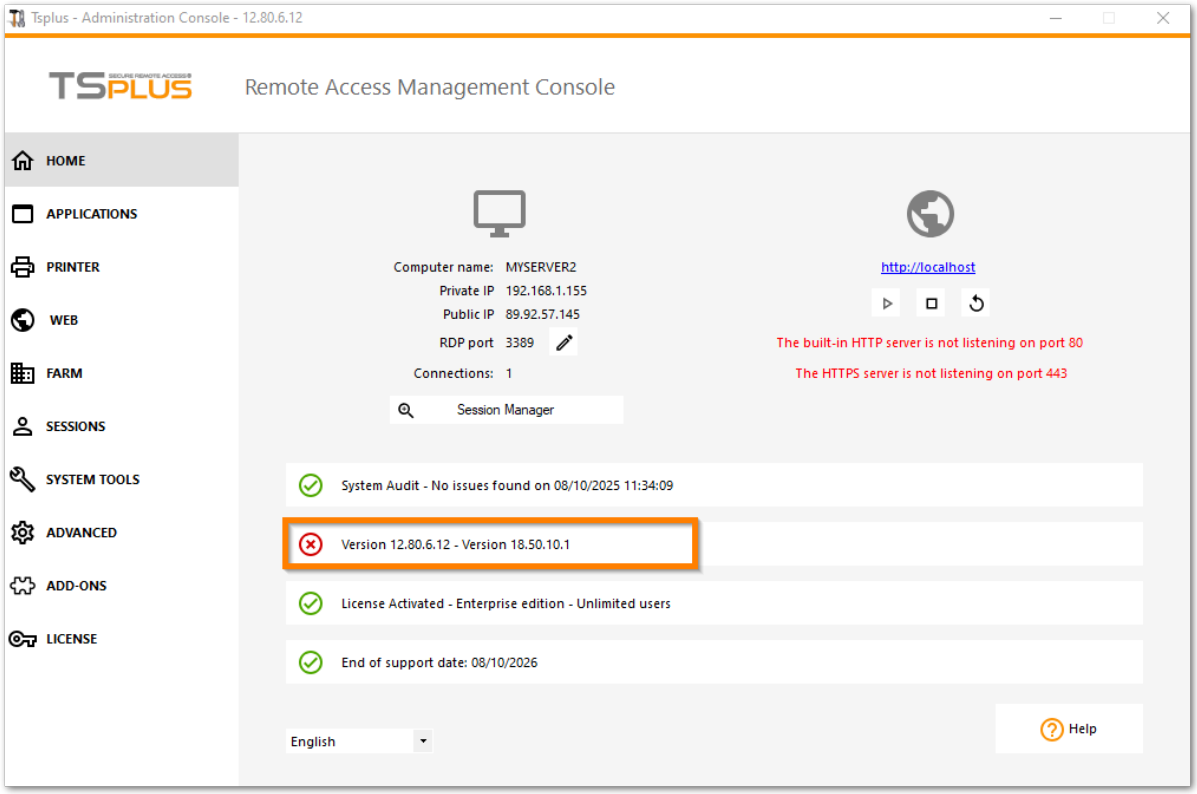
Mensaje de error v10

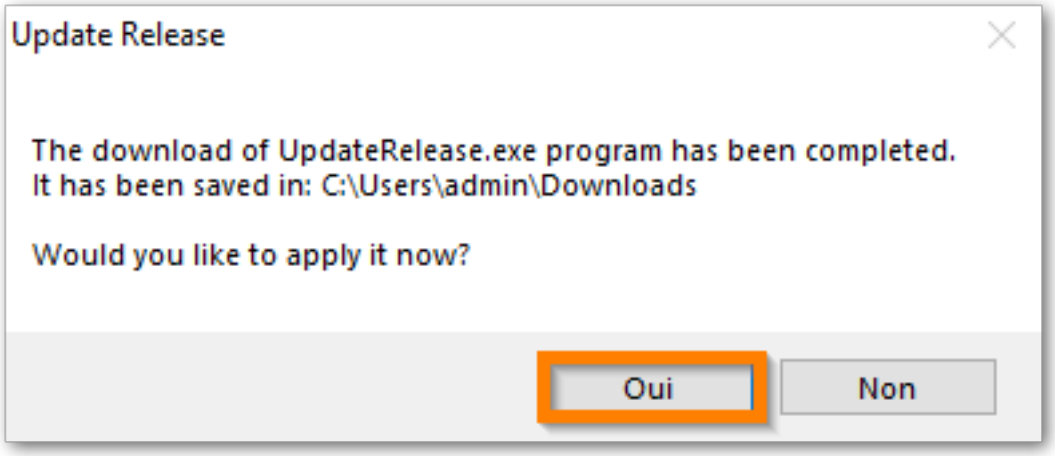
Si recibe este mensaje de error,
Contact Support
para desinstalar Remote Access. Por favor, proporcione el número de licencia en el formato PXX XXX XXX y también una prueba de la factura de compra del soporte.

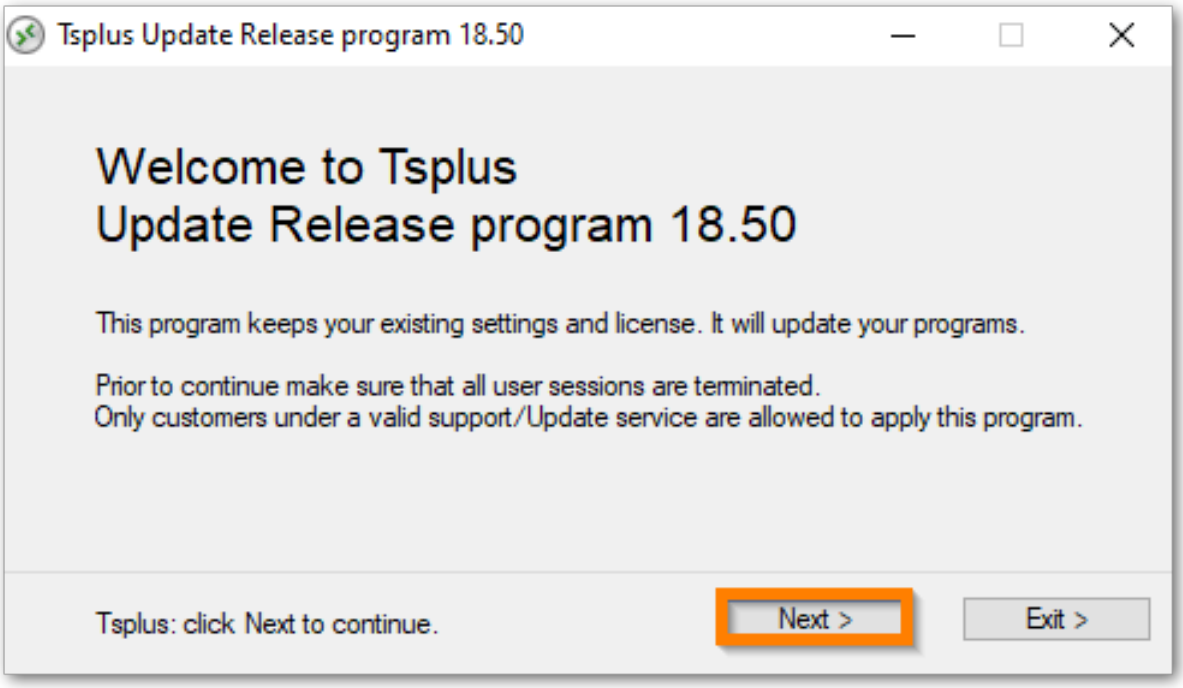


Actualizando su versión v12

Desde tu versión en línea 12, haz clic en el siguiente campo para descargar el **UpdateRelease.exe**
También puedes descargar el UpdateRelease.exe para iniciar el procedimiento de actualización.

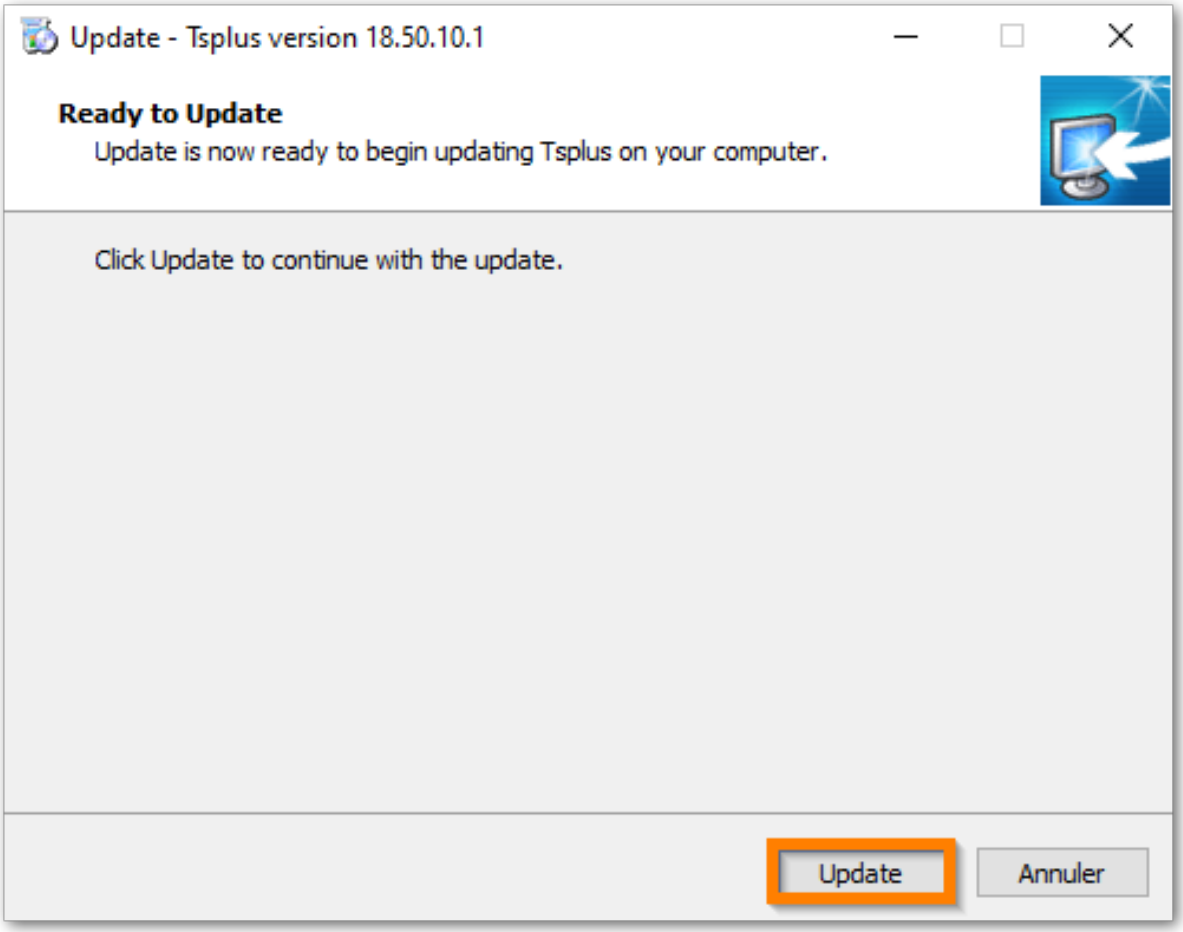

Tsplus - Administration Console - 12.80.6.12
TSPLUS
Remote Access Management Console
HOME
APPLICATIONS
PRINTER
WEB
FARM
SESSIONS
SYSTEM TOOLS
ADVANCED
ADD-ONS
LICENSE
Computer name: MYSERVER2
Private IP 192.168.1.155
Public IP 89.92.57.145
RDP port 3389
Connections: 1
Session Manager
http://localhost
The built-in HTTP server is not listening on port 80
The HTTPS server is not listening on port 443
System Audit - No issues found on 08/10/2025 11:34:09
Version 12.80.6.12 - Version 18.50.10.1
License Activated - Enterprise edition - Unlimited users
End of support date: 08/10/2026
English
Help

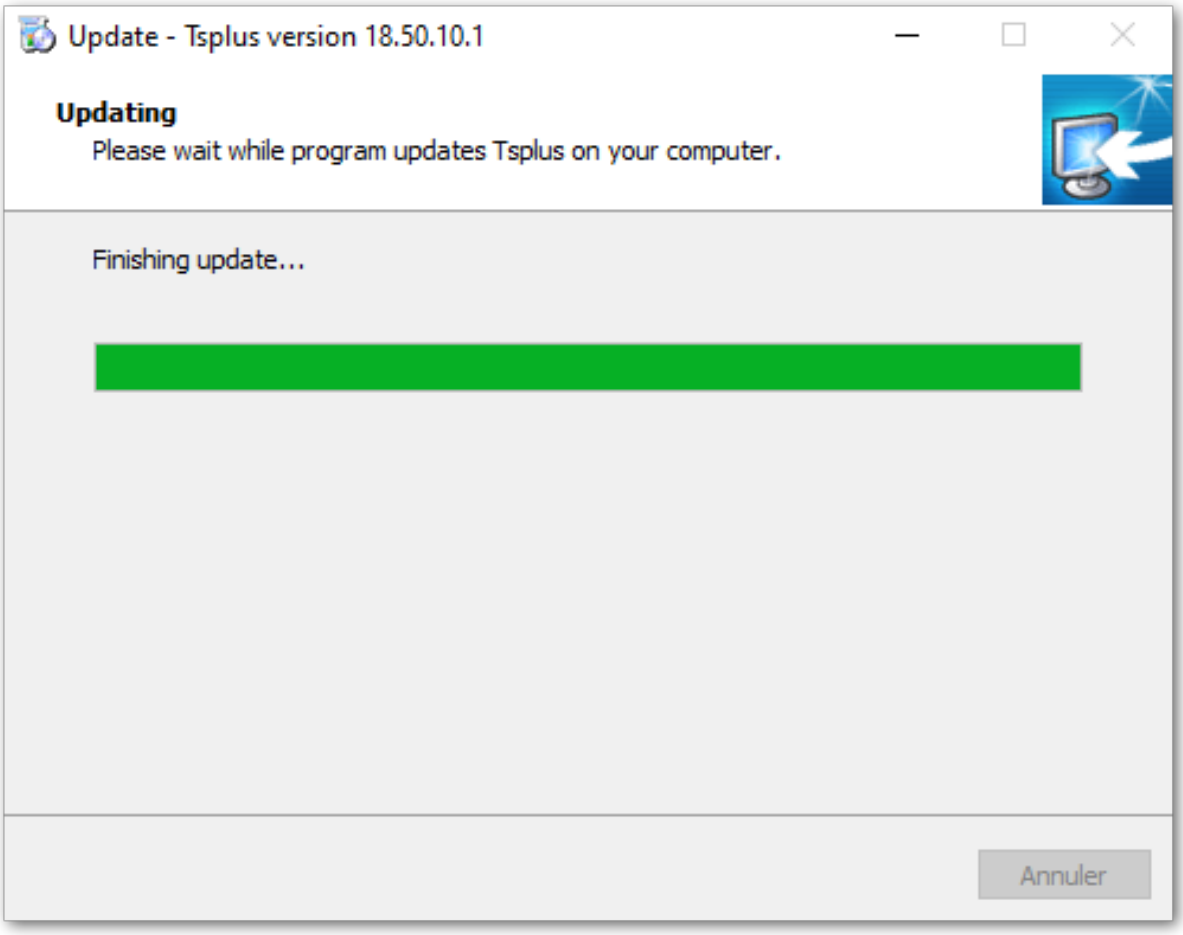

Update Release
The download of UpdateRelease.exe program has been completed.
It has been saved in: C:\Users\admin\Downloads
Would you like to apply it now?
Oui
Non



- Acepta los términos y haz clic en SIGUIENTE

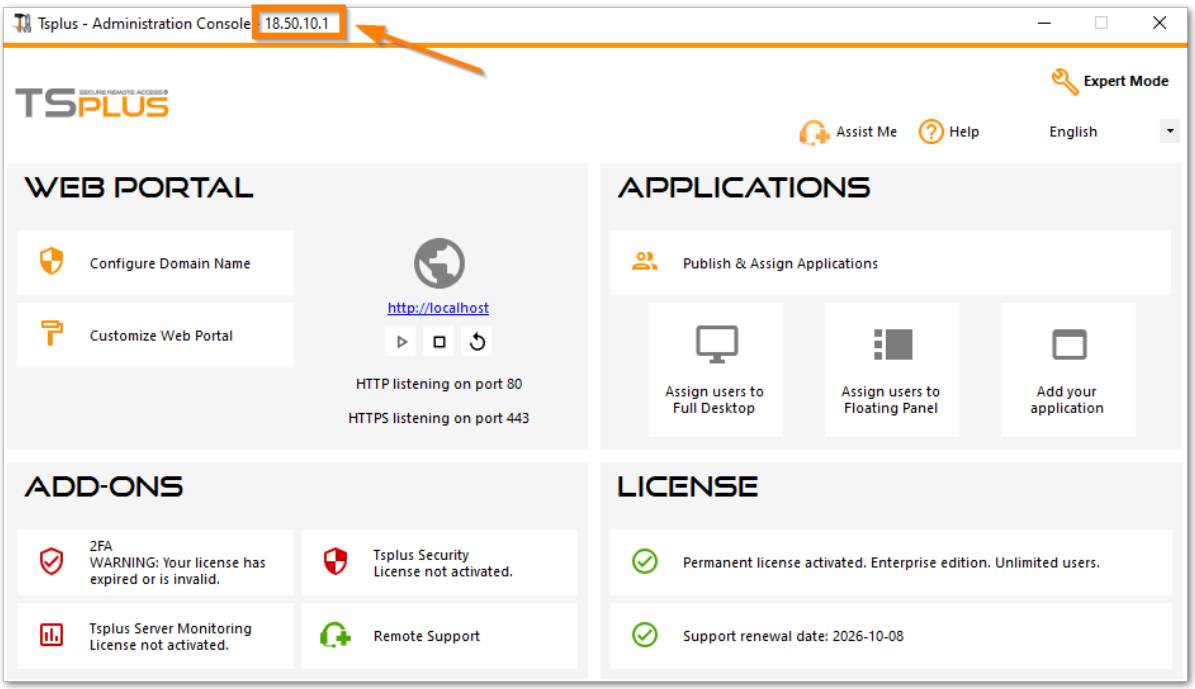
Una vez descargado, haga clic
Actualizar
para iniciar el proceso.





- Cuando haya terminado, **Reinicie su servidor** para completar la actualización.

Lanza el AdminTool. Felicitaciones, ahora estás en la versión 19.



Mensaje de error v12

Si recibe este mensaje de error, Contact Support desinstalar Remote Access.
Por favor, proporcione el número de licencia en el formato PXX XXX XXX y también la prueba de la factura de compra del soporte.

Habilitar el protocolo HTTPS

Caso estándar

A partir de la versión 9.20 de Terminal Service Plus, puedes redirigir cada solicitud web que utilice HTTP al protocolo seguro HTTPS.

Para activar esta función en un servidor, edita (o crea) el archivo “C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin” y añade la siguiente línea:

disable_http_only=true

Guarde el archivo y reinicie los servidores web de Terminal Service Plus (AdminTool > Web > Reiniciar servidores web o vuelva a leer la configuración accediendo http://127.0.0.1/w0j3?settings.bin).

Una vez que esta función esté habilitada, puede intentar navegar a la página web insegura en:

http://tu-servidor

y redirigirá automáticamente su solicitud a la página del Portal Web seguro en:

https://your-server

Caso especial: Puertos web personalizados

Si está utilizando un puerto específico para servir HTTPS, edite el archivo “C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin” y use la siguiente línea en lugar de la línea descrita anteriormente:

disable_http_only="dominio.com:4431"

donde domain.com es el nombre de host de su propio servidor y 4431 es su puerto HTTPS personalizado.

Guarde el archivo y reinicie los servidores web de Terminal Service Plus (AdminTool > Web > Reiniciar servidores web).

Una vez que esta función esté habilitada, puede intentar navegar a la página web insegura en:

http://domain.com

y redirigirá automáticamente su solicitud a la página del Portal Web seguro en:

https://domain.com:4431

Comentario: Incluso si esto no es seguro, pero deseas deshabilitar ssl/https en el puerto http, edita el archivo settings.bin y añade: disable_ssl_on_http=true, guarda y reinicia los servidores.

Deshabilitar http en https

Por defecto, se permite el acceso https://my-domain.com , https://my-domain.com:80 , http://my-domain.com:443 Así que permite http en el puerto 443 o permite https en el puerto 80, no tiene impacto en la seguridad y facilita volver a una conexión xhr degradada cuando no es posible el soporte de websockets. Pero si se desea deshabilitarlo, edite el archivo settings.bin y agregue la siguiente línea:

disable_http_on_https=true

Luego reinicie los servidores web de Terminal Service Plus (AdminTool > Web > Reiniciar servidores web o volver a leer la configuración). http://127.0.0.1/w0j3?settings.bin)

Cumplimiento de HTTPS y validación gratuita del certificado SSL

Tenga en cuenta que esta función de aplicación de HTTPS es completamente compatible con nuestro Certificado SSL gratuito característica.

Hacer obligatorio el uso del portal web para conectarse al servidor

A partir de la versión 6.60 de Terminal Service Plus, puedes bloquear/deshabilitar cualquier intento de conexión utilizando mstsc.exe (o cualquier cliente RDP) a través del puerto abierto/redirigido (80 o 443).

Esta función solo permite accesos desde el Portal Web de Terminal Service Plus y desactiva cualquier otra conexión RDP en el puerto 80/443.

Para activar esta función en un servidor, edita el archivo C:\Program Files (x86)\TSplus\UserDesktop\files\AppControl.ini y añade/modifica la siguiente variable:

Seguridad Block_rdp_splitter=si

Balanceo de Carga

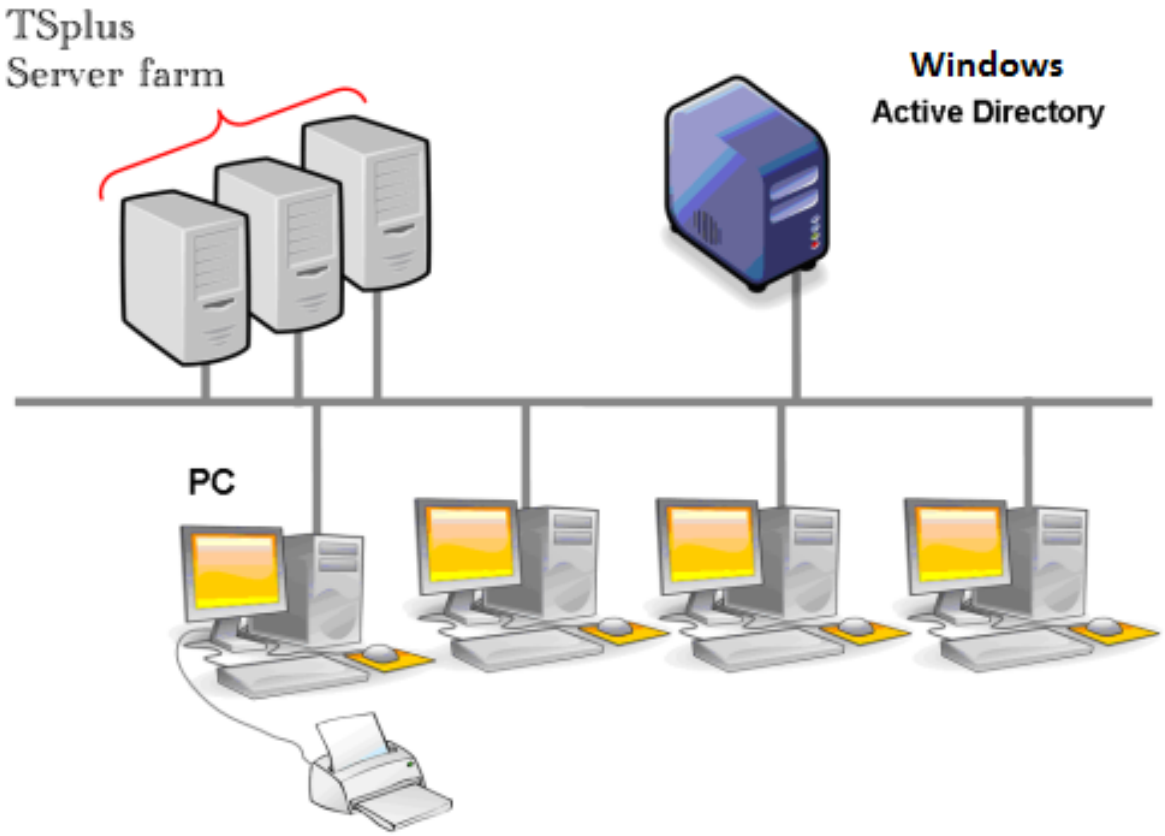
Requisitos previos

Usando esta función, podrá gestionar un entorno con balanceo de carga.

Significa que la carga de todos sus usuarios se distribuirá entre sus servidores. La carga de trabajo se compartirá entre todos los servidores de su granja.

El balanceo de carga permite utilizar un número ilimitado de servidores con balanceo de carga y está disponible con la edición Enterprise (una licencia válida por servidor). Esta capacidad muy poderosa y avanzada debe ser utilizada cuando se tiene que desplegar un gran número de usuarios/servidores.

Importante: Simplemente habilitar el balanceo de carga redirigirá a los usuarios al servidor menos cargado de la granja, independientemente de los servidores asignados configurados para los usuarios. Si tiene la intención de usar el balanceo de carga Y la asignación de servidores, asegúrese de marcar la casilla "Balancear carga en servidores asignados".



Normalmente recomendamos usar un servidor para 50 usuarios concurrentes.
Puedes superar los +50 usuarios dependiendo de la potencia de tu servidor y el consumo de los recursos de las aplicaciones de los usuarios.

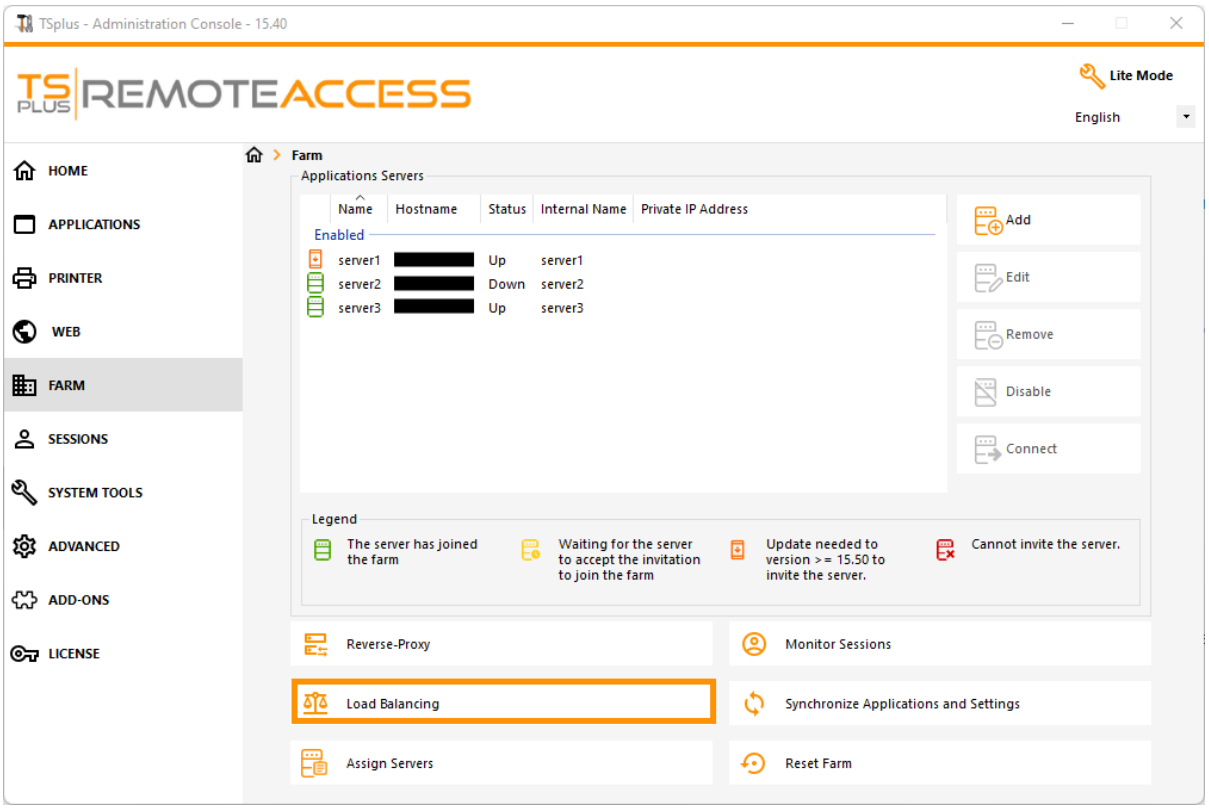
Clientes Generados y Acceso Web

Hay tres formas de conectarse a un clúster con balanceo de carga:

- Usando un **Cliente Generado** programa ejecutable, creado por el Generador de Cliente Portátil)
- Usando un **Acceso al Portal Web** activándolo en la ventana de Preferencias del Portal Web.
- Con el TSplus App desde tu dispositivo móvil.

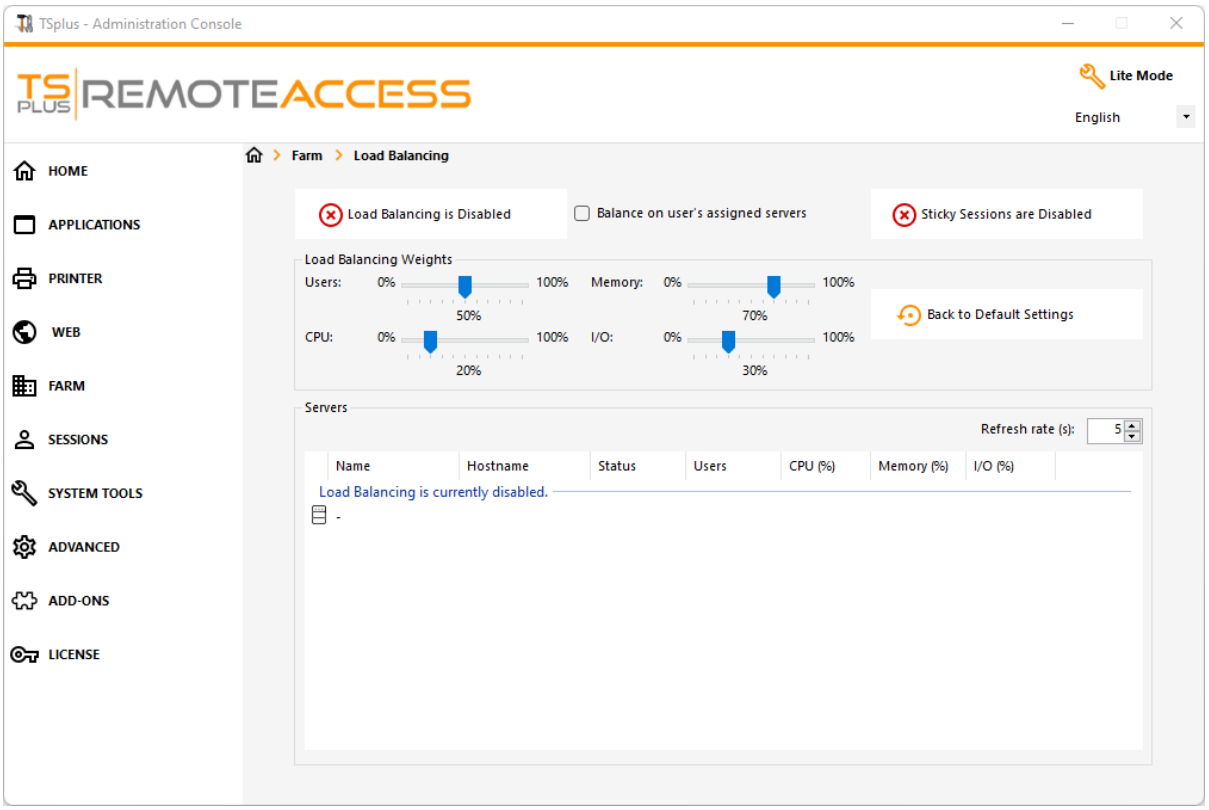
Ventana Principal de Balanceo de Carga

El Administrador de Balanceo de Carga se puede encontrar en la pestaña Granja de la Herramienta de Administración:



Esta ventana le permite configurar el balanceo de carga. Enumera todos los servidores en su granja de servidores con balanceo de carga y le permite habilitar, deshabilitar y configurar el balanceo de carga (más sobre esto a continuación).

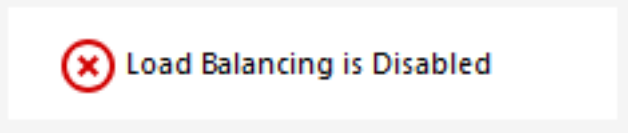
Haga clic en los botones de la imagen a continuación para acceder a la información correspondiente:



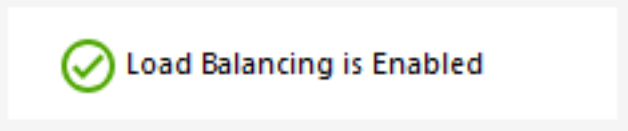
En la parte superior de la ventana de Balanceo de Carga, verás un gran botón:

- Este botón muestra el estado actual del balanceo de carga.
- Si haces clic en él, habilitará o deshabilitará el balanceo de carga dependiendo de su estado actual.

Aquí está el botón cuando el balanceo de carga está **Deshabilitado** Un clic en él lo activará.



Aquí está el botón cuando el balanceo de carga está **Habilitado** Un clic en él lo desactivará.



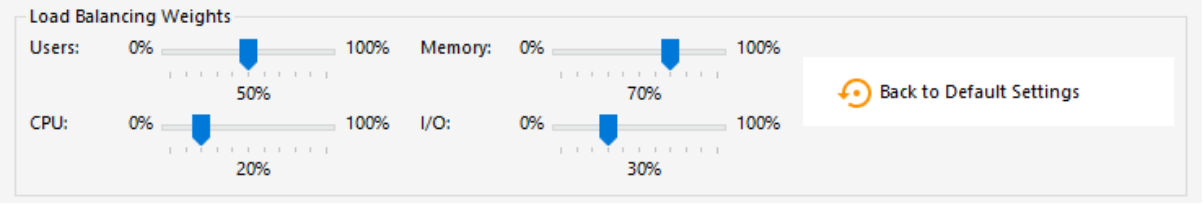
¿Cómo elige un servidor el Balanceo de Carga?

Cuando se habilita el balanceo de carga, el usuario será enviado al servidor menos cargado en el momento de su conexión.

Para determinar cuál es el servidor menos cargado, se calcula la carga de cada servidor utilizando un promedio ponderado entre varios indicadores de rendimiento:

- número de usuarios conectados
- uso del procesador
- uso de memoria
- uso del disco

Puedes modificar el peso (importancia) de estos indicadores utilizando los siguientes deslizadores:



Usando estos deslizadores, podrá ajustar el Balanceo de Carga y optimizarlo según sus propias necesidades. Por ejemplo, si sus usuarios inician una aplicación empresarial con grandes requisitos de memoria, podría ser una buena idea aumentar el impacto de la RAM en el cálculo de carga utilizando el deslizante de "Memoria".

También puede restablecer estos valores haciendo clic en el botón "Restablecer a la configuración predeterminada".

¿Cómo se calcula la carga del servidor?

La carga de cada servidor se calcula cuando es necesario para decidir a qué servidor debe ser enviado el usuario.

Para este cálculo, utilizamos un **promedio ponderado** entre 4 métricas de hardware.

Los 4 controladores te permiten dar más (o menos) peso a cada una de estas métricas, que son:

- Usuarios: número de usuarios conectados
- CPU: porcentaje de tiempo de procesador no ocioso
- Memoria: porcentaje de memoria utilizada
- I/O: porcentaje de tiempo de disco no inactivo

Por ejemplo, si colocas el control deslizante de "Memoria" en su lado derecho y todos los demás controles deslizantes en su lado izquierdo, la carga de cada servidor se calculará utilizando casi solo el porcentaje de memoria utilizada, y tus usuarios serán enviados al servidor que tenga la mayor cantidad de memoria disponible.

- Cuando un control deslizante está completamente a la izquierda, el peso utilizado en el cálculo de carga será 1.
- Cuando un control deslizante está completamente a la izquierda, el peso utilizado en el cálculo de carga será 100.

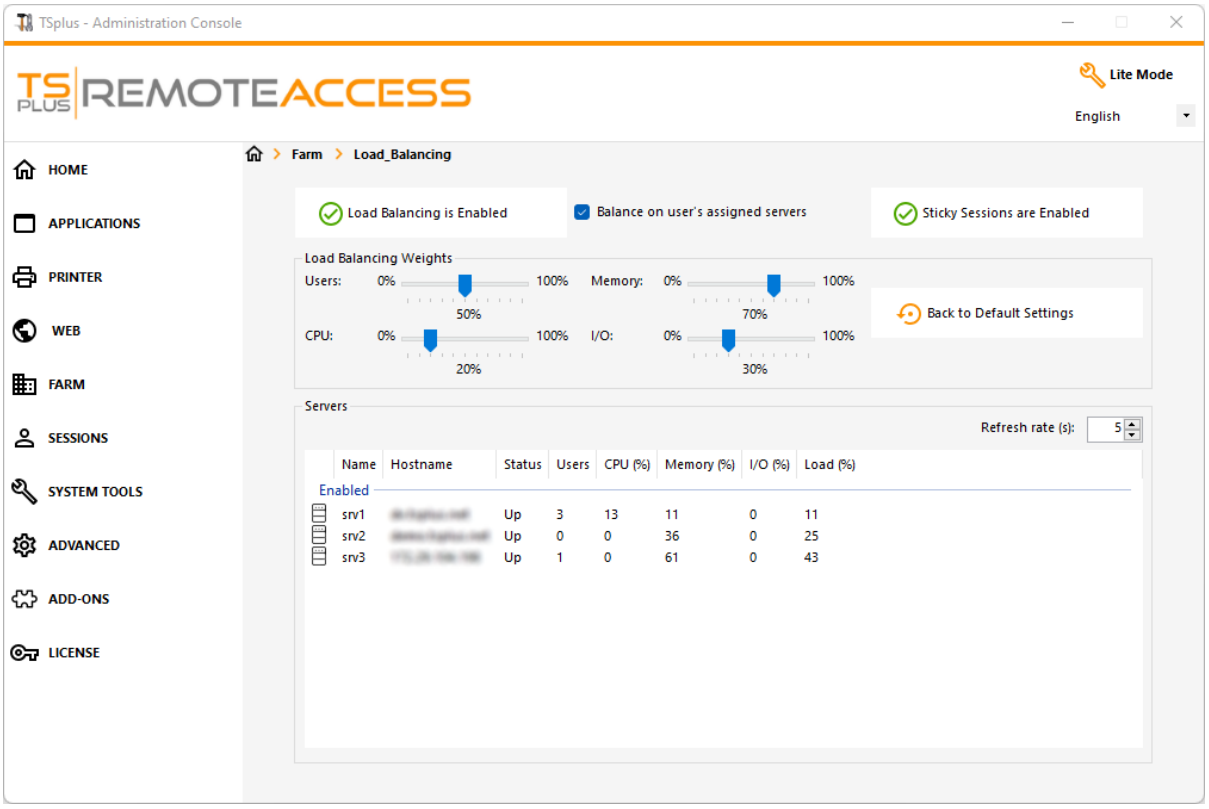
Además, la carga de un servidor dado depende de la relación [recursos utilizados / recursos totales]; por lo tanto, si un servidor A es el doble de potente que un servidor B, se deben enviar el doble de usuarios al servidor A que al servidor B (todas las demás cosas siendo iguales).

Puedes ver la lista de estado de servidores con balanceo de carga y detalles sobre los indicadores de rendimiento de cada servidor.

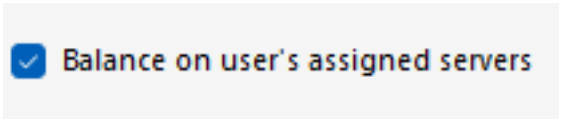
Los servidores están ordenados desde el menos cargado hasta el más cargado según su configuración.

La lista de estado de servidores con balanceo de carga se actualiza automáticamente. Esta actualización automática se detiene si la conexión se vuelve no disponible. Puedes cambiar la

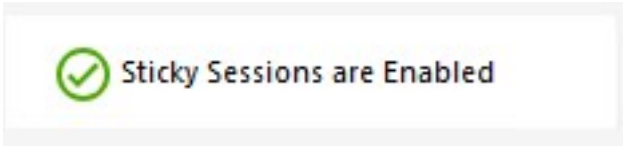
tasa de actualización en la esquina superior derecha del cuadro "Servidor".



El balanceo de carga también se puede realizar directamente en el servidor asignado al usuario utilizando el **casilla "Equilibrio en los servidores asignados al usuario"** .
Como resultado, podrá realizar balanceo de carga en los servidores del departamento de contabilidad solo para usuarios contables, una vez que estos servidores específicos hayan sido asignados a los usuarios contables.



Puedes activar la función de sesión persistente haciendo clic en el botón derecho de la ventana de Load balancing:



Habilitando **listado de sesiones existentes en la web** es necesario para la función de sesiones adhesivas de balanceo de carga.

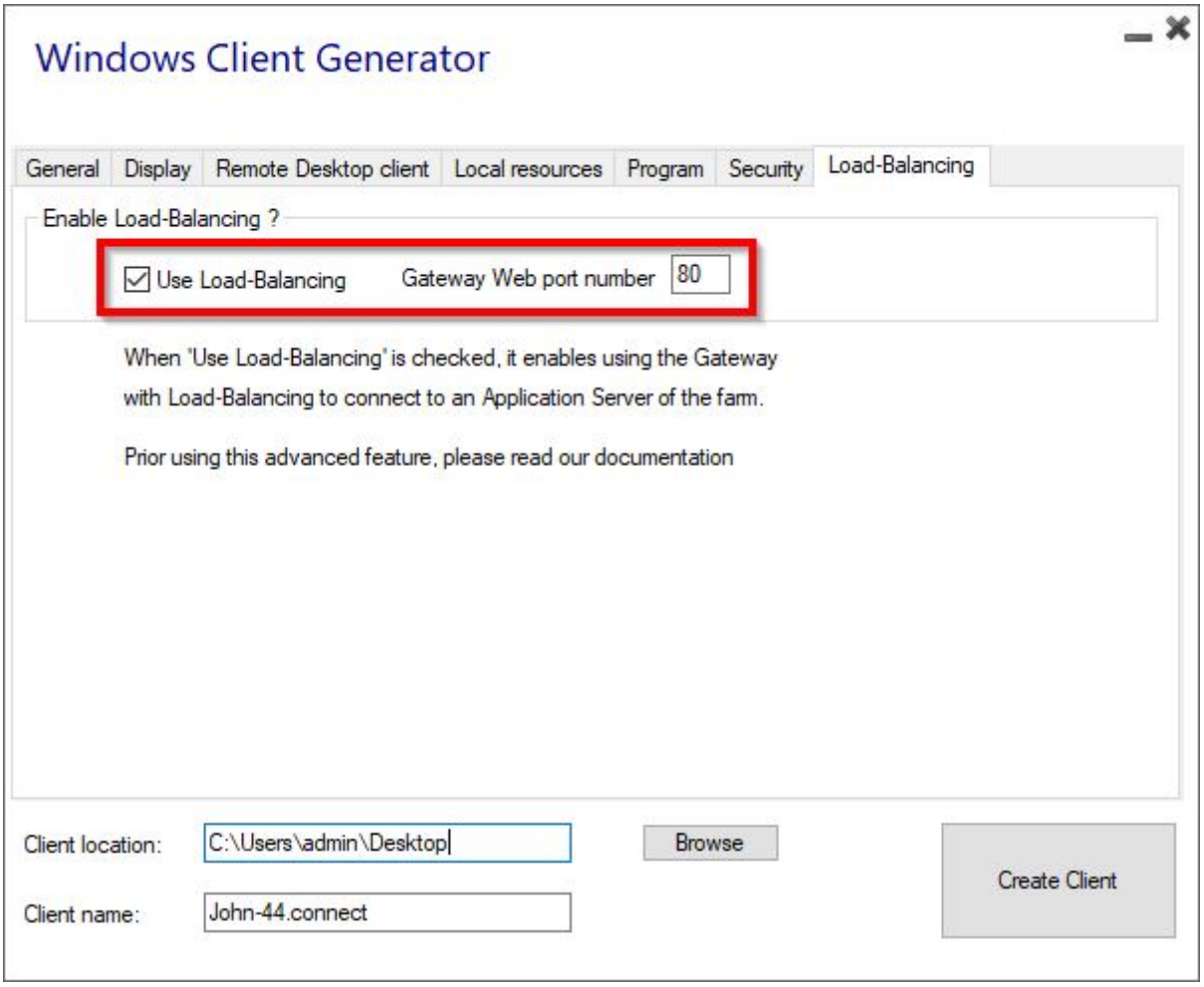
Le permitirá reconectarse a una sesión desconectada en lugar de abrir una nueva sesión en un servidor diferente.

Para habilitar **listado de sesiones existentes en la web** , establezca lo siguiente configuración a "no".

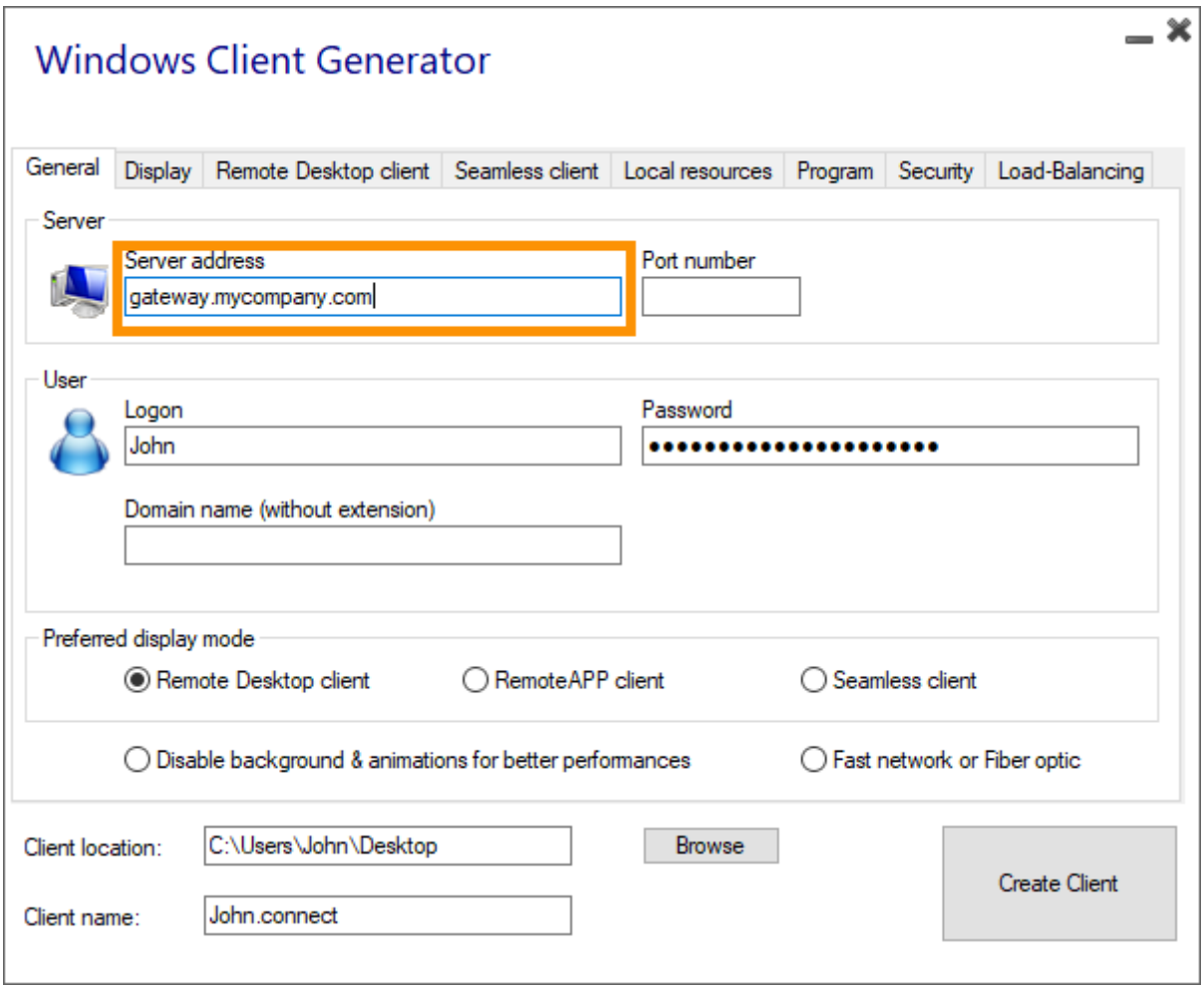
Balanceo de Carga utilizando un Cliente de Conexión

Si deseas generar un Cliente de Conexión para que un usuario se conecte al servidor menos cargado , necesitarás de la Generador de Clientes en el " Balanceo de Carga " pestaña a:

- Marque la casilla "Usar balanceo de carga"
- Rellene el campo "Número de puerto web del Gateway" con el puerto HTTP o HTTPS utilizado por su servidor Gateway.



- Utilice la dirección IP pública o el nombre de host de su Servidor Gateway directamente en el campo "Servidor".


Windows Client Generator
General
Display
Remote Desktop client
Seamless client
Local resources
Program
Security
Load-Balancing
Server
Server address
gateway.mycompany.com
Port number
User
Logon
John
Password
Domain name (without extension)
Preferred display mode
Remote Desktop client
RemoteAPP client
Seamless client
Disable background & animations for better performances
Fast network or Fiber optic
Client location:
C:\Users\John\Desktop
Browse
Client name:
John.connect
Create Client

Farm Manager API

Estamos emocionados de ofrecerle una API poderosa diseñada para proporcionar capacidades de gestión completas para sus granjas de servidores.

Esta API le permite integrar sin problemas nuestro software con su infraestructura existente, lo que le permite gestionar y automatizar las operaciones del servidor con sus propios scripts personalizados.

Descubre todo el potencial de nuestro software con la robusta y versátil API que ofrecemos.

Requisitos

Para consultar la API del administrador de la granja, su servidor necesitará:

- tener un certificado SSL/TLS válido
- ser abierto en el puerto 19956
- ser accesible utilizando el dominio que cubre su certificado.

Ejemplos de uso

Por ejemplo, los administradores pueden usar el **Granja > Obtener lista de servidores** función para recuperar una lista completa de todos los servidores dentro de su granja, optimizando la gestión de inventario. El **Granja > Inicializar granja** la función permite la configuración rápida de una nueva granja de servidores, asegurando un proceso de implementación fluido. Para la gestión de servidores específica del usuario, el **Granja > Lista de servidores asignados a un usuario** La función ayuda a rastrear y gestionar las asignaciones del servidor.

En escenarios de balanceo de carga, el **Balanceo de carga > elegir servidor** y **Balanceo de carga > Recargar** las funciones permiten la selección dinámica de servidores y la recarga de configuraciones del equilibrador de carga, optimizando la distribución de recursos y el rendimiento. El **ReverseProxy > Recargar** la función garantiza que los cambios en la configuración del proxy se apliquen sin tiempo de inactividad. Además, el **Servidor > Agregar** y **Servidor > Editar** las funciones facilitan la adición y modificación sin problemas de servidores en la granja.

Los administradores pueden mejorar aún más sus operaciones utilizando el **Configuración > listar configuraciones** y **Configuración > Aplicar configuraciones** funciones para recuperar y aplicar configuraciones en toda la granja de servidores.

Para la gestión de sesiones, el **Sesión > Desconectar** y **Sesión > Cerrar sesión** las funciones permiten la terminación controlada de las sesiones de usuario, mientras que el **Sesión > Listar sesiones de usuarios** proporciona una vista detallada de las sesiones activas con fines de monitoreo.

Al aprovechar estas potentes funciones de API, puede lograr una mayor automatización, eficiencia y control sobre sus procesos de gestión de servidores, asegurando un rendimiento y una fiabilidad óptimos de su infraestructura.

Documentación

Documentación completa de esta API se puede encontrar aquí : Documentación de la API

Resumen

Resumen y Nomenclatura

El objetivo de las funciones de TSplus Farm es permitir al Administrador gestionar todos sus servidores TSPlus desde un único servidor. Este servidor puede ser referido como el **Controlador de Granja** .

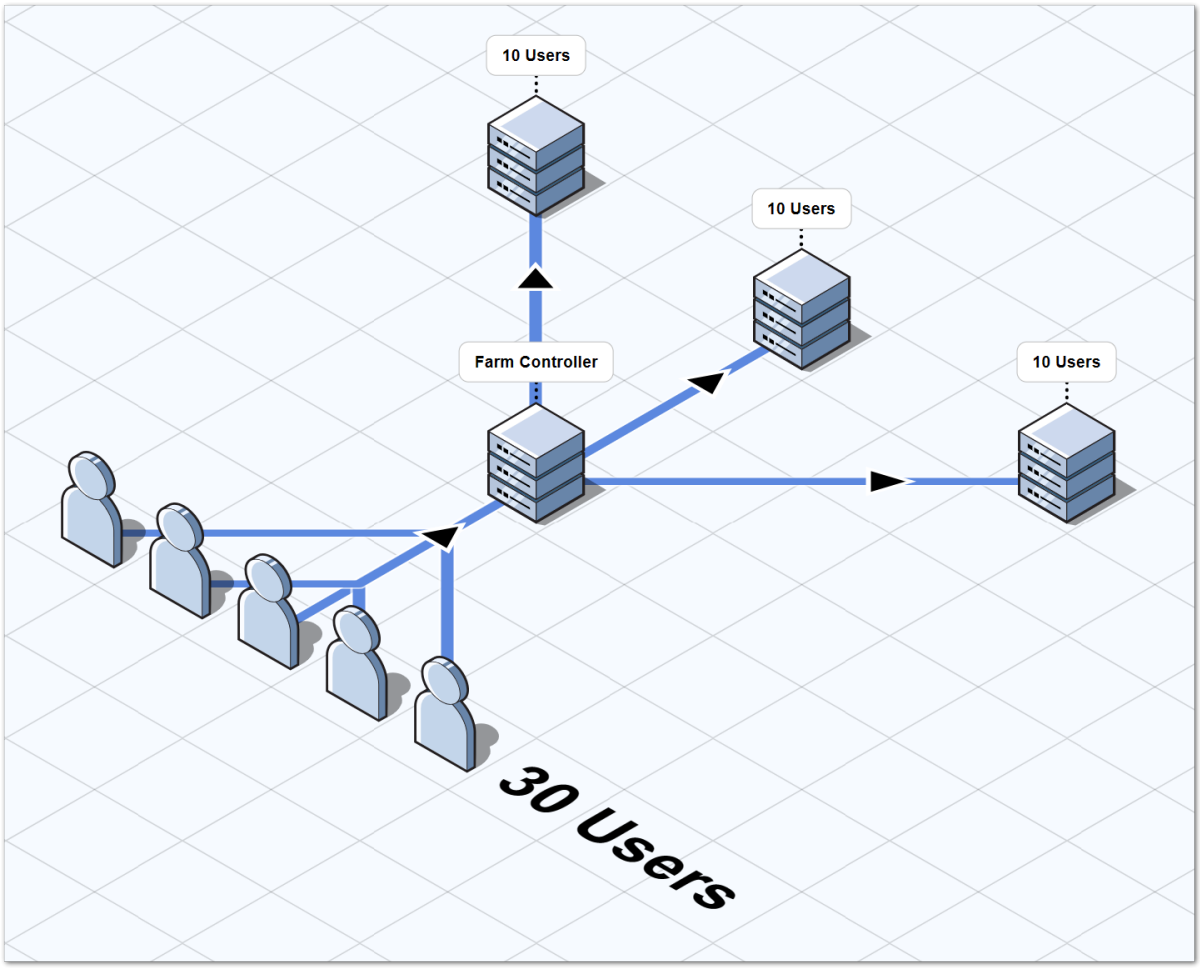
Los servidores de TSplus en la Granja se llaman el **Servidores de Aplicaciones** , o solo Servidores.

Este Controlador de Granja, una vez que tenga su granja poblada con Servidores de Aplicaciones, también se convertirá en un **Servidor de puerta de enlace** una vez que habilitó cualquiera de las funciones de la Granja, como:

- Load balancing
- Proxy inverso
- Asignar Servidores

Este servidor de puerta de enlace se convertirá básicamente en el punto de entrada principal de todos sus usuarios cuando se habilite "Balanceo de Carga" o "Asignar Servidores".

Finalmente, este Controlador de Granja también le permitirá monitorear cualquier Servidor de Aplicaciones y enviar fácilmente configuraciones relacionadas con TSplus, como Aplicaciones y configuraciones Avanzadas, desde su Controlador de Granja a sus Servidores de Aplicaciones.



TSplus Granja de Servidores Arquitectura

Hay 2 opciones para implementar un conjunto de servidores TSplus:

Opción 1 Todos sus servidores tienen direcciones IP públicas y se pueden alcanzar desde Internet.

O bien

Opción 2 Solo se puede acceder al Portal de Gateway desde Internet. El Servidor Gateway está proporcionando un "Rol de Proxy Inverso".

En ambas opciones:

- Cada servidor tiene la misma configuración de TSplus.
- Cada servidor tiene los mismos puertos HTTP/HTTPS.
- Para publicar una nueva aplicación, simplemente agrégala a tus usuarios/grupos de usuarios en el AdminTool.

Por supuesto, asegúrate de que esta aplicación esté instalada en los Servidores de Aplicaciones objetivo.

Todos los tipos de acceso web están disponibles sin ninguna configuración específica: RemoteApp y clientes HTML5.

Opción 1 - Todos los servidores tienen su propia dirección IP pública y se pueden alcanzar desde Internet.

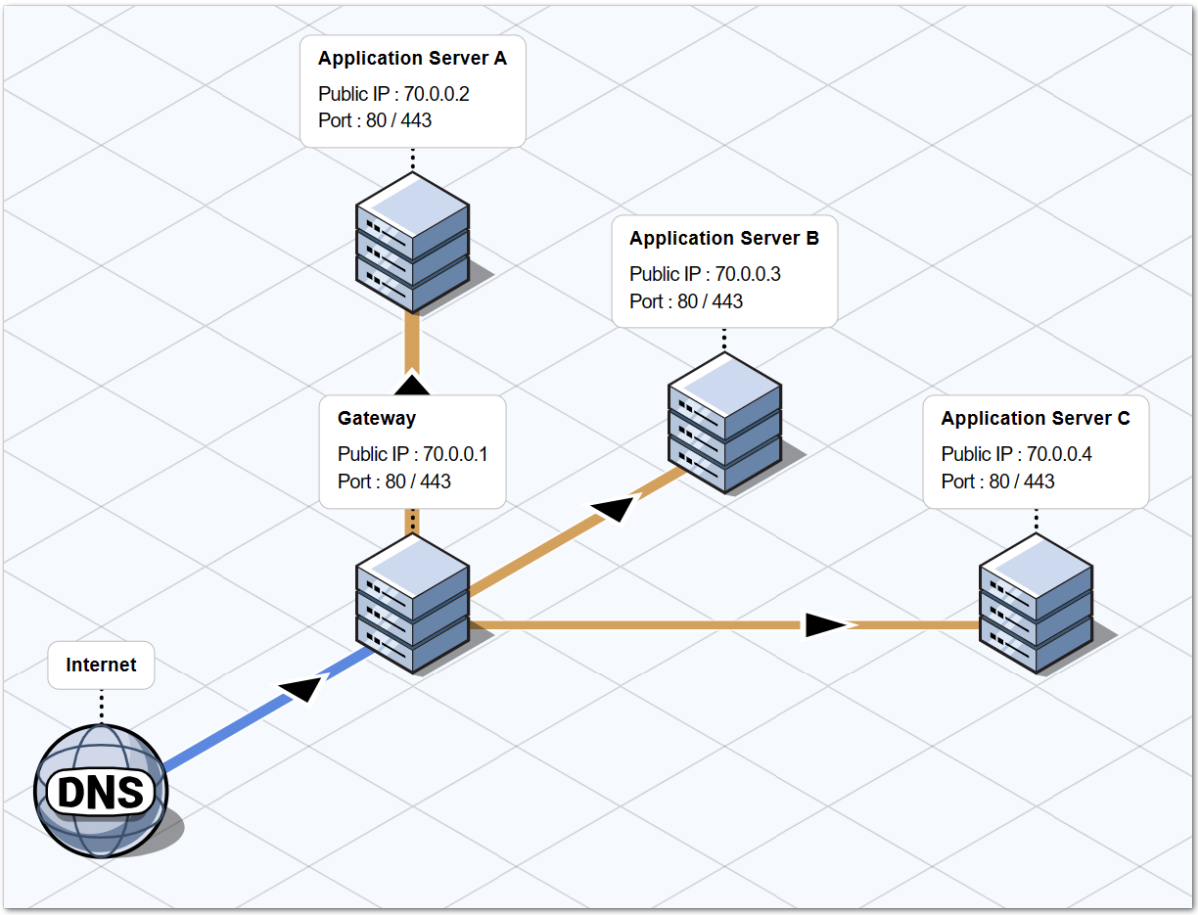
Esta es la arquitectura recomendada para usar Terminal Service Plus Gateway.

Esta arquitectura sigue las mejores prácticas y permite al Administrador de TI industrializar su entorno:

- Cada servidor tiene la misma configuración de Terminal Service Plus.
- Cada servidor tiene los mismos puertos HTTP/HTTPS
- Desplegar un nuevo servidor de aplicaciones es solo cuestión de minutos (solo agrega el servidor a la granja en el AdminTool en el servidor Gateway)

Con esta arquitectura, todos los tipos de acceso están disponibles sin ninguna configuración específica: Remoteapp y clientes HTML5.

Esta arquitectura se describe en el diagrama a continuación:



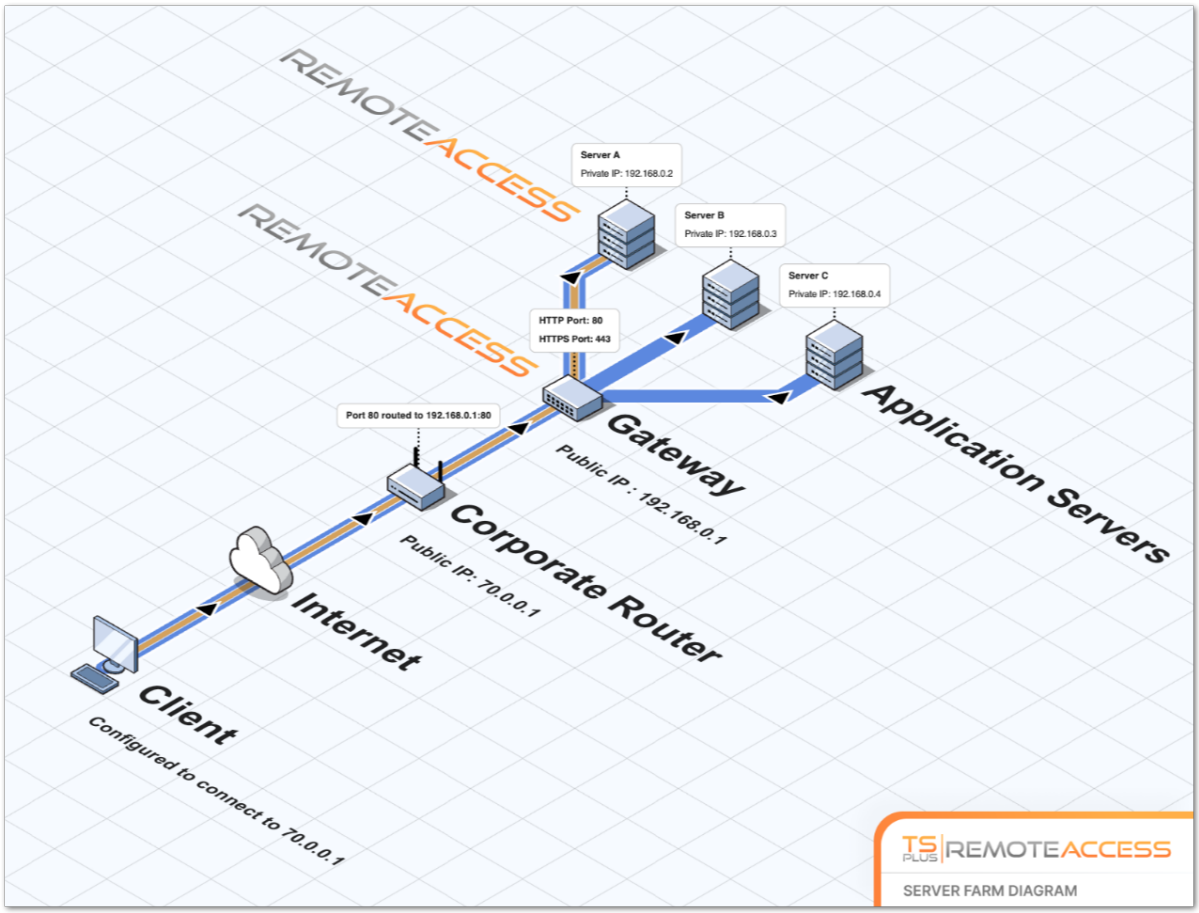
-
-
  -

Opción 2: Solo se puede acceder al Portal Gateway desde Internet e incluye un "Rol de Proxy Inverso".

El Gateway de Terminal Service Plus también se puede configurar con solo 1 dirección IP pública.

El Gateway redirige cualquier solicitud de conexión externa a cualquier servidor disponible. Si no utiliza la función de balanceo de carga, los usuarios se conectarán a su(s) servidor(es) asignado(s).

Esta arquitectura se describe en el diagrama a continuación:



Para más información sobre el rol de Proxy Inverso, consulte el Documentación de la función de Proxy Inverso .

Historial de lanzamientos

- API 1.5 (lanzado con TSplus 15.50)
  - Integración de Reverse-Proxy, configuración de balanceo de carga y asignación de servidor de aplicaciones
  - Añadida la sincronización entre las aplicaciones/configuraciones del controlador de la granja y todos los servidores de aplicaciones.

- API 1.4 (lanzado con TSplus 10.10)
  - Monitoreo centralizado de balanceo de carga
  - Habilitar/Deshabilitar un Servidor en el Administrador de Balanceo de Carga de TSplus
  - Traducciones en múltiples idiomas (se utilizará el idioma de TSplus)
  - Se añadieron varias configuraciones + se corrigieron errores de visualización

- API 1.3 (lanzado con TSplus 9.70)
  - Configuración de monitoreo y gestión centralizados (Configuraciones globales / Panel flotante / Cliente RemoteApp / Cliente HTML5)

- API 1.2 (lanzado con TSplus 9.60)
  - Gerente de Granja

    - Gestión centralizada de servidores (agregar/eliminar)
    - Monitoreo y gestión centralizados de sesiones (mensajes/desconexión/cierre de sesión)

- API 1.1 (lanzado con TSplus 9.30)
    - Internos de balanceo de carga
    - Balanceo de Carga Sesiones Pegajosas

Requisitos

Requisitos de hardware

Controlador de granja y servidores de aplicaciones tienen el estándar Requisitos de Terminal Service Plus para hardware.

Requisitos del sistema operativo

Los controladores de granja y los servidores de aplicaciones deben utilizar uno de los siguientes sistemas operativos:

- Windows **7 Pro**
- Windows **8/8.1 Pro**
- Windows **10 Pro**
- Windows **11 Pro**
- Windows **Server 2008 SP2/Small Business Server SP2 o 2008 R2 SP1**
- Windows **Server 2012 o 2012 R2**
- Windows **Server 2016**
- Windows **Servidor 2019**
- Windows **Server 2022**
- Windows **Servidor 2025**

Ambas arquitecturas de 32 y 64 bits son compatibles.

Requisitos de red

Cada servidor de aplicaciones debe ser accesible desde el controlador de la granja.

Más específicamente, el Controlador de Granja enviará solicitudes a cada Servidor de Aplicaciones en su puerto API (19955 por defecto) y este puerto debe estar abierto en cualquier firewall que se encuentre entre el Controlador de Granja y los Servidores de Aplicaciones.

La latencia de la red debe ser baja entre el Controlador de Granja y los Servidores de Aplicaciones. Se recomienda una latencia inferior a 200 ms, y se requiere una latencia inferior a 2 000 ms.

Requisitos del software

Se requiere .NET 2.0 o superior; esto no debería ser un problema, ya que una versión compatible de .NET está habilitada por defecto en cada sistema operativo compatible con Terminal Service Plus Farm.

Licencia y Requisitos de Versión de Terminal Service Plus

Terminal Service Plus debe estar en la edición "Enterprise" en el Controlador de Granja y en todos los Servidores de Aplicaciones.

Todos los servidores también deben ejecutar la misma versión de Terminal Service Plus.

Requisitos de configuración

Los controladores de granja y los servidores de aplicaciones deben tener la misma fecha/hora configurada. Se recomienda encarecidamente sincronizar el reloj de Windows de todos los servidores con un servidor de hora de Internet si no se ha hecho ya.

Requisitos de los usuarios

Un Active Directory es **no** es necesario, sin embargo, si tiene un Active Directory, entonces sus Administradores de Dominio también deben ser Administradores Locales del Controlador de Granja para poder usar Terminal Service Plus Farm Manager.

Proxy inverso

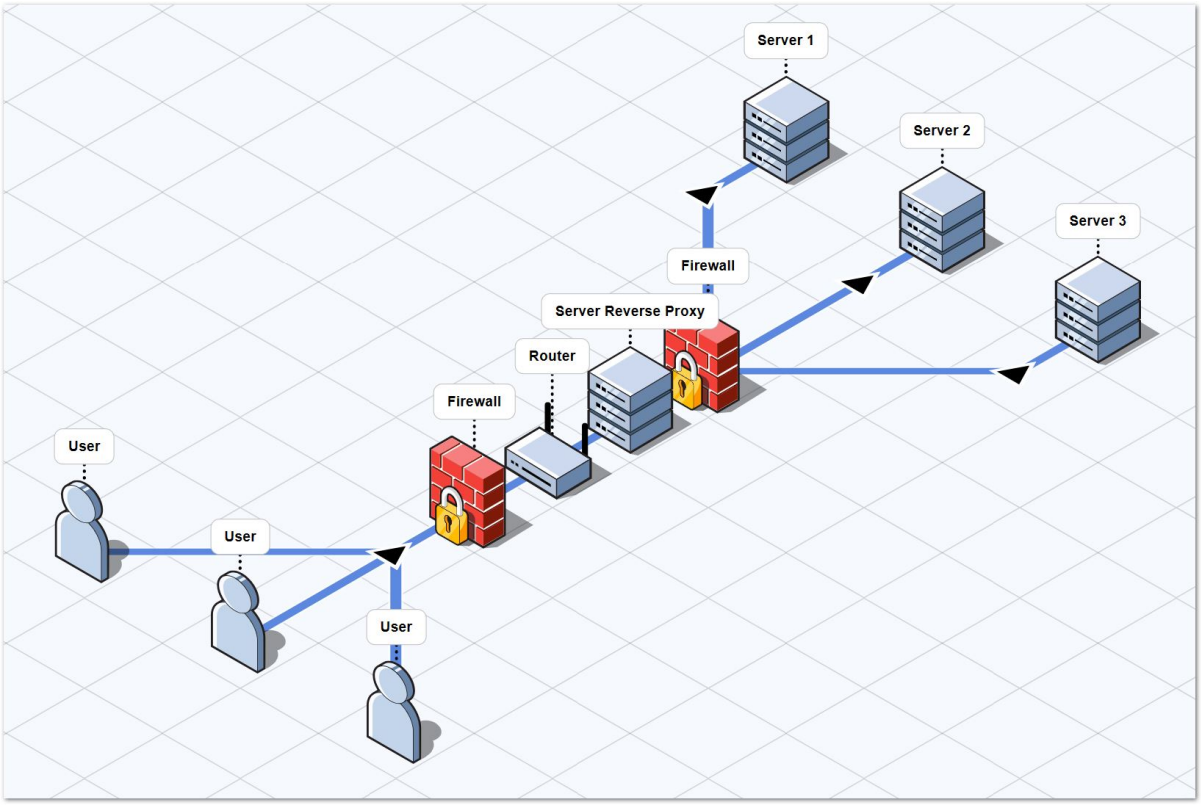
Resumen

Esta función está disponible en la Edición Empresarial de TSplus.

El sistema de Proxy Inverso actúa como un intermediario para que sus servidores asociados sean contactados por cualquier cliente.

La ventaja de usar un proxy inverso es simple: ya no necesitarás crear tantas reglas de redirección de puertos como el número de servidores TSplus.

Ya sea que esté utilizando la función de balanceo de carga o no, necesita activarla para conectarse utilizando el proxy inverso. En TSplus, proporciona un punto de acceso único a un conjunto de servidores TSplus balanceados.

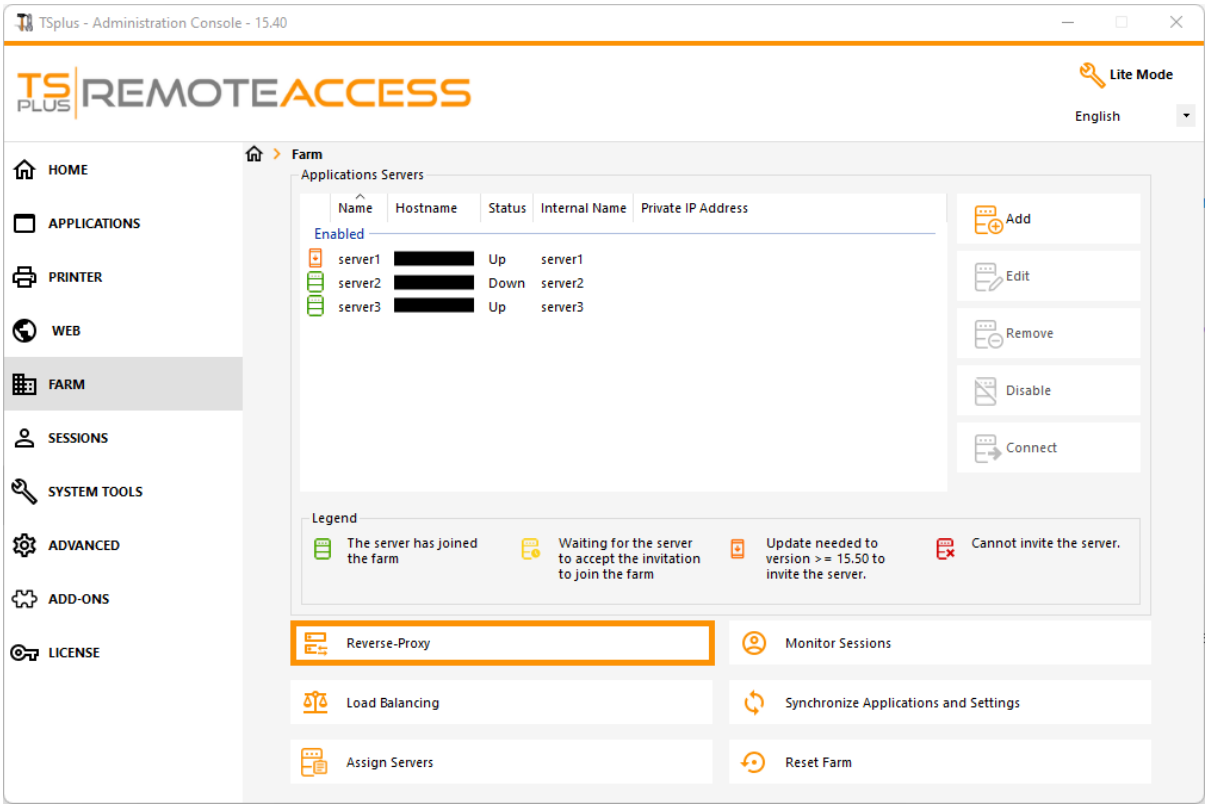


Este punto de acceso único será su Servidor Gateway Portal TSplus Web.

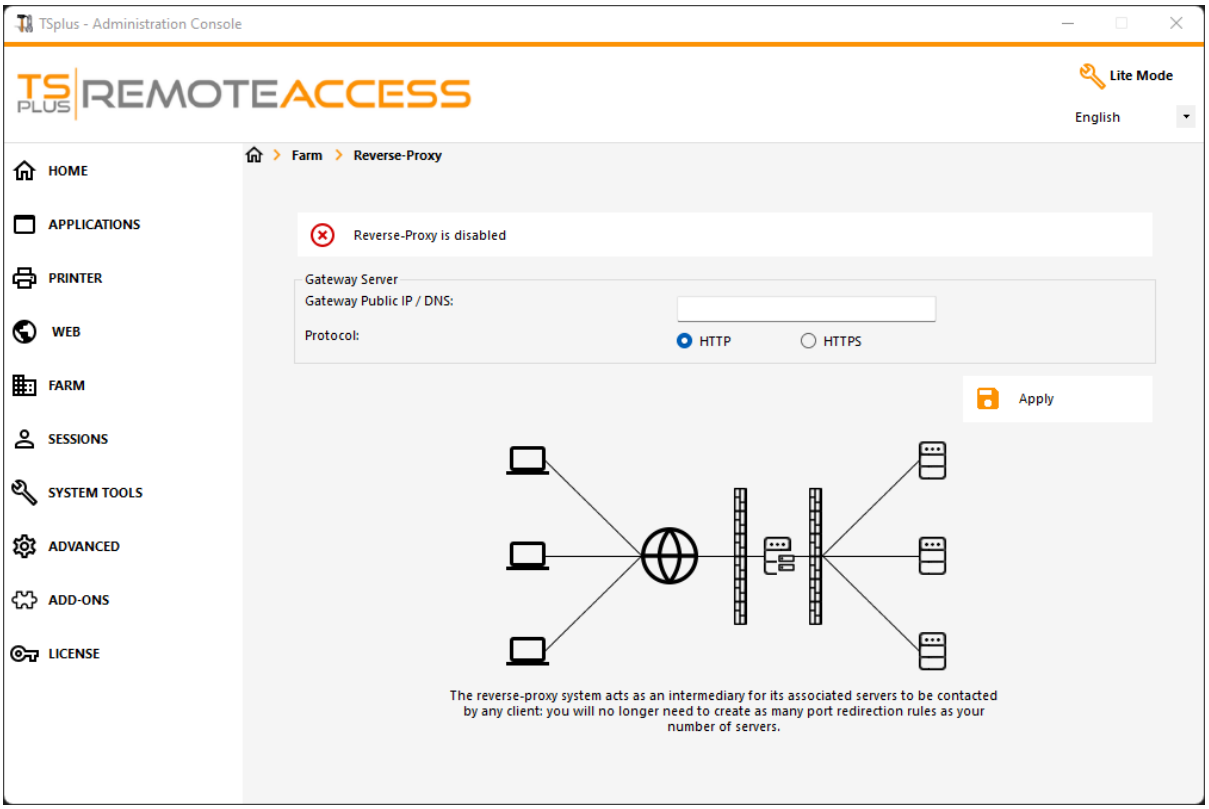
Dado que este servidor va a ser accedido de forma remota, necesitarás configurar una regla de redirección de puertos en tu enrutador, incluyendo los puertos http o https dependiendo de tu preferencia (80 siendo el puerto predeterminado para http y 443 para https).

Configuración

Puedes acceder a la interfaz de configuración del Proxy Inverso a través de la pestaña FARM:



Haga clic en el botón de Reverse-Proxy.



- Haga clic en el botón "Reverse-Proxy está deshabilitado" para activarlo.
- La IP pública del Gateway debe configurarse con una dirección IP válida fija o un nombre de dominio.
- Seleccione HTTP o HTTPS como su método de conexión preferido, los servidores de su granja deben poder comunicarse entre sí a través del puerto 80 o 443, dependiendo del método de conexión que utilice. También es importante que su firewall de Windows no bloquee estos puertos.

Una vez que haya completado su configuración, haga clic en "Aplicar" para guardar estos ajustes de Proxy Inverso.

Acceso a servidores de aplicaciones a través del Servidor Gateway

Una vez habilitada y operativa, la función de Proxy Inverso le permite acceder al servidor de aplicaciones utilizando una URL especial con el siguiente formato:
1 :// **2** : **3** /~~ **4**
con:

- (1): el protocolo de Proxy Inverso configurado
- la dirección IP pública del servidor Gateway o el nombre de dominio
- (3): el puerto web del servidor Gateway asociado al protocolo de Proxy Inverso configurado
- el nombre interno del servidor de aplicaciones utilizado por Reverse Proxy

Por ejemplo, asumiendo que:

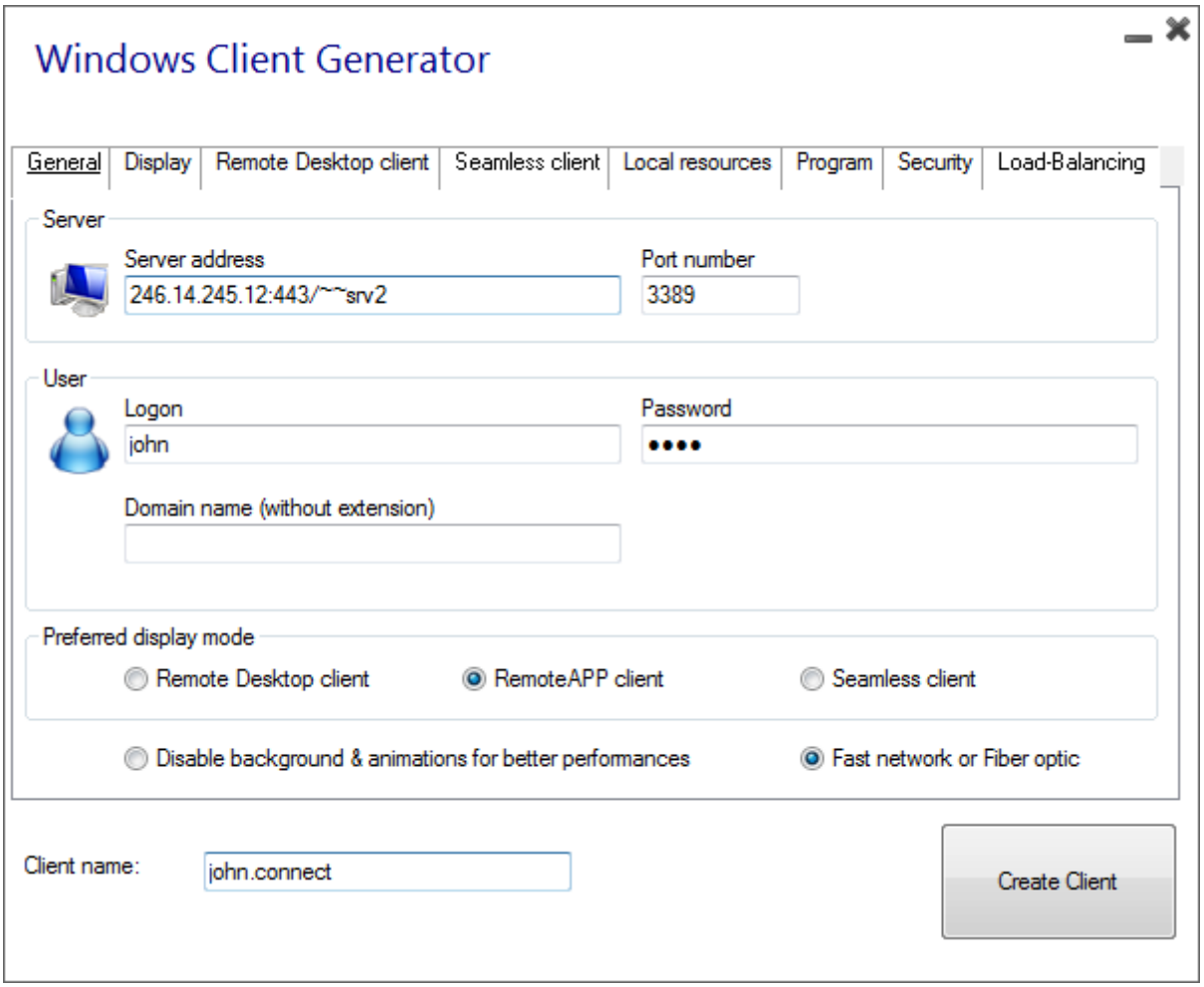
- el protocolo de proxy inverso configurado es HTTPS
- tu Servidor Gateway tiene la IP pública 1.1.1.1
- su servidor de puerta de enlace está utilizando el puerto HTTPS 443
- el servidor de aplicaciones al que desea conectarse utiliza el nombre interno "srv2"

La URL especial que se debe utilizar para acceder al servidor de aplicaciones objetivo será 1.1.1.1:443/~~srv2

Como resultado, puedes acceder al portal web de este servidor de aplicaciones utilizando esta URL especial.

También puede generar un Cliente de Conexión que se conectará a este Servidor de Aplicaciones específico a través del Servidor Gateway utilizando este mismo método. Simplemente use la URL especial en el campo de dirección del servidor del Generador de Cliente de Conexión.

Por ejemplo:


Windows Client Generator
General
Display
Remote Desktop client
Seamless client
Local resources
Program
Security
Load-Balancing
Server
Server address
246.14.245.12:443/~~srv2
Port number
3389
User
Logon
john
Password
Domain name (without extension)
Preferred display mode
Remote Desktop client
RemoteAPP client
Seamless client
Disable background & animations for better performances
Fast network or Fiber optic
Client name:
john.connect
Create Client

Asignación de Servidor

Resumen

El controlador de la granja puede actuar como un servidor de puerta de enlace, redirigiendo a los usuarios al conectarse a servidores de aplicaciones específicos de su granja. Podrá asignar uno o varios servidores a un usuario / un grupo local / un grupo de Active Directory.

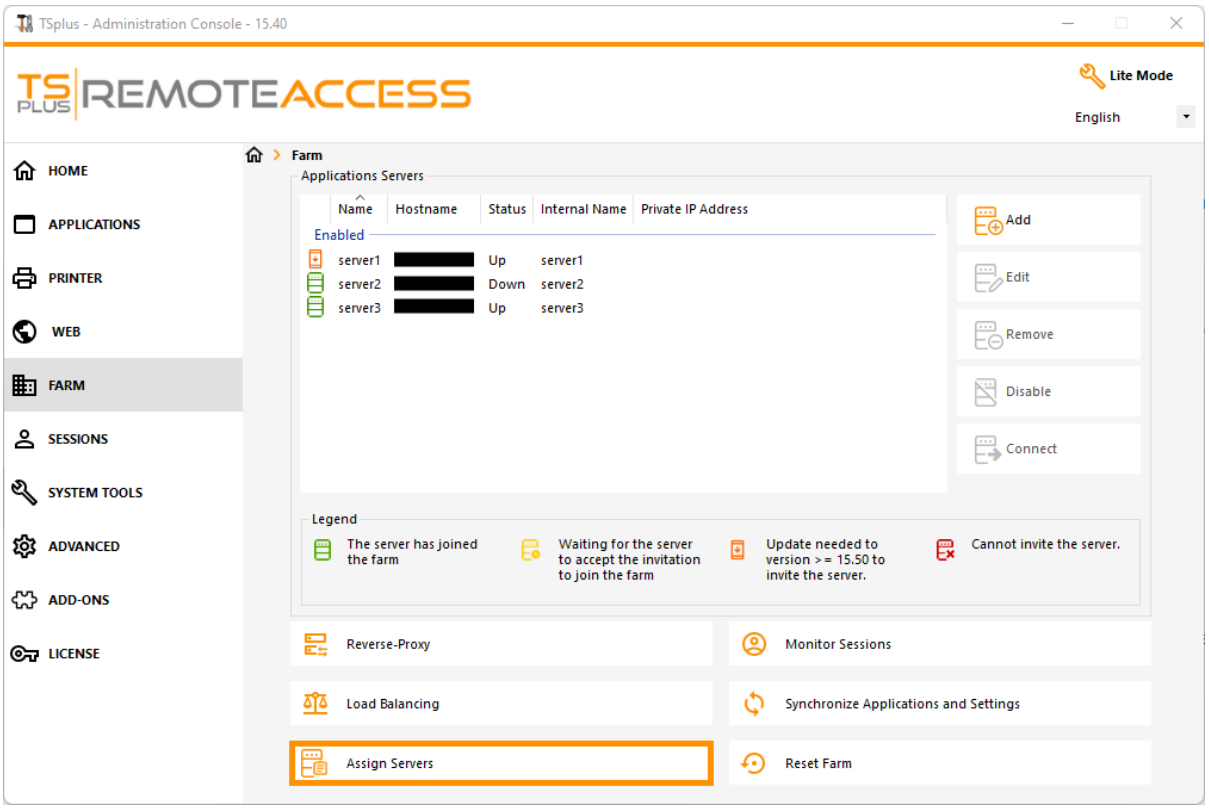
Importante: La asignación de servidores solo funciona desde el Portal Web de TSplus, y no con clientes de conexión.

Si el usuario tiene más de un servidor asignado, podrá elegir qué servidor desea acceder en la lista de servidores asignados a él.

Si la granja está dentro de un Dominio, el Gateway utilizará sus credenciales de AD y el usuario se conectará con Single Sign-On (SSO).

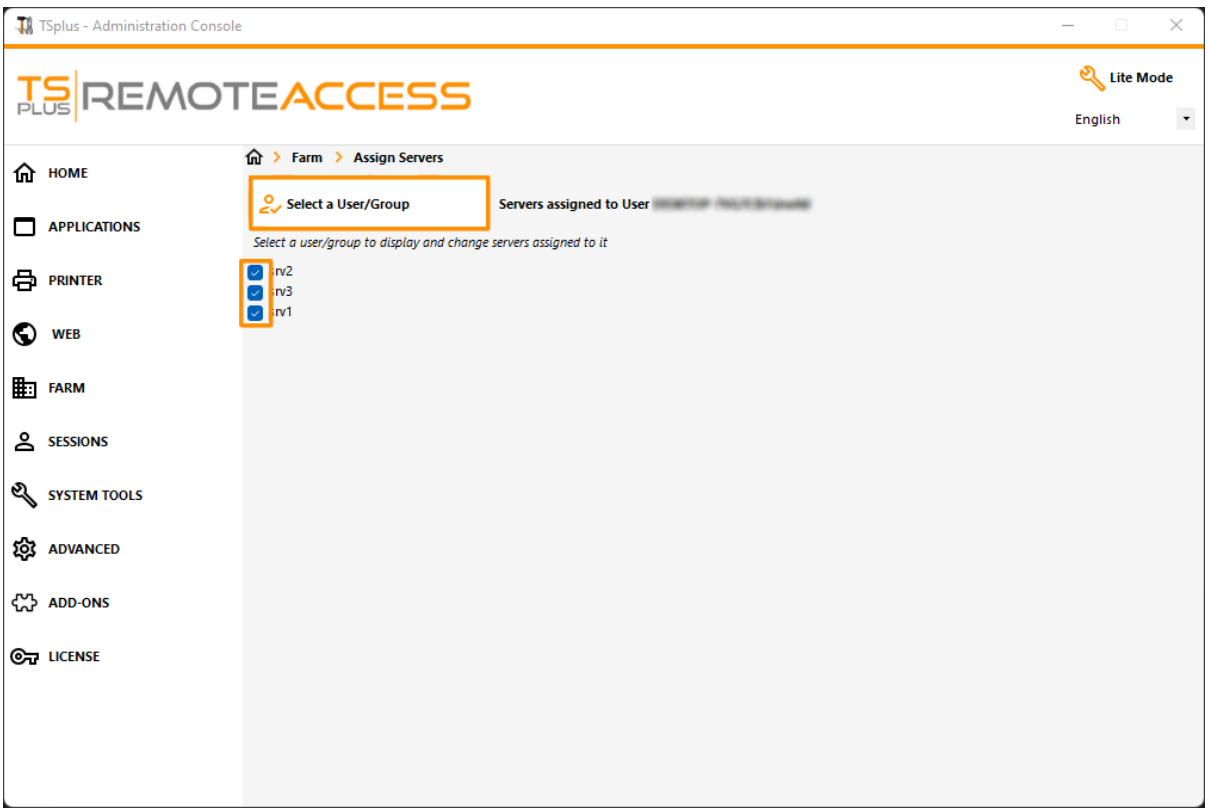
De lo contrario, debe tener las mismas credenciales locales en cada servidor.

Para asignar servidores, haga clic en el botón “Asignar Servidores”:



Para asignar un servidor a un usuario, simplemente selecciónelo con el botón “Seleccionar un Usuario/Grupo” y luego marque la casilla del servidor en la lista de “Servidores”.

Para eliminar un servidor asignado a un usuario, simplemente desmarque la casilla del servidor en la lista de "Servidores".

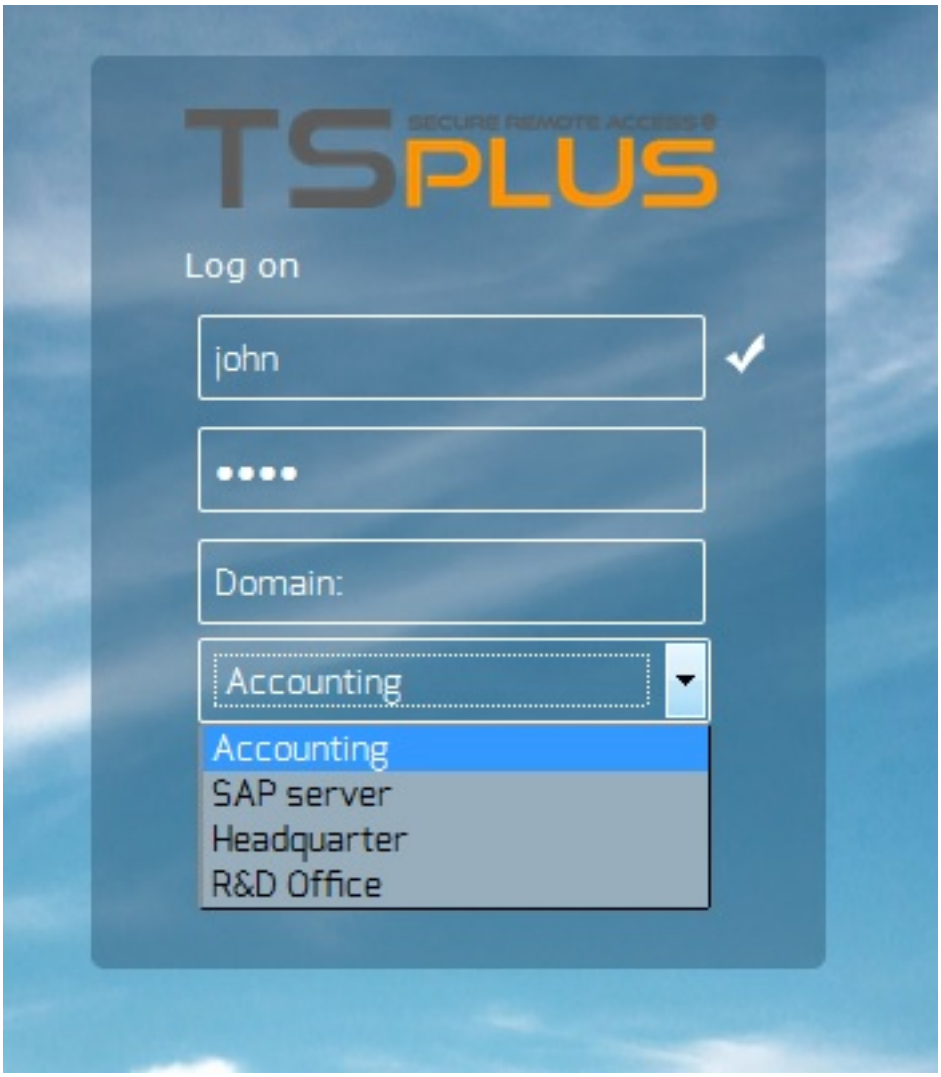


Notas Importantes

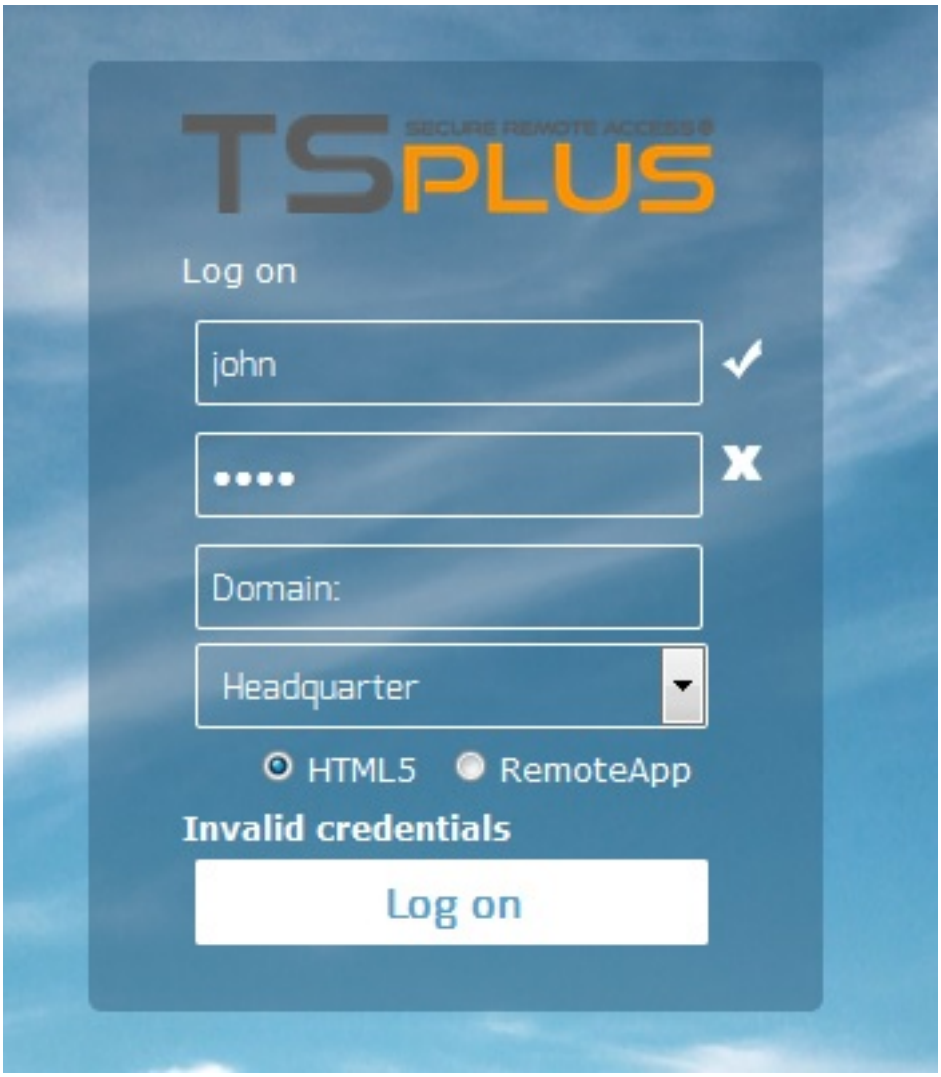
- El ejemplo anterior es para un Dominio o un Grupo de Trabajo.
- Si utiliza un grupo de trabajo, los inicios de sesión de los usuarios deben ser los mismos en cada servidor de aplicaciones que asigne.
- Esta función de asignación de servidores se puede configurar y utilizar simultáneamente con la función de balanceo de carga, lo que permite al controlador de la granja equilibrar la carga en los servidores asignados. Para hacerlo, habilite el balanceo de carga y marque la opción "Balancear carga en servidores asignados".
- Si la función de Asignación de Servidor y el Balanceo de Carga están habilitados, a menos que la opción "Balancear carga en servidores asignados" en la configuración de Balanceo de Carga esté habilitada, el Servidor Gateway redirigirá a los usuarios al servidor menos cargado sin importar sus servidores asignados.

Ejemplo de lo que obtendrán los usuarios al conectarse al Gateway

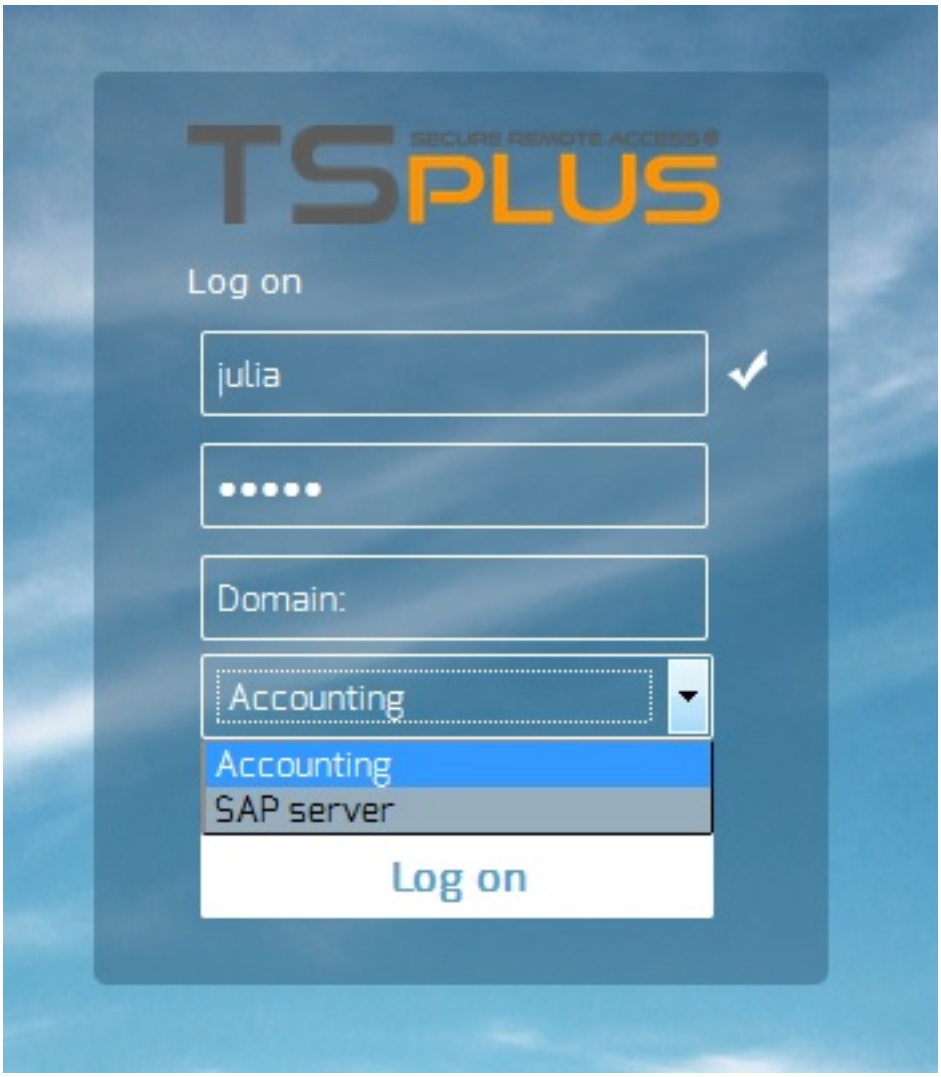
John puede seleccionar el servidor. Él quiere y obtendrá un inicio de sesión automático en este servidor:



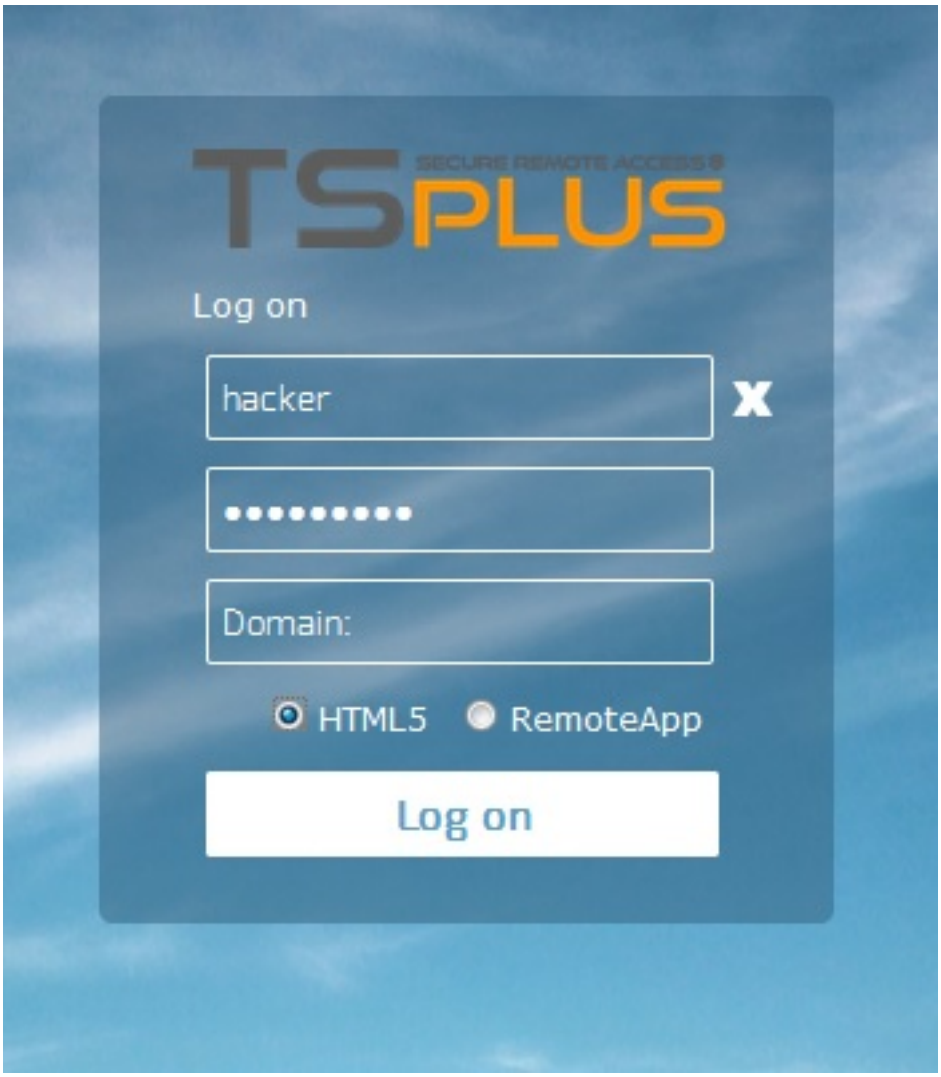
Si escribe una contraseña incorrecta, John tendrá que volver a escribir su contraseña:



Julia tiene una lista diferente de servidores posibles:



Alguien intenta hackear el Gateway. No ve ningún servidor y el Gateway bloquea su acceso web.

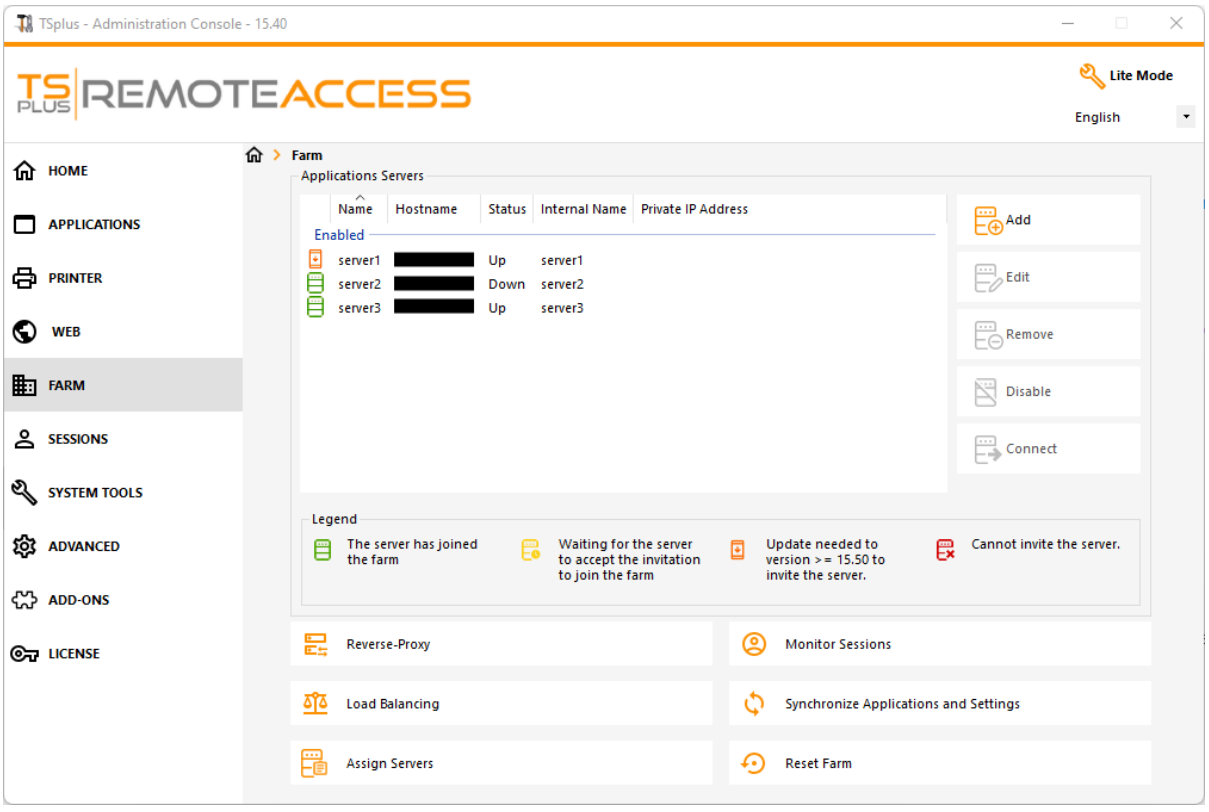

TSPLUS
SECURE REMOTE ACCESS
Log on
hacker
Domain:
HTML5
RemoteApp
Log on

Configuración de granja

Resumen

Para crear una granja, simplemente necesita agregar servidores de aplicaciones desde el TSplus AdminTool.

Podrás gestionar servidores de aplicaciones en la sección "Granja" del AdminTool.



Desde esta ventana, podrá realizar varias acciones:

- “ Agregar : agregar un nuevo servidor de aplicaciones
- “ Editar ”: editar el servidor seleccionado.
- “ Eliminar : eliminar permanentemente el servidor seleccionado de la granja (puedes volver a agregarlo más tarde con el botón "Agregar").
- “ Desactivar/Activar : deshabilitar o habilitar temporalmente el servidor seleccionado (los

usuarios no podrán conectarse a este servidor).
- “ Conectar ”: abra el cliente RDP predeterminado y conéctese automáticamente al servidor seleccionado. Si sus credenciales están guardadas en MSTSC, se utilizarán; de lo contrario, tendrá que ingresar sus credenciales.

También puedes acceder a estas acciones desde el menú contextual que se muestra con un clic derecho en un servidor.

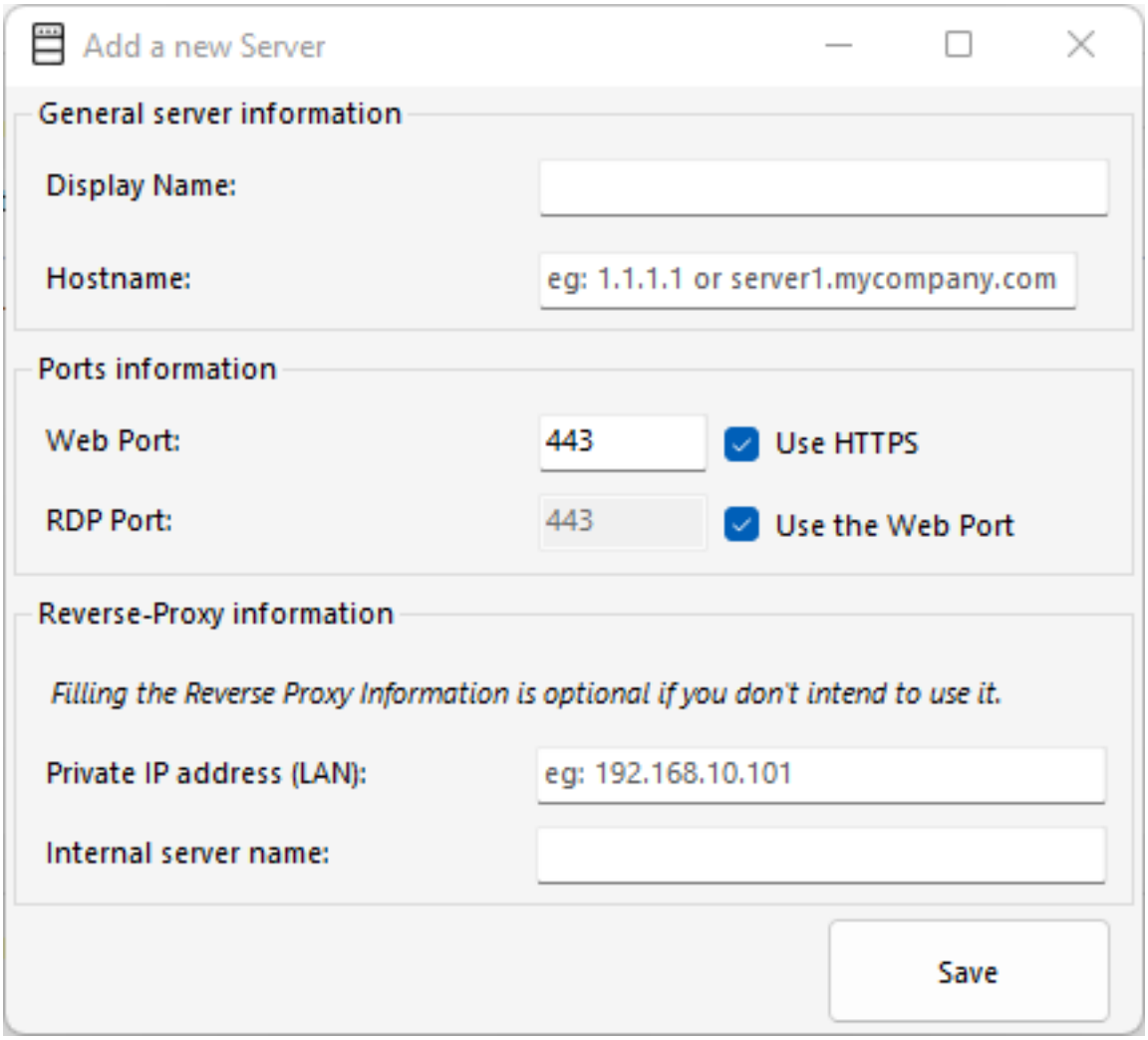
En el panel inferior encontrará un acceso rápido a las principales características de la granja disponibles una vez que se hayan agregado los servidores de aplicaciones:

- “Balanceo de Carga”: permite redirigir a los usuarios que se conectan desde el servidor de puerta de enlace al servidor menos cargado de la granja
- “Proxy inverso”: permite exponer solo el servidor de gateway y hace que los servidores de aplicaciones sean accesibles utilizando URL como https://gateway-server-domain-or-ip-address/~~nombre-del-servidor-de-aplicaciones-interno
- “Asignar Servidores”: permite restringir los servidores de aplicaciones disponibles para usuarios y grupos al conectarse desde el servidor de puerta de enlace, permitiéndoles elegir el servidor al que desean conectarse si se asignan múltiples servidores.
- “Monitorear Sesiones” * permite monitorear la sesión actual y realizar rápidamente acciones como desconectar, cerrar sesión, enviar un mensaje, ver la sesión o controlar la sesión.
- Sincronizar aplicaciones y configuraciones * permite enviar todas las configuraciones avanzadas y las aplicaciones publicadas a los servidores de aplicaciones seleccionados
- “Restablecer Granja”: te permite restablecer la granja, lo que eliminará todos los servidores y restablecerá todas las configuraciones de características de la granja, por ejemplo, las configuraciones de “Proxy Inverso”, “Balanceo de Carga” y “Asignar Servidores”.

* Estas características son accesibles solo para servidores de aplicaciones que se unieron completamente a la granja por razones de seguridad, lo que significa que primero deberá aceptar la invitación enviada por su Controlador de granja, en el lado del servidor de aplicaciones.

Agregar un servidor de aplicaciones a la granja

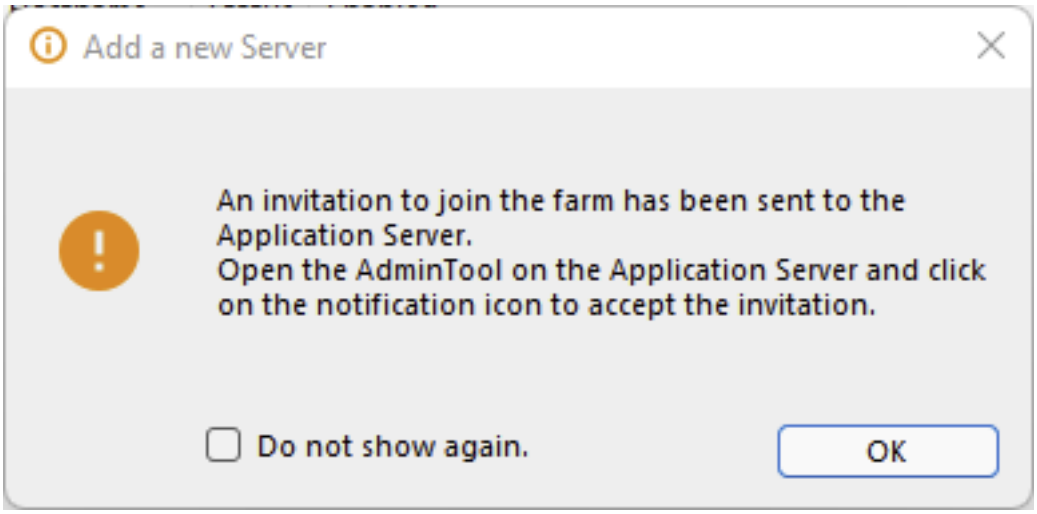
Para agregar un servidor de aplicaciones, haga clic en el botón "Agregar". Se mostrará la siguiente ventana:



Deberá especificar su Nombre de Visualización y Nombre de Host (puede escribir una IP o un nombre de dominio, sin un número de puerto).
Llenar los campos de información del Proxy Inverso es opcional solo si no está utilizando actualmente la función de Proxy Inverso.
El nombre interno se completará automáticamente con un nombre de visualización disponible si está vacío para facilitar la configuración general del servidor.

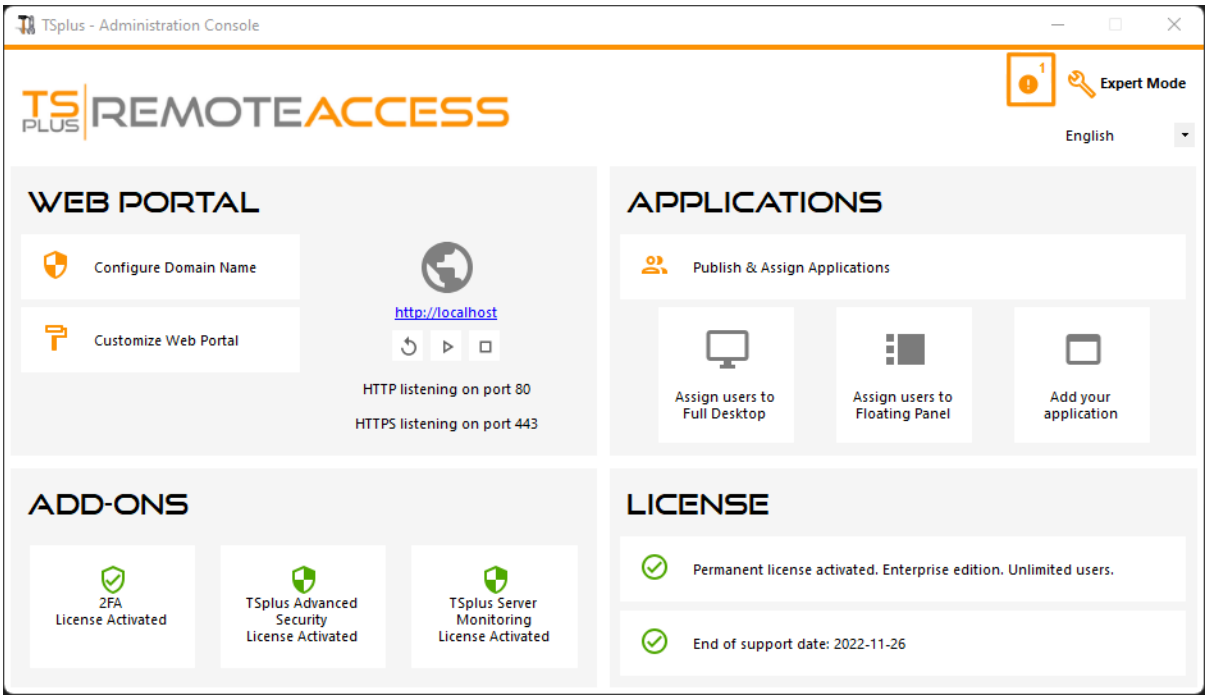
IMPORTANTE: la opción de puerto RDP “Usar el puerto web” especifica que desea aprovechar la función de reenvío de puerto RDP (habilitada por defecto) ofrecida por el servidor web de la aplicación.
Como resultado, si desea utilizar la opción “Usar el puerto web”, asegúrese de que en el servidor de aplicaciones agregado, la opción “Deshabilitar el reenvío de RDP” en AdminTool > Avanzado > Seguridad esté configurada en “No”.

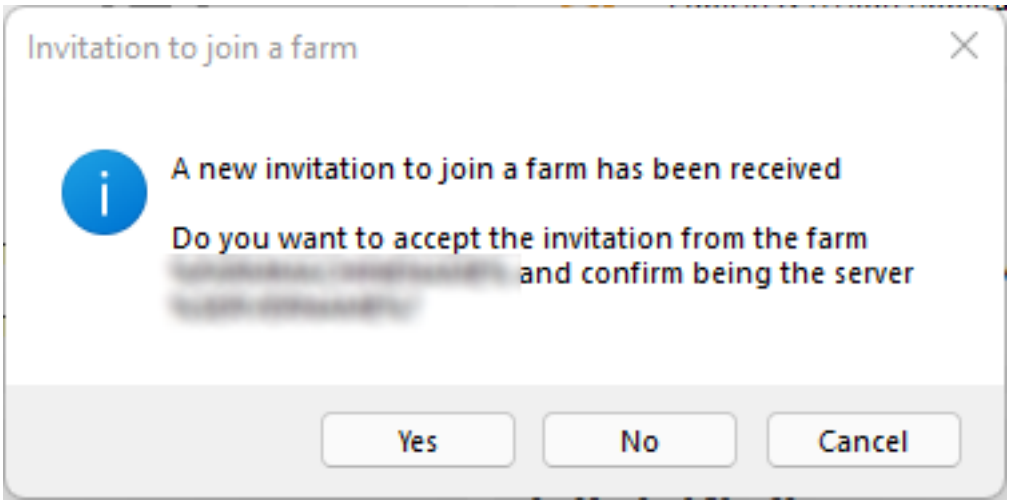
Ingrese los detalles del Servidor de Aplicaciones, luego haga clic en el botón "Guardar". Se enviará una invitación para unirse a la Granja al Servidor de Aplicaciones agregado.



Aceptar esta invitación en el lado del servidor de la aplicación es necesario si desea poder utilizar el “Monitorear Sesiones” y “Sincronizar Aplicaciones y Configuraciones” por razones de seguridad.
No se requiere si solo necesita utilizar las funciones de “Proxy Inverso”, “Balanceo de Carga” y “Asignar Servidores”.

Para aceptar la invitación, abre una sesión de Administrador. **en el Servidor de Aplicaciones** agregaste a la Granja. Haz clic en el botón de alerta en la esquina superior derecha de la TSplus AdminTool, luego haz clic en "Sí":





En el lado del Controlador de la Granja, puedes ver la lista de Servidores de Aplicaciones en la Granja. Pueden tener tres estados representados por íconos de colores:

- 

  Unido El servidor de aplicaciones se ha unido completamente a la granja al aceptar la invitación.

-

  Pendiente El servidor de aplicaciones se ha unido parcialmente a la granja, esperando a que el servidor de aplicaciones acepte la invitación.

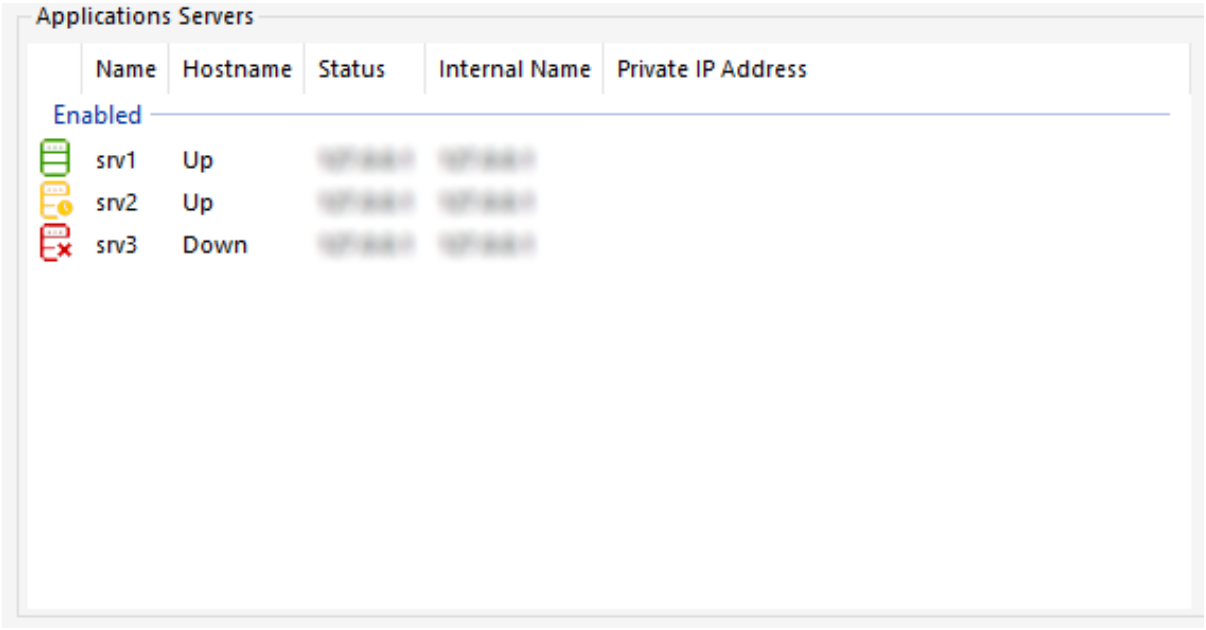
- 

  Actualización necesaria El servidor de aplicaciones se ha unido parcialmente a la granja, pero la invitación no se puede enviar porque el servidor está utilizando una versión de TSplus Remote Access < 15.50.

- 

  Inalcanzable El servidor de aplicaciones se ha unido parcialmente a la granja, pero la

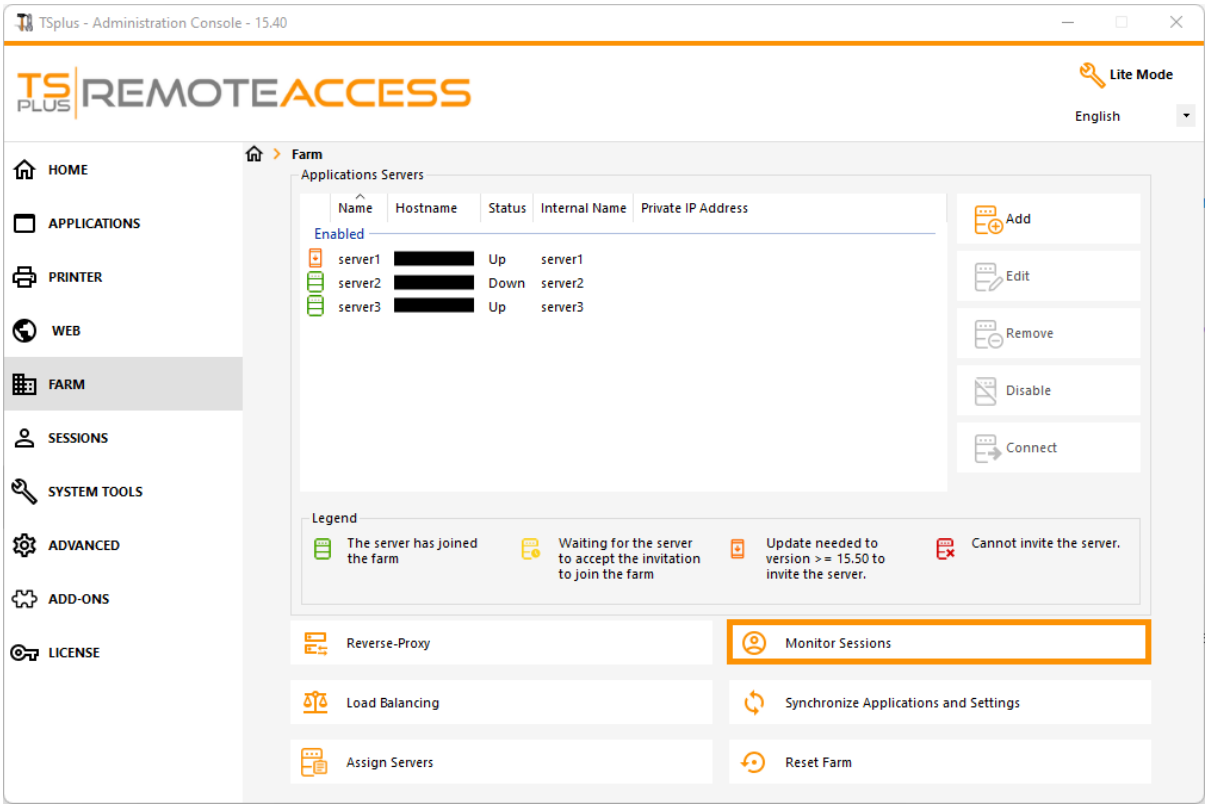
invitación no se puede enviar porque el servidor es inalcanzable.



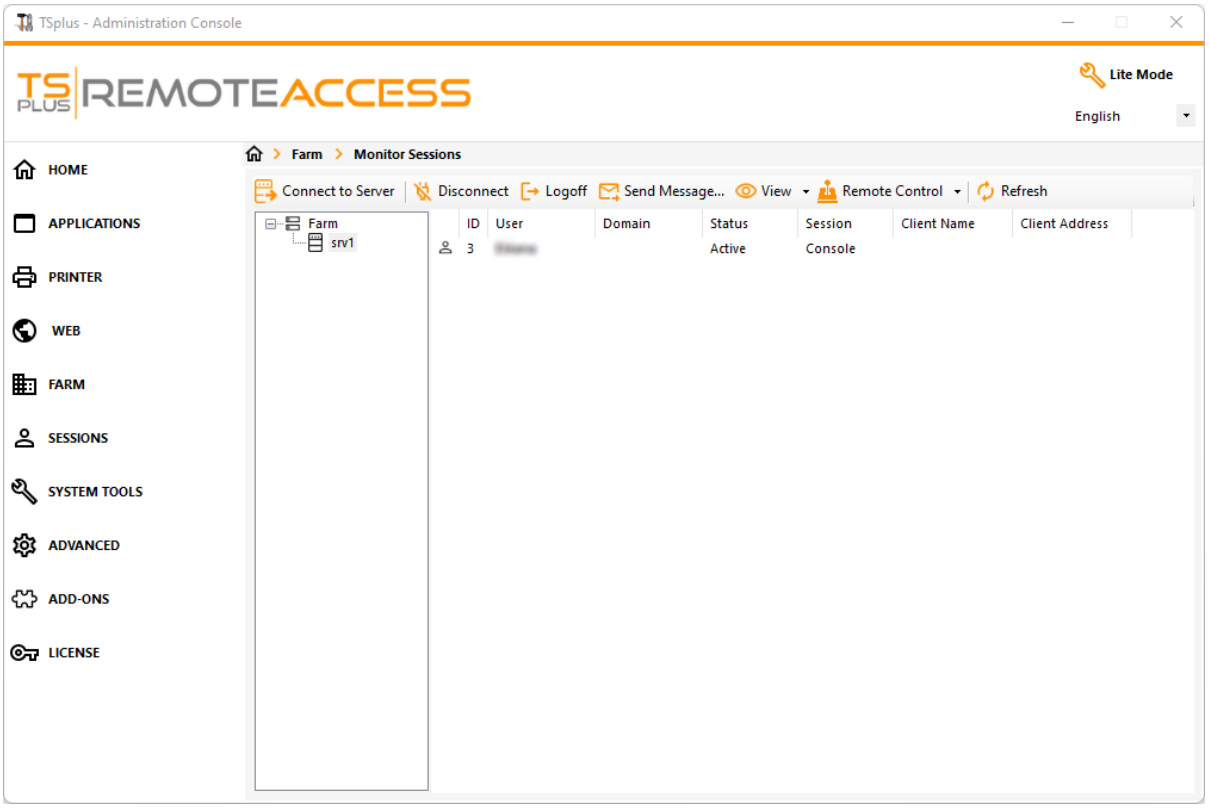
Monitorear sesiones

Resumen

Puedes acceder a la interfaz de sesión de monitoreo a través de la pestaña FARM:



Haga clic en el botón "Monitorear Sesiones" para mostrar la siguiente pestaña:



En esta pestaña, puedes ver la lista de Sesiones de Usuario en cualquier Servidor de Aplicaciones de la Granja.
Haga clic en un servidor de aplicaciones en el panel izquierdo para seleccionarlo y mostrar sus sesiones de usuario activas actuales. Una vez mostradas, puede seleccionar una o más sesiones y realizar varias acciones haciendo clic en uno de los siguientes botones:

- “Desconectar”: desconectar la(s) sesión(es) de usuario seleccionada(s) (el usuario aún podrá volver a conectarse a su sesión).
- “Cerrar sesión”: cerrar la(s) sesión(es) de usuario seleccionada(s) (todas las modificaciones no guardadas se perderán, las aplicaciones se cerrarán abruptamente).
- Enviar mensaje: mostrar una ventana para ingresar un título y un texto, luego enviar este mensaje a la(s) sesión(es) de usuario seleccionada(s).
- Ver: Ver una sesión de usuario seleccionada con/sin***** permisos.
- “Control Remoto”: Controle remotamente uma sessão de usuário selecionada com/sem***** permissões.
- “Actualizar”: realizar una actualización completa de la lista de sesiones de usuario para el(los) servidor(es) seleccionado(s).

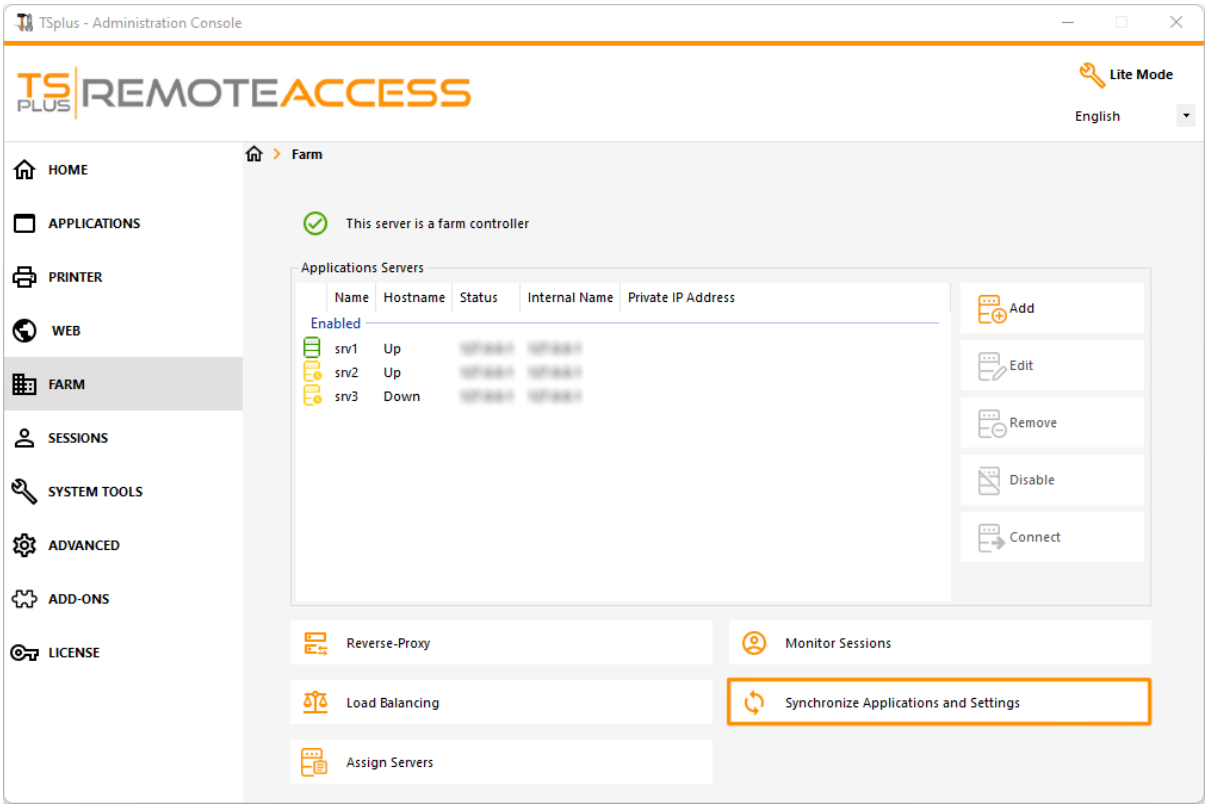
* Para ver o controlar una sesión **sin permisos** , necesitarás **cambia la siguiente GPO en el servidor de aplicaciones que deseas ver y/o controlar las sesiones de** .
Ubicación de GPO: Configuración del equipo > Plantillas administrativas > Componentes de Windows > Servicios de escritorio remoto > Host de sesión de escritorio remoto > Conexiones .
Clave GPO: Establecer reglas para el control remoto de sesiones de usuario de Servicios de Escritorio Remoto

La lista de sesiones de usuario se actualiza automáticamente cada 5 segundos. Este refresco

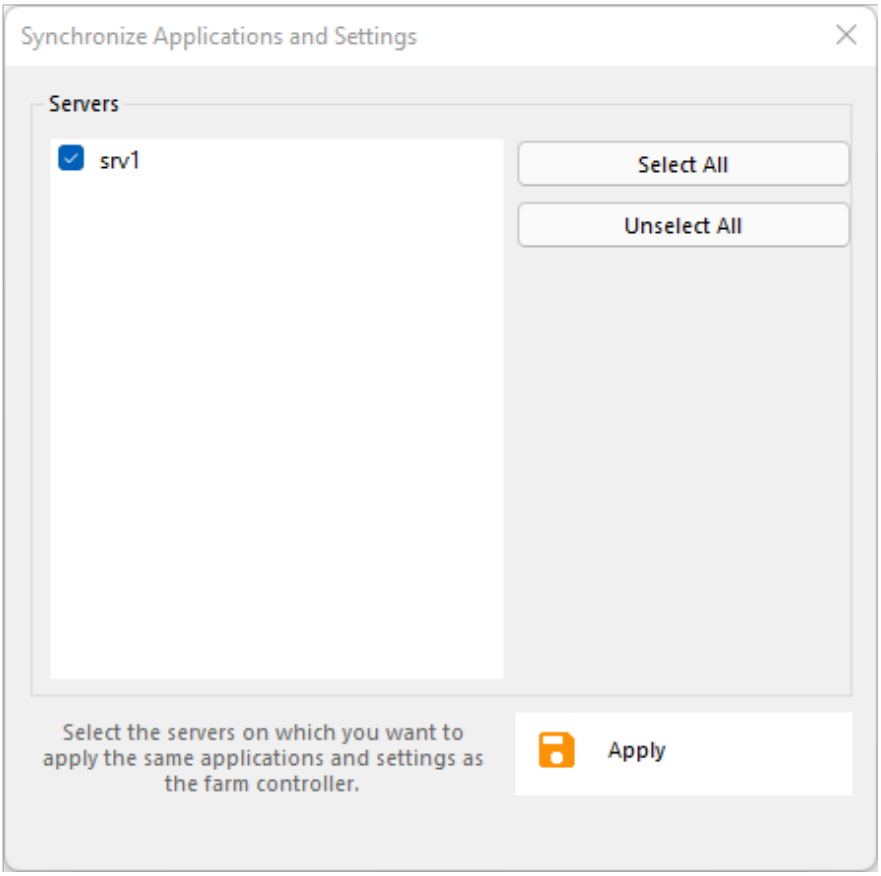
automático se detiene si el servidor seleccionado se vuelve no disponible. Un clic en el botón "Actualizar" reanudará el refresco automático.

Sincronización de Aplicaciones y Configuraciones

Resumen

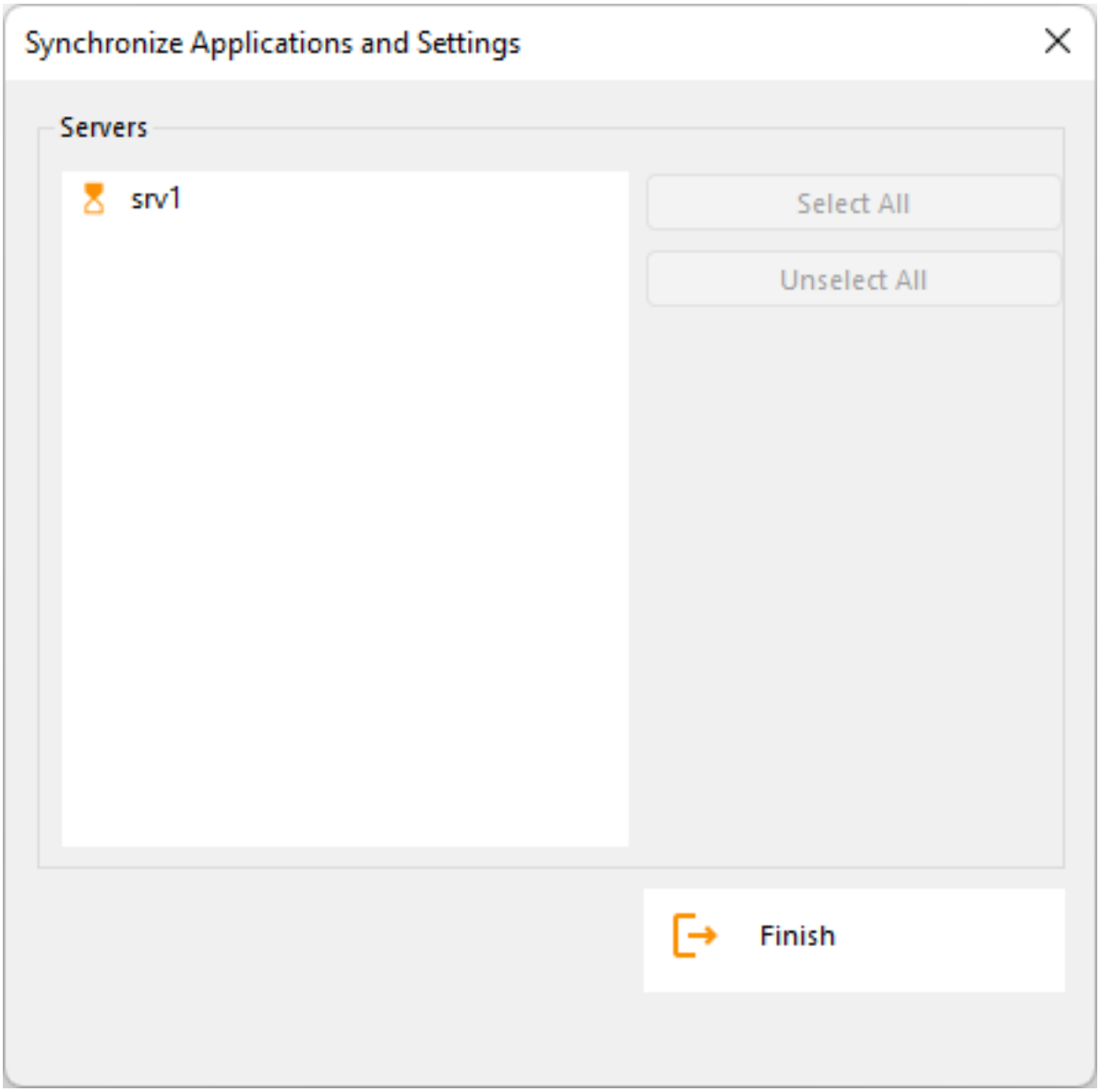


Haga clic en el botón "Sincronizar aplicaciones y configuraciones" para mostrar la siguiente ventana:



Verifique todos los servidores en los que desea aplicar la misma configuración y publicar las mismas aplicaciones que el Controlador de Granja, luego haga clic en "Aplicar".

La siguiente ventana se mostrará, permitiéndole monitorear el progreso de la tarea:


Synchronize Applications and Settings
Servers
srv1
Select All
Unselect All
Finish

Transferencia de archivos rápida y fácil entre el usuario y el servidor

Resumen

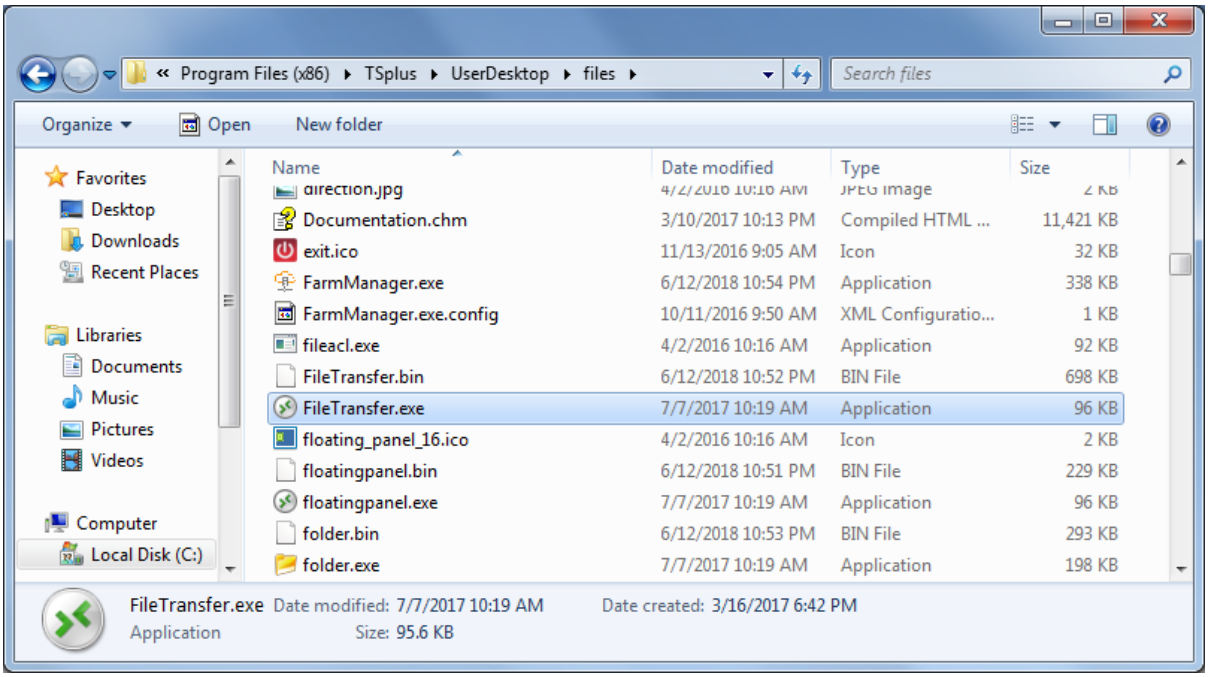
TSplus incluye un método único de transferencia de archivos:

- desde la estación de trabajo del usuario local => al Escritorio Remoto del usuario
- desde el servidor TSplus => al escritorio del usuario local

Porque las transferencias de archivos se basan en un Canal Virtual, es mucho más rápido que una copia de archivos, y se puede hacer. **incluso cuando las unidades de disco del usuario local no están mapeadas** .

Programa de transferencia de archivos y clientes generados

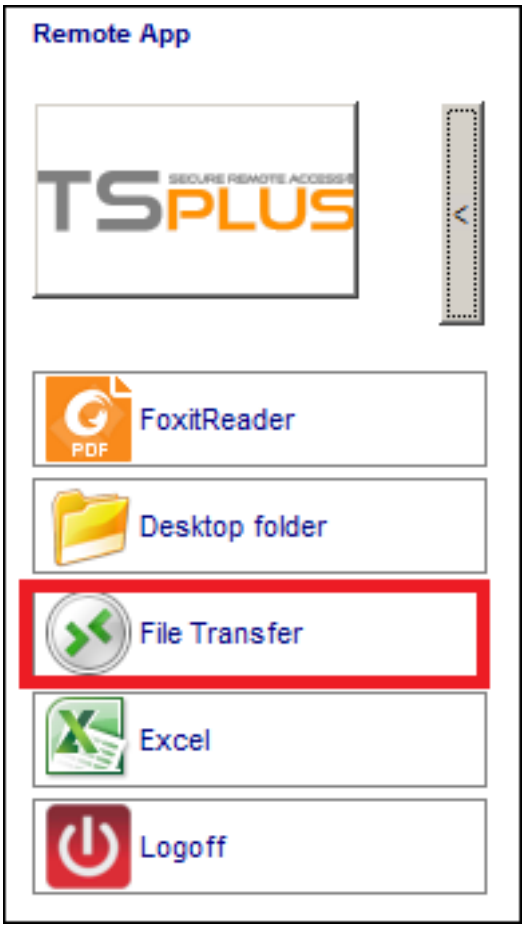
El programa de transferencia de archivos se encuentra en la carpeta de su programa TSplus, bajo el nombre "FileTransfer.exe" en la siguiente ruta: "UserDesktop\files"



Transferencia de archivos

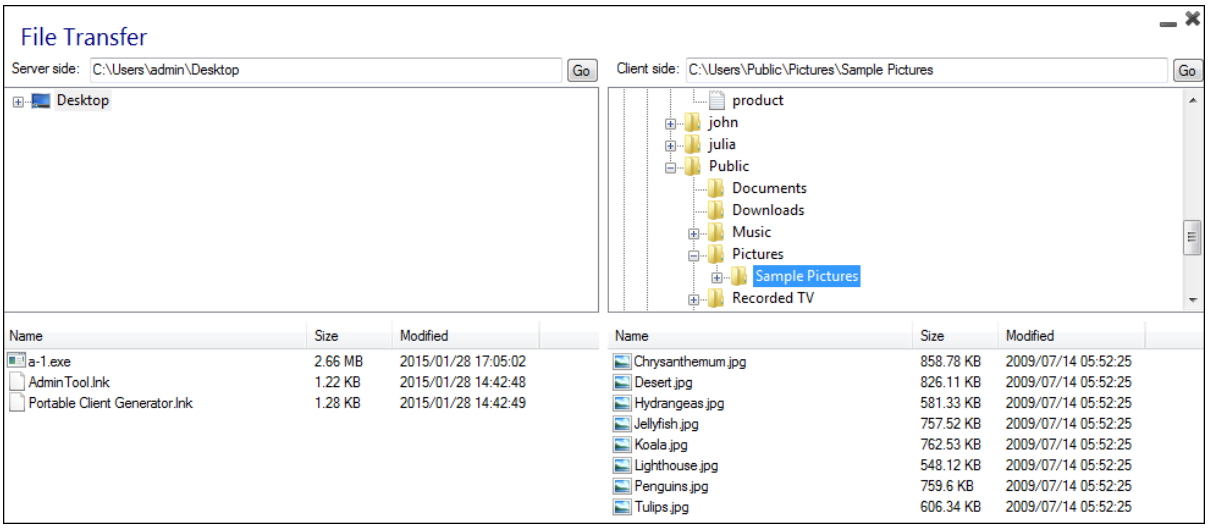
Transferir archivos es muy fácil.

Primero, lance la Transferencia de Archivos (por ejemplo, utilizando el Panel Flotante de TSplus):



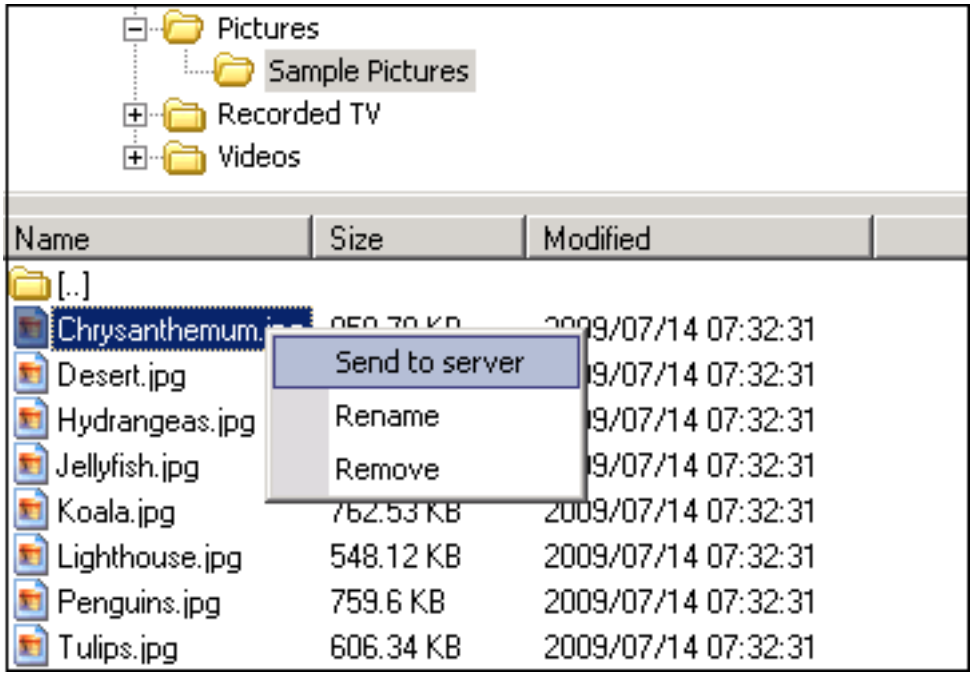
Luego navega a tu archivo utilizando el árbol de carpetas:

- las carpetas y archivos del servidor están en el **parte izquierda de la ventana (lado del servidor)**
- las carpetas y archivos de la estación de trabajo local están en el **parte derecha de la ventana (lado del cliente)**



Finalmente, haz clic derecho en el archivo que deseas transferir al otro lado y haz clic en "Enviar

al servidor" (o "Enviar al cliente"):



La transferencia de archivos funciona desde la estación de trabajo local al servidor, así como en la otra dirección (del servidor a la estación de trabajo local).

Nota Al utilizar la utilidad de transferencia de archivos desde una sesión HTML5, podrá transferir sus archivos del servidor al cliente únicamente. Por favor, prefiera el Método de menú superior HTML5 donde puedes subir archivos al servidor, descargar al cliente y gestionar tu lista de transferencias de archivos.

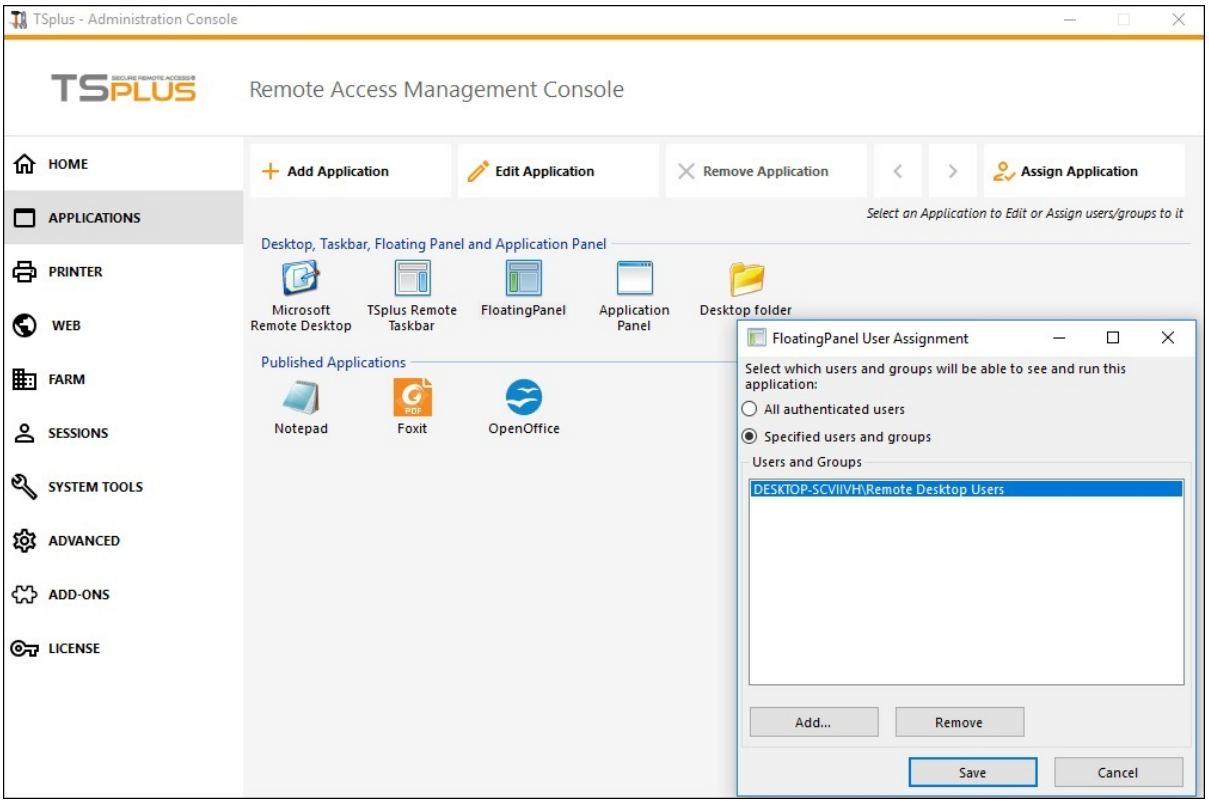
Panel flotante y panel de aplicaciones

Puedes elegir habilitar el Panel Flotante o el Panel de Aplicaciones para tus usuarios o grupos.

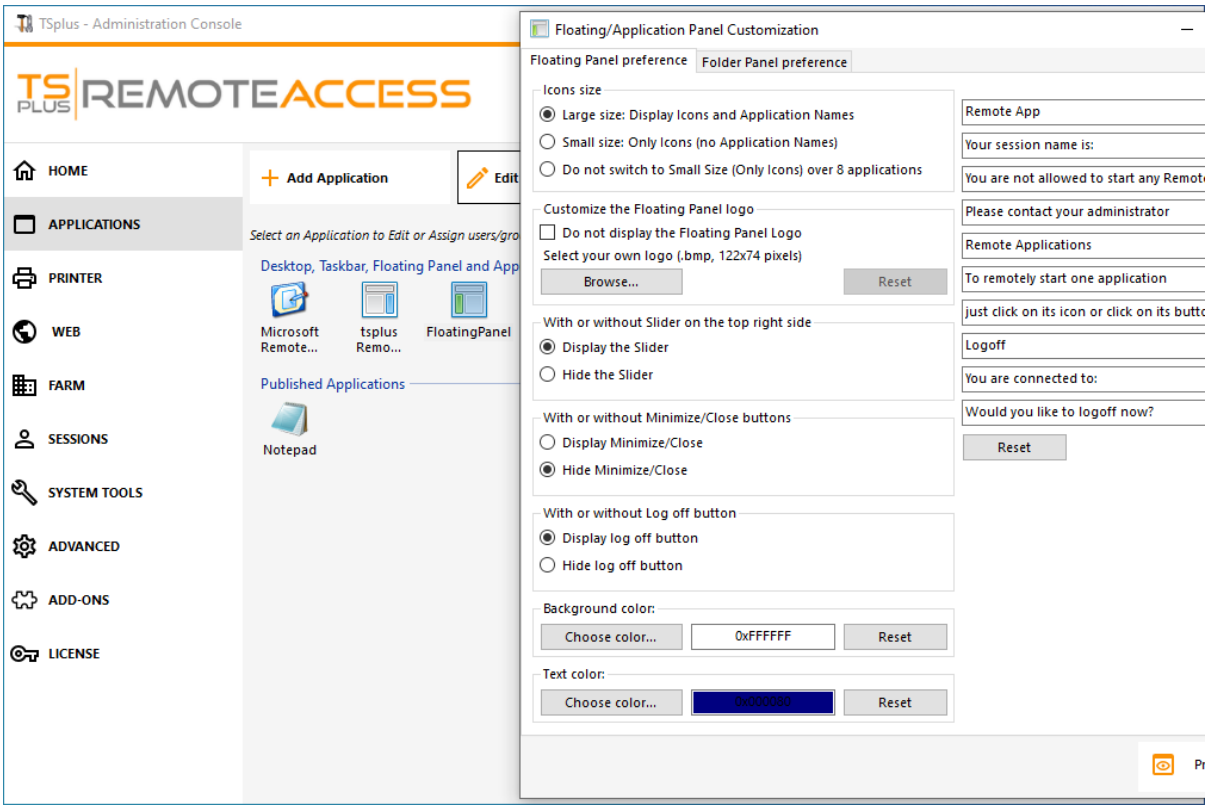
Estas dos formas de publicar aplicaciones están disponibles para cualquier método de conexión.

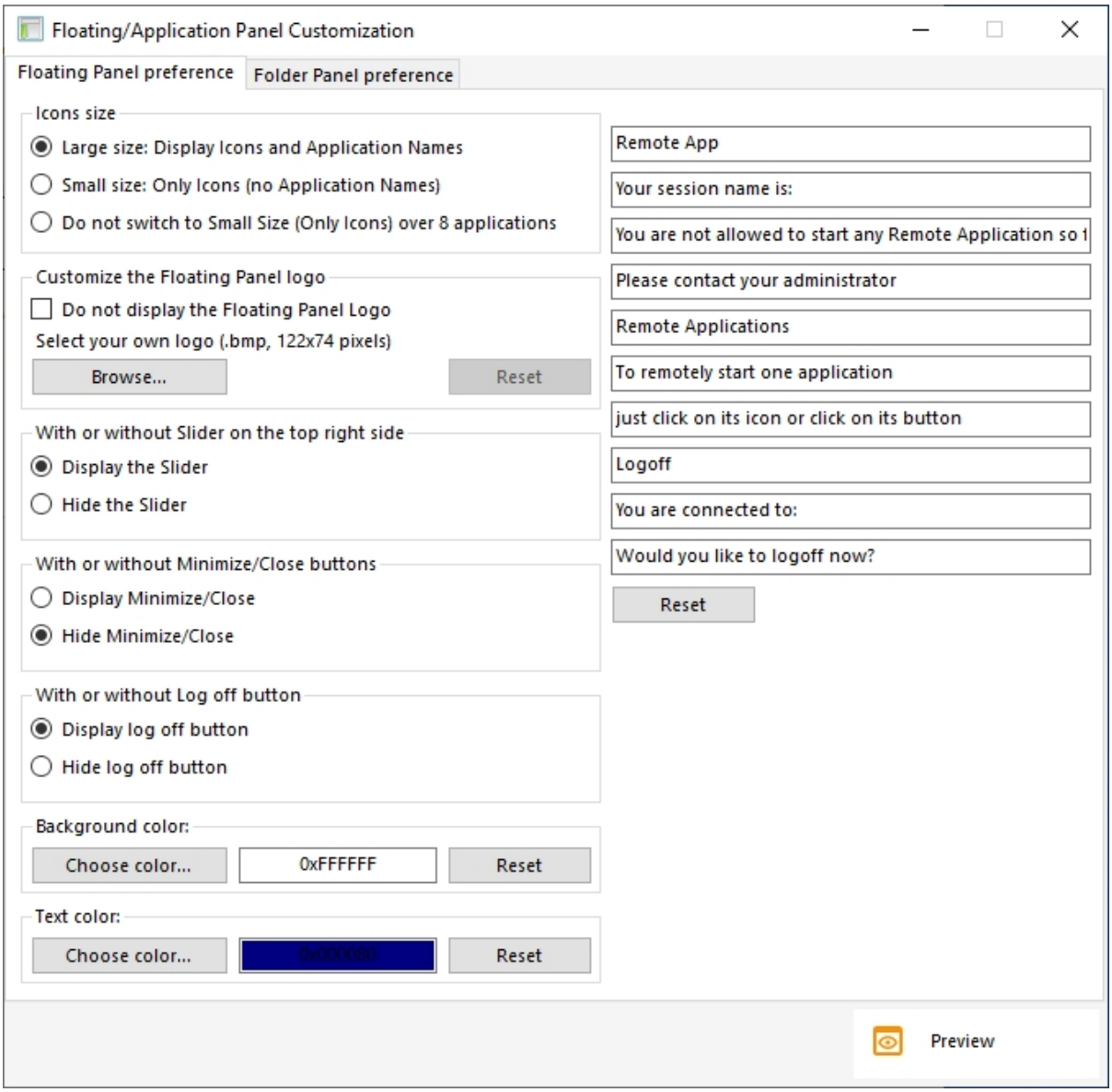
Si se activa con las aplicaciones asignadas, puede ver en la parte media-izquierda de la pantalla del usuario la mini lista desplegable de aplicaciones o panel flotante (muy apreciado por los usuarios de TSplus):

Asignarlo como una aplicación:



Seleccione el Panel Flotante, luego haga clic en el mosaico "Editar Aplicación" para personalizar el Panel Flotante a su conveniencia:


TSplus - Administration Console
TS PLUS REMOTEACCESS
HOME
APPLICATIONS
PRINTER
WEB
FARM
SESSIONS
SYSTEM TOOLS
ADVANCED
ADD-ONS
LICENSE
Add Application
Edit
Select an Application to Edit or Assign users/gro
Desktop, Taskbar, Floating Panel and App
Microsoft Remote...
tsplus Remo...
FloatingPanel
Published Applications
Notepad
Floating/Application Panel Customization
Floating Panel preference
Folder Panel preference
Icons size
Large size: Display Icons and Application Names
Small size: Only Icons (no Application Names)
Do not switch to Small Size (Only Icons) over 8 applications
Customize the Floating Panel logo
Do not display the Floating Panel Logo
Select your own logo (.bmp, 122x74 pixels)
Browse...
Reset
With or without Slider on the top right side
Display the Slider
Hide the Slider
With or without Minimize/Close buttons
Display Minimize/Close
Hide Minimize/Close
With or without Log off button
Display log off button
Hide log off button
Background color:
Choose color...
0xFFFFFF
Reset
Text color:
Choose color...
Reset
Remote App
Your session name is:
You are not allowed to start any Remot
Please contact your administrator
Remote Applications
To remotely start one application
just click on its icon or click on its butt
Logoff
You are connected to:
Would you like to logoff now?
Reset



Estas diversas opciones pueden permitirte personalizar la experiencia del usuario final.

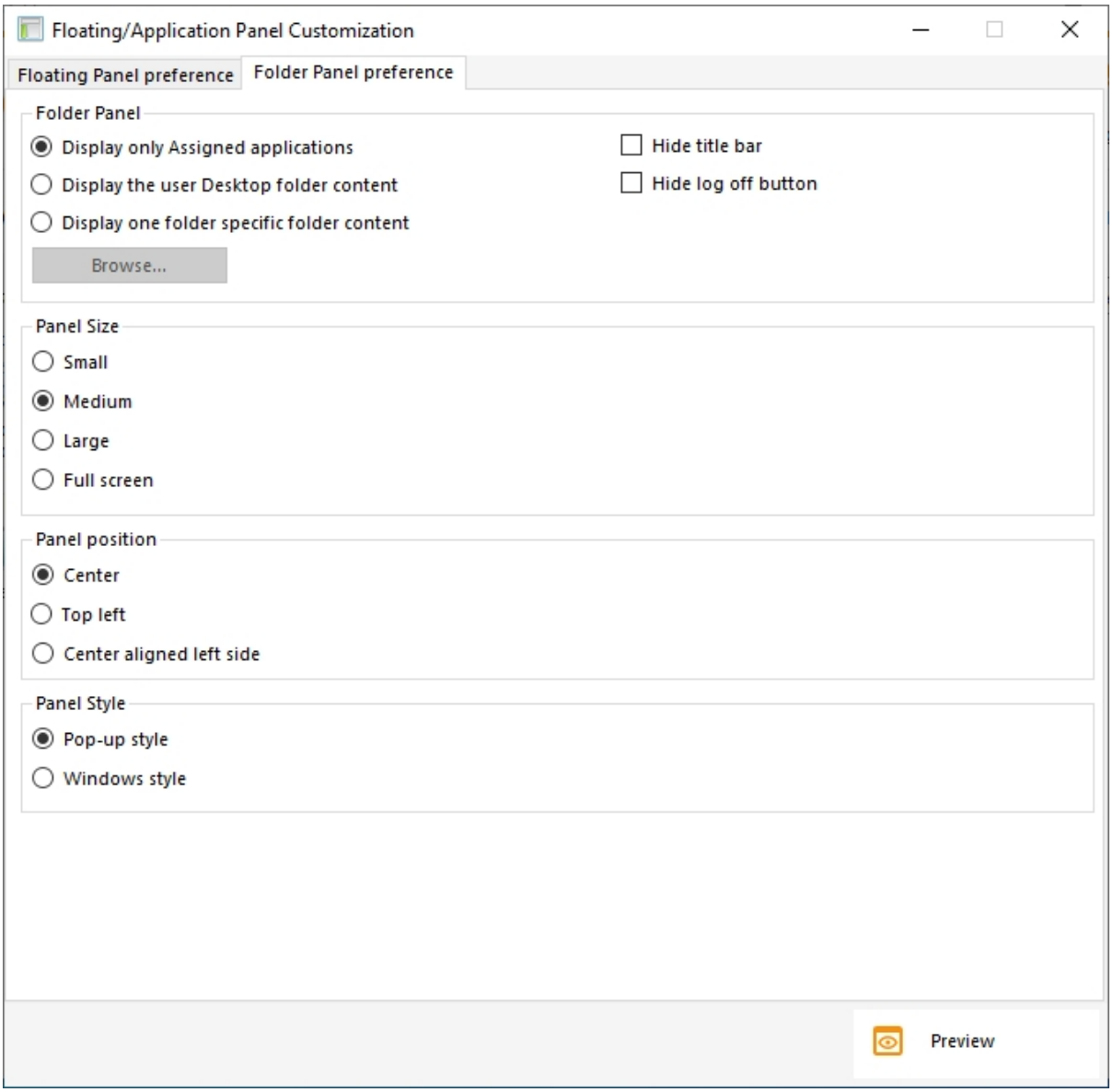
Aquí están las diferentes opciones de visualización del Panel Flotante, donde puedes configurar,

- Modificar el texto mostrado,
- Elige tu tamaño preferido, entre grande y pequeño, donde solo puedes mostrar íconos.
- Agrega tu propio logotipo,
- Personaliza el color del fondo y del texto,
- Mostrar el control deslizante o no,
- Mostrar los botones de Minimizar/Cerrar o no,
- Mostrar el ícono de cierre de sesión o no…

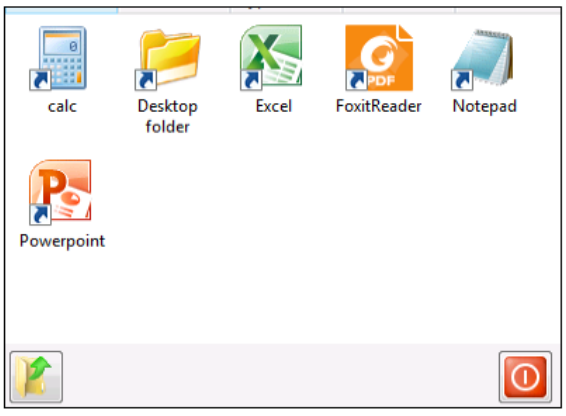


Por favor, tenga en cuenta que más de 8 aplicaciones, el Panel Flotante se cambia automáticamente a tamaño pequeño. Si aún desea que se muestren los nombres de las aplicaciones, seleccione “No cambiar a tamaño pequeño (solo íconos) con más de 8 aplicaciones.

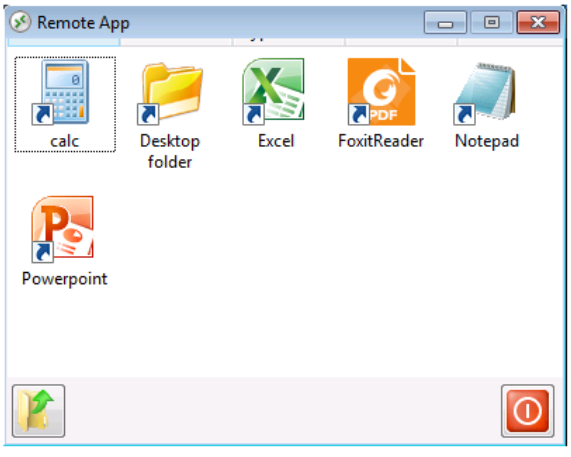
El **Panel de carpetas** es personalizable también y permite mostrar las aplicaciones asignadas, la carpeta de escritorio del usuario o el contenido de una carpeta específica en su sesión con muchas opciones de visualización:



Puedes cambiar el tamaño, la posición y el estilo del Panel de Carpetas (Emergente o Ventanas) a tu conveniencia:

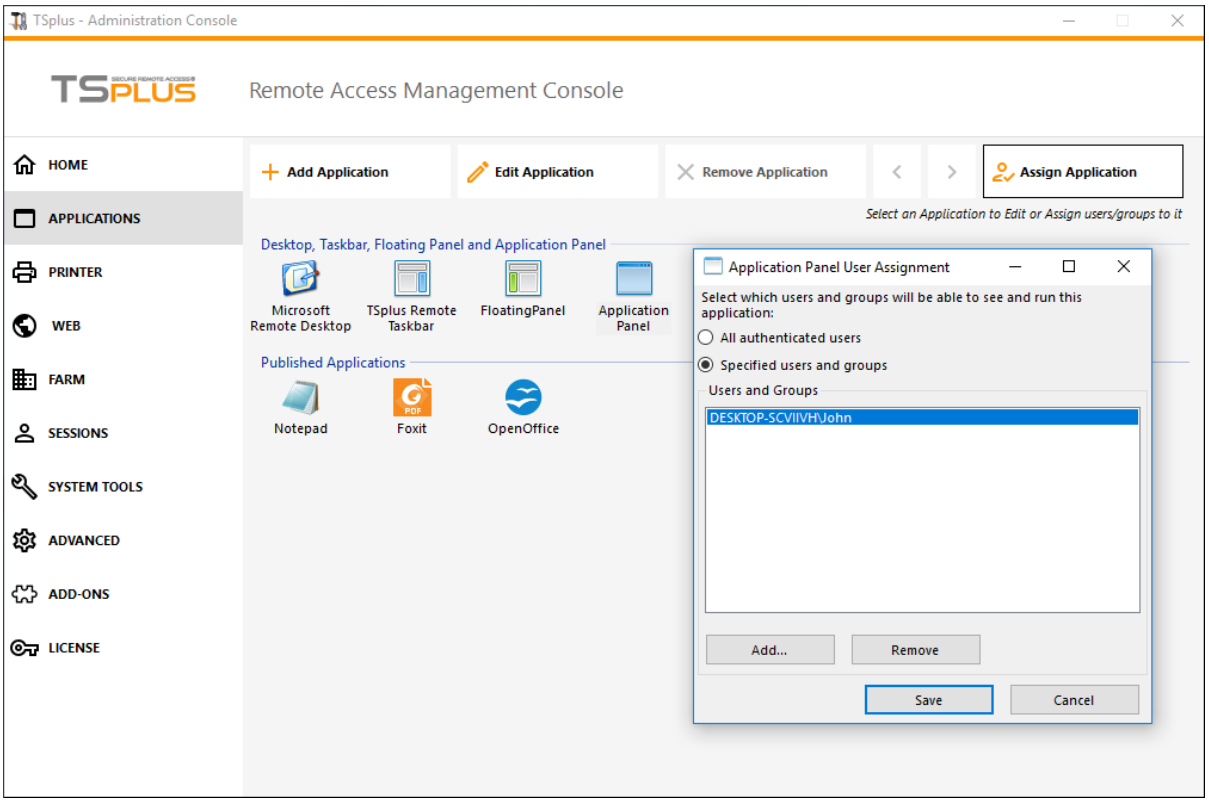


Pop-up style

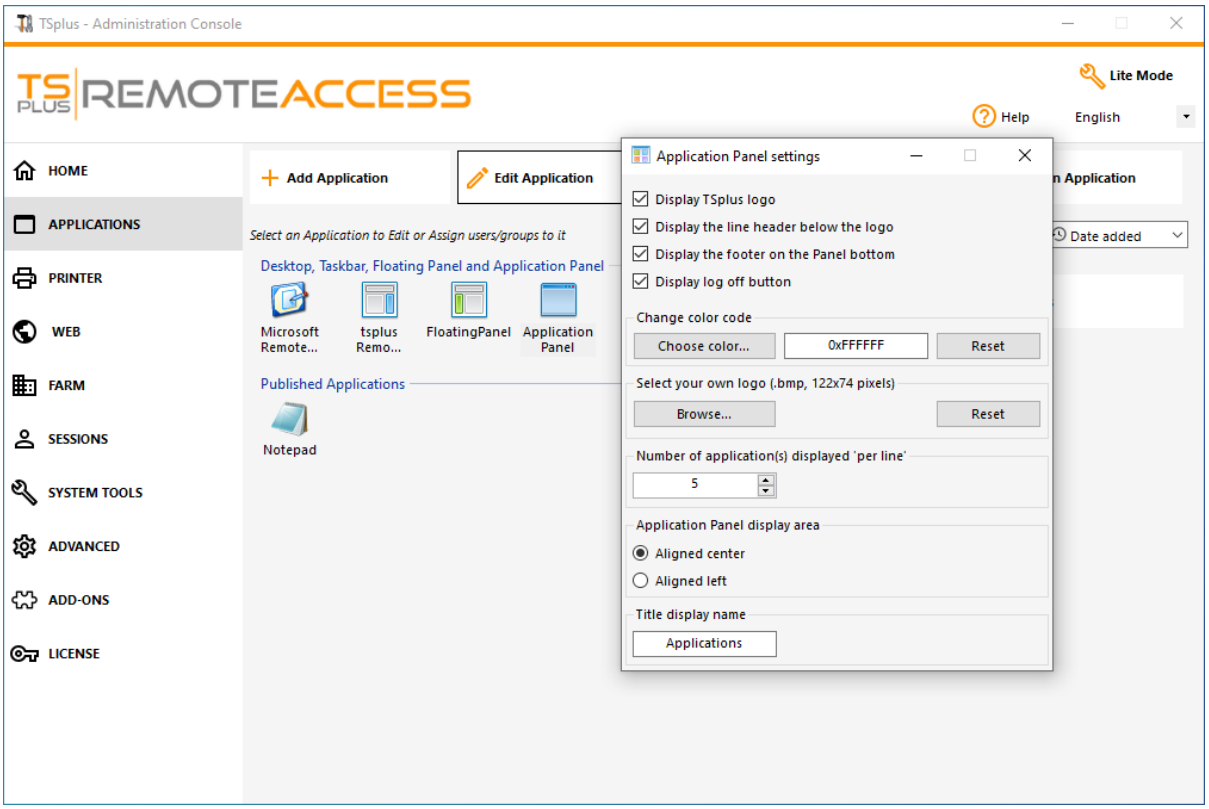


Windows style

El Panel de Aplicaciones te da la posibilidad de organizar las aplicaciones mostradas, exactamente como en el Portal de Aplicaciones Web, pero simplemente asignándolo a un usuario o grupo.



El Administrador puede personalizarlo eligiendo mostrar el logo de TSplus o su propio logo, mostrar la línea de encabezado debajo del logo y el pie de página, cambiar el color o elegir no mostrar nada de esto desmarcando las casillas correspondientes. También puede ajustar el número de aplicaciones mostradas por líneas y columnas ingresando el número de aplicaciones mostradas por línea, así como la alineación y el nombre del panel de Aplicaciones.



Por ejemplo, mostrar seis aplicaciones en una columna, sin logo; o mostradas en 2 columnas y 3 filas, con el logo de TSplus:


Notepad
FoxitReader
Excel
Powerpoint
calc
Desktop folder

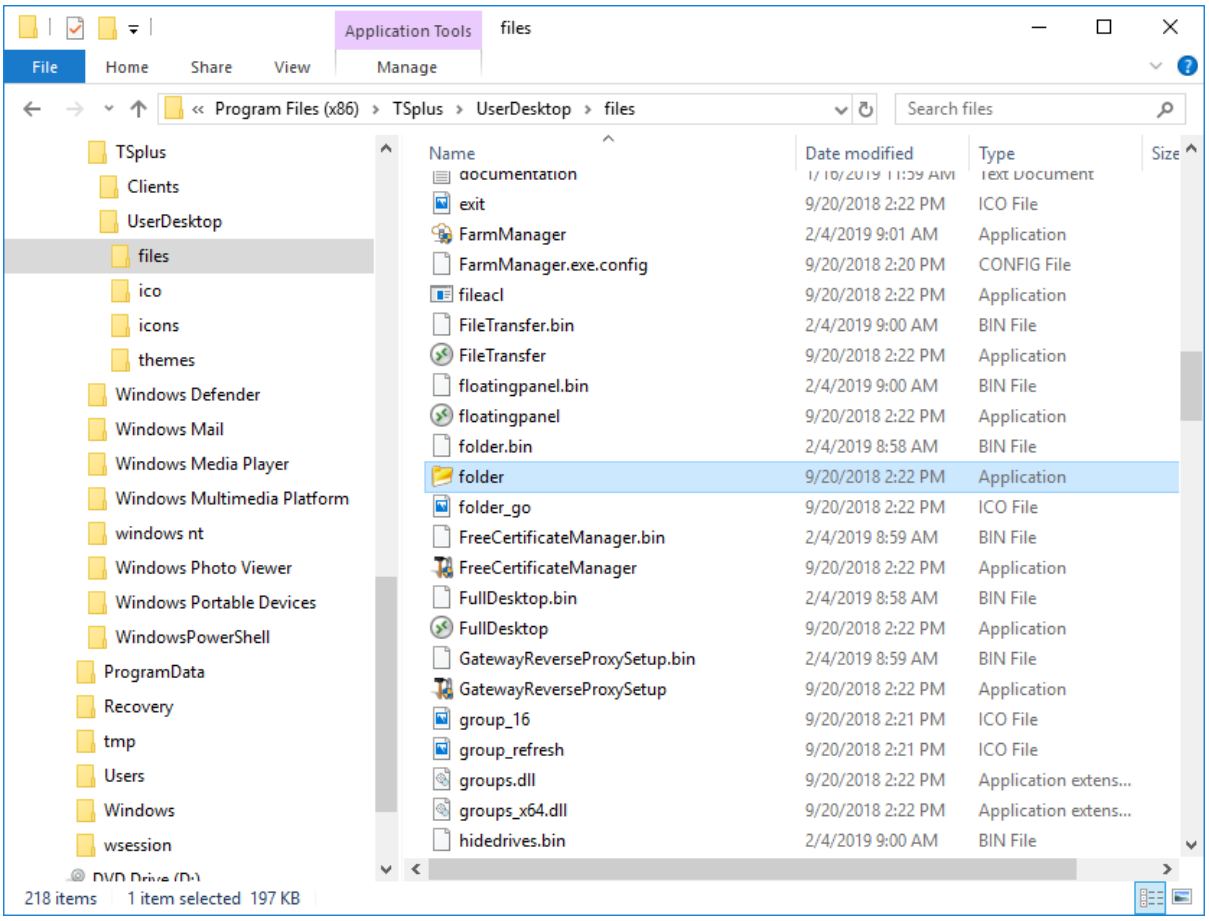

TSPLUS
Notepad
FoxitReader
Excel
Powerpoint
calc
Desktop folder

Compartición de carpetas asegurada - Folder.exe

La aplicación de carpeta mostrará de manera segura el contenido de una carpeta que pondrá a disposición de sus usuarios.

Primero, crea una carpeta en tu servidor con aplicaciones o documentos que deseas compartir.

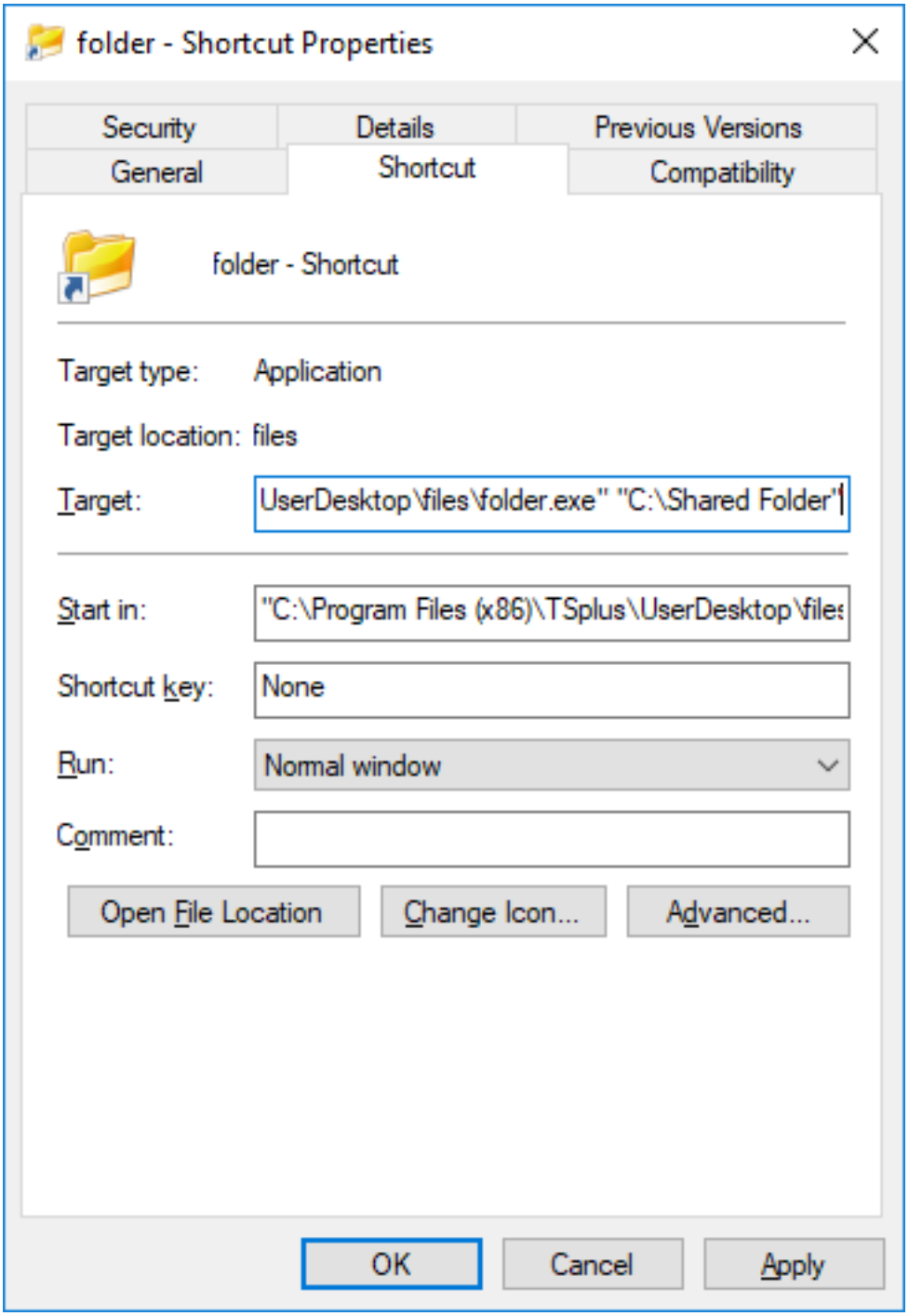
Abre un explorer.exe y localiza la aplicación folder.exe en C:\Program Files\tsplus\UserDesktop\files:



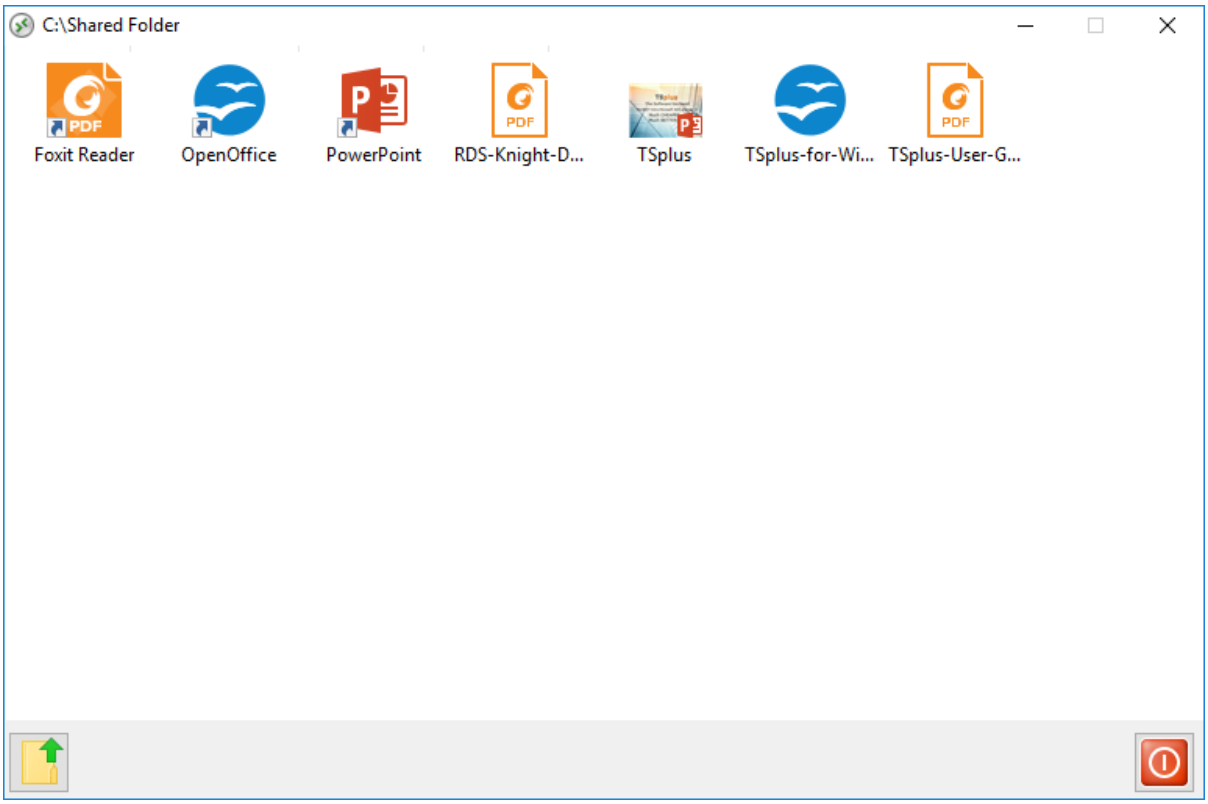
Crea un acceso directo de este archivo. Edita las propiedades de este acceso directo haciendo clic derecho sobre él.

Luego modifica la ruta de destino del acceso directo ingresando la ruta de tu carpeta de aplicaciones en la línea "Destino", después de la ruta de destino original, por ejemplo:

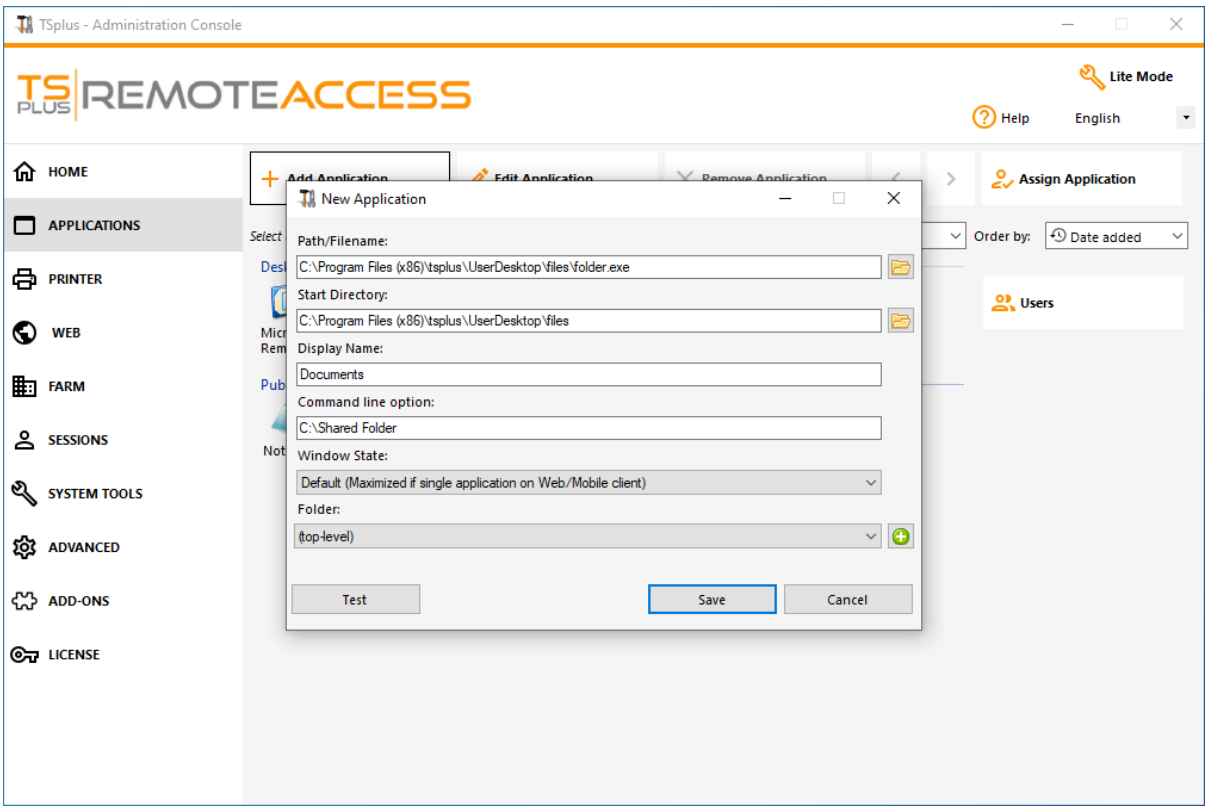
“C:\Program Files\tsplus\UserDesktop\files\folder.exe” “C:\Shared Folder”



Cuando abras el acceso directo de la carpeta.exe, debería verse así (con tus propios documentos y aplicaciones):



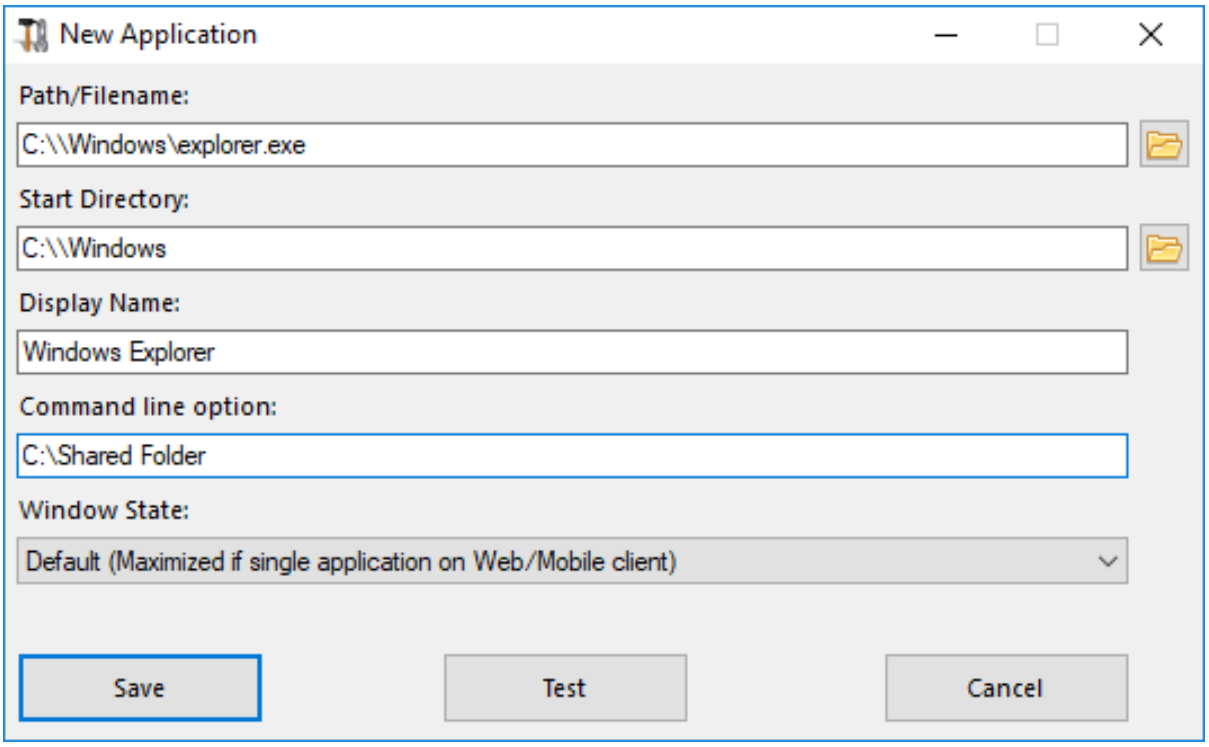
Este acceso directo se puede copiar a la carpeta de escritorio del perfil de un usuario o puedes publicar el folder.exe para un usuario como una aplicación. Si haces lo último, tendrás que indicar la ruta de tu carpeta en la sección de opciones de la línea de comandos.



Hay una forma alternativa de compartir una carpeta de documentos.

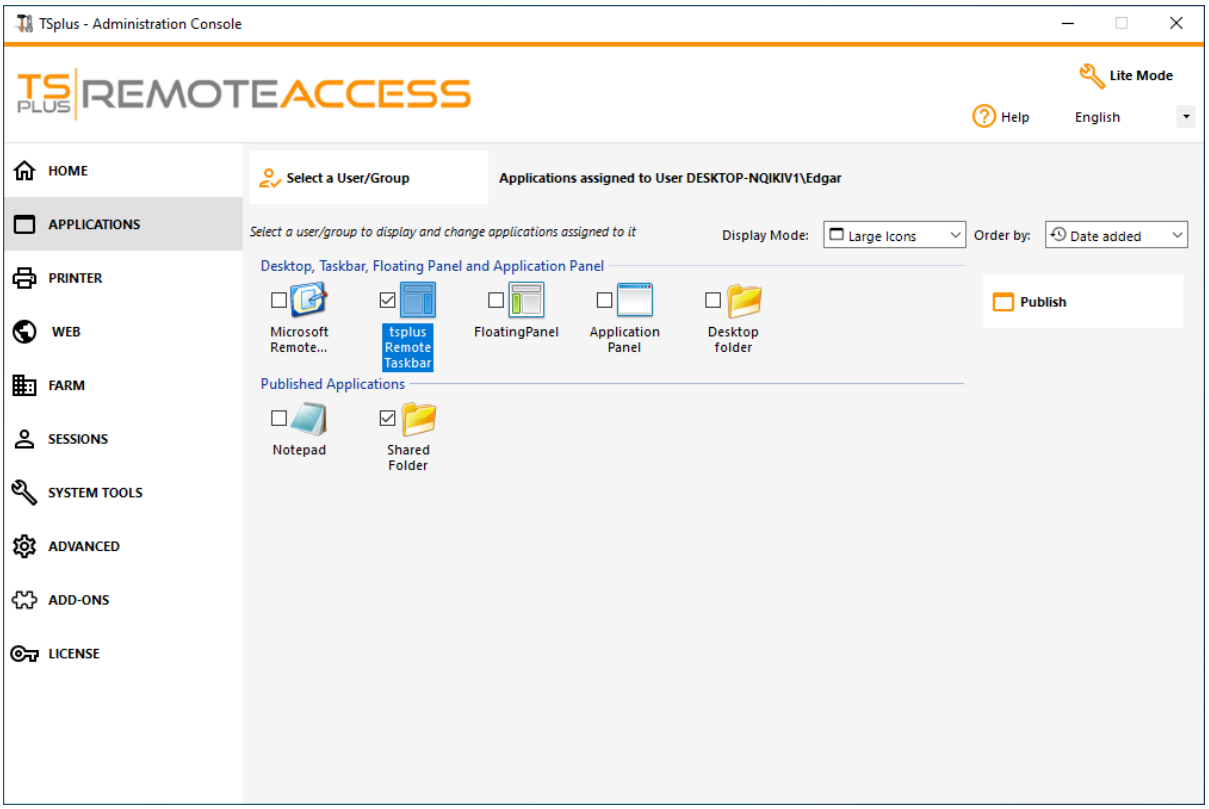
Publicando una carpeta compartida como una aplicación única :

Agregue una nueva aplicación. En el nombre para mostrar, escriba el nombre de la carpeta compartida o cualquier nombre que desee. Haga clic en el botón de explorar ubicado en el lado derecho del campo "Ruta/Nombre de archivo" y localice C:\Windows\explorer.exe. El directorio de inicio se completará automáticamente con la ruta de explorer.exe. En el campo de opción de línea de comando, escriba la ruta de la carpeta compartida, puede ser una carpeta local o una carpeta compartida en red utilizando una ruta UNC (ejemplo: \data\carpeta compartida). Complete el campo a continuación con la información de su carpeta compartida.

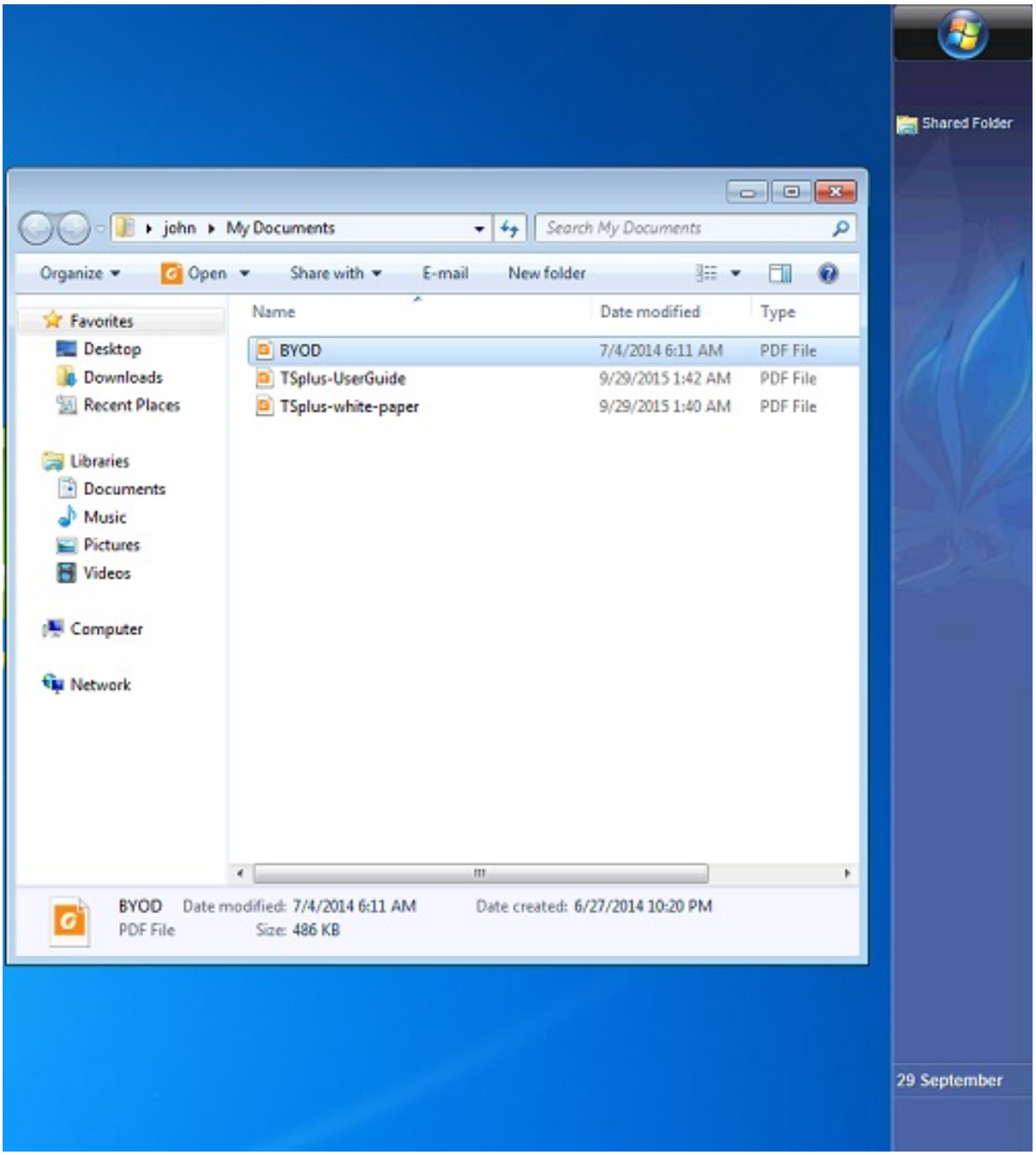


Luego haga clic en "Guardar".

Haga clic en la pestaña "Usuarios". Seleccione su usuario y marque las casillas de TSplus Remote Taskbar y Shared Folder.

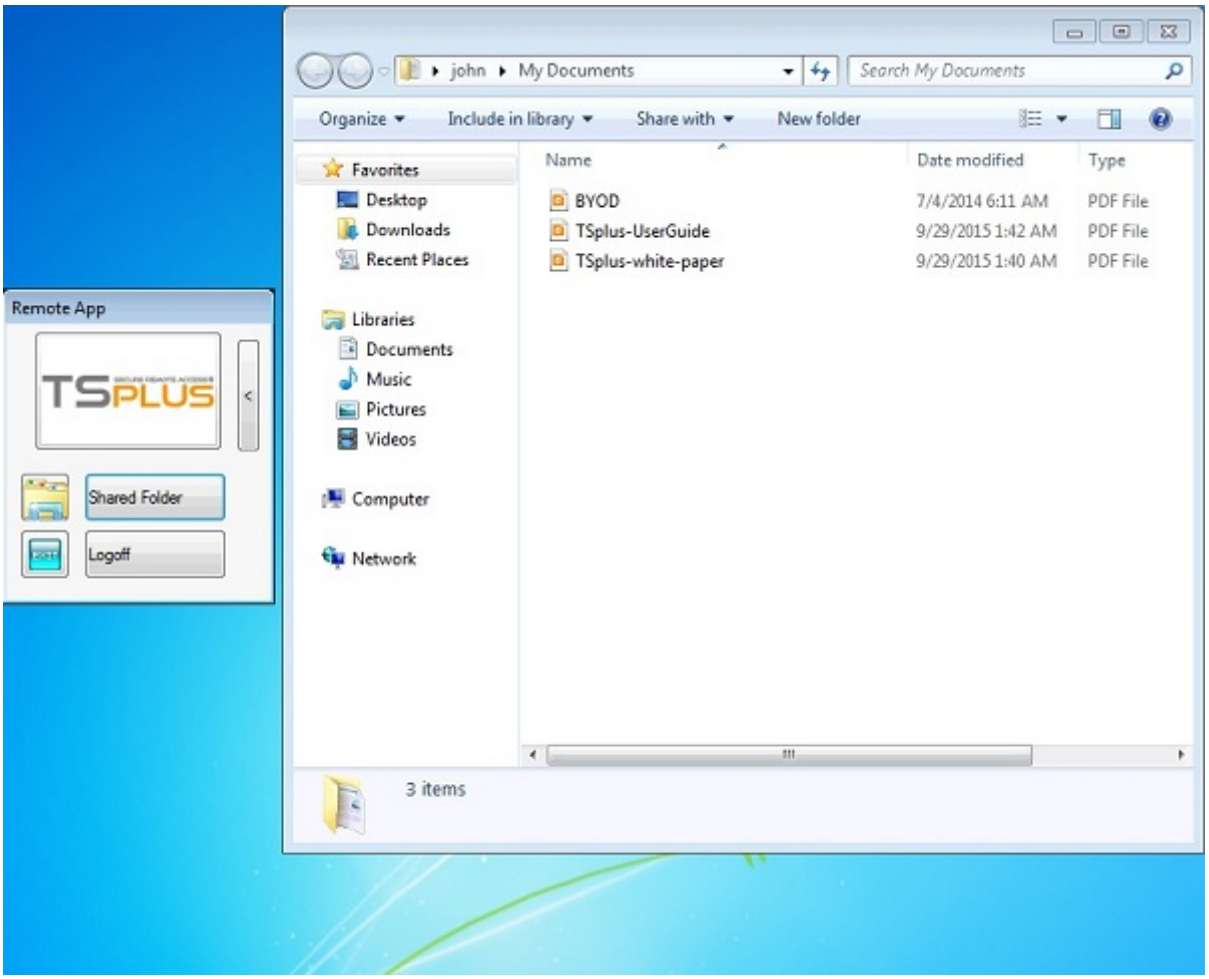


Aquí está el resultado, cuando abres una sesión con un cliente rdp, verás la barra de tareas de TSplus con la aplicación de carpeta compartida:



También puedes hacer esto con el panel flotante. Abre una herramienta de administración y haz clic en la pestaña "Asignar aplicación". Marca las casillas del Panel Flotante y la Carpeta Compartida.

Aquí está el resultado:


Remote App
TSPLUS
Shared Folder
Logoff
john ▸ My Documents
Search My Documents
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
BYOD
7/4/2014 6:11 AM
PDF File
TSplus-UserGuide
9/29/2015 1:42 AM
PDF File
TSplus-white-paper
9/29/2015 1:40 AM
PDF File
3 items

Certificado HTTPS gratuito y fácil de instalar

Resumen

A partir de la versión 9.20, TSplus ofrece una función fácil de usar para generar un certificado HTTPS gratuito y válido.

En 3 clics de ratón obtendrá un certificado válido y seguro, renovado automáticamente y configurado automáticamente en el servidor web integrado de TSplus.

Esta función utiliza Let's Encrypt proporcionar un certificado HTTPS gratuito y seguro para sus conexiones HTTPS.

Requisitos

Por favor, asegúrese de que su servidor TSplus cumpla con estos requisitos antes de usar el Administrador de Certificados Gratuito:

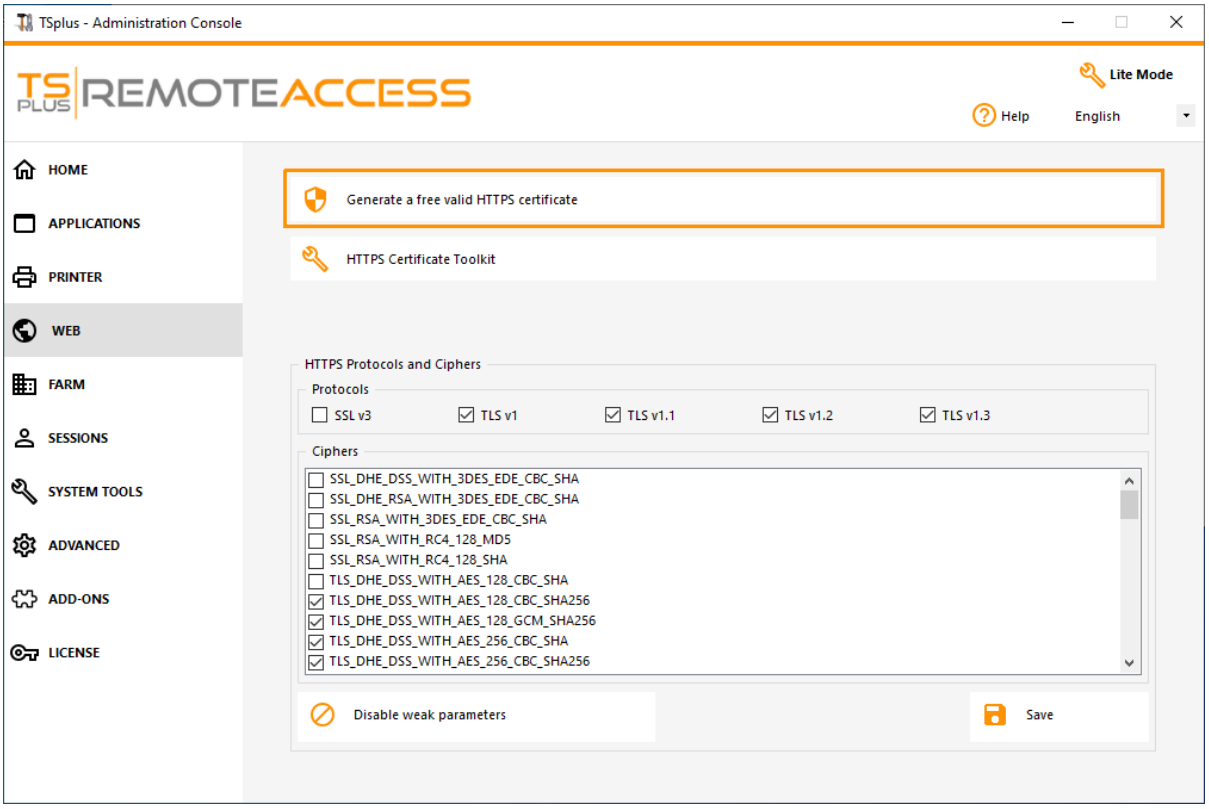
- Debes **utilice el servidor web integrado de TSplus escuchando en el puerto 80 para HTTP** Esto es requerido por el proceso de validación de propiedad de dominio de Let's Encrypt.
- Tu **el nombre de dominio del servidor debe ser accesible** desde Internet público. Esto también es necesario para validar que usted es el verdadero propietario del dominio.
- Debes **ejecute este programa en el servidor Gateway o en un servidor independiente, no en un servidor de aplicaciones** (excepto si su Servidor de Aplicaciones es accesible desde Internet público y tiene un nombre de dominio público).

No es posible obtener un certificado para una dirección IP, ya sea pública o privada.

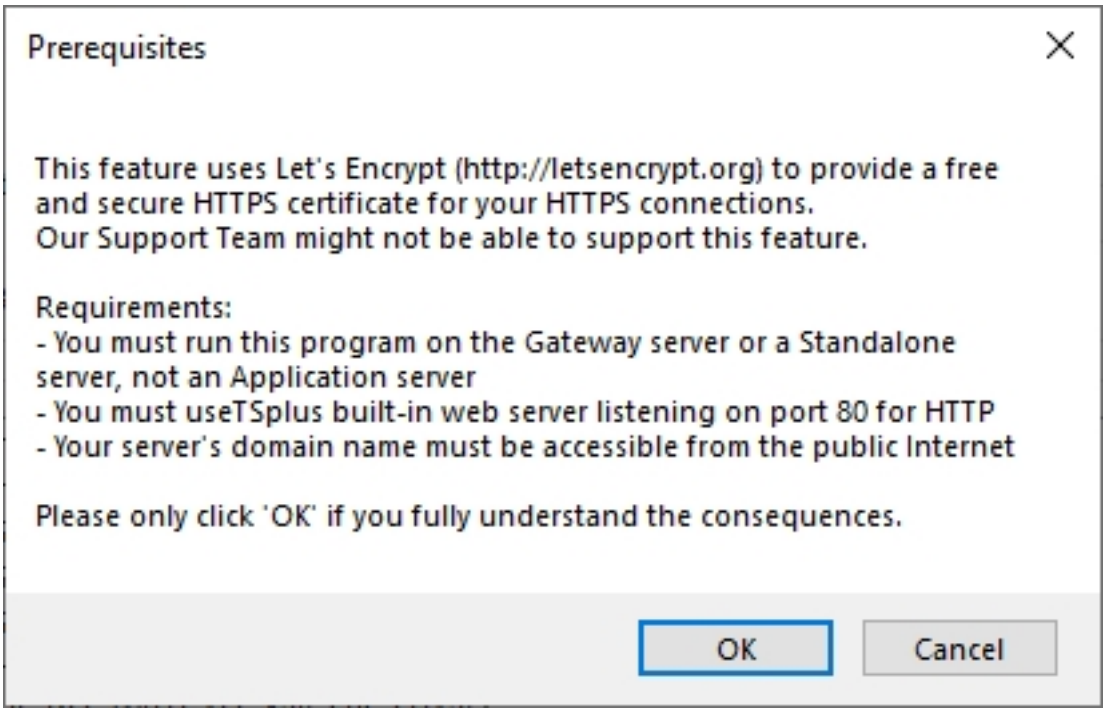
No es posible obtener un certificado para un nombre de dominio interno (es decir, un dominio que solo se resuelve dentro de su red privada).

Administrador de Certificados Gratuito GUI

Para abrir la interfaz gráfica del administrador de certificados gratuitos de TSplus, abra TSplus AdminTool, haga clic en la pestaña “Web - HTTPS” y luego haga clic en “Generar un certificado HTTPS válido gratuito” como se muestra en la captura de pantalla a continuación:



El Administrador de Certificados Gratuito GUI se abrirá y te recordará los requisitos previos, como se muestra en la captura de pantalla a continuación:



Por favor, lea atentamente y verifique que su servidor cumpla con todos los requisitos, luego haga clic en el botón "Ok".

Paso 1: Ingresa tu correo electrónico

Este correo electrónico no se utilizará para enviarte spam. De hecho, ni siquiera se enviará a TSplus ni a ningún tercero, excepto al emisor del certificado: Let’s Encrypt.

Solo se pondrán en contacto contigo si es necesario, de acuerdo con sus Términos de Servicio.

Paso 2: Ingrese el nombre de dominio del servidor

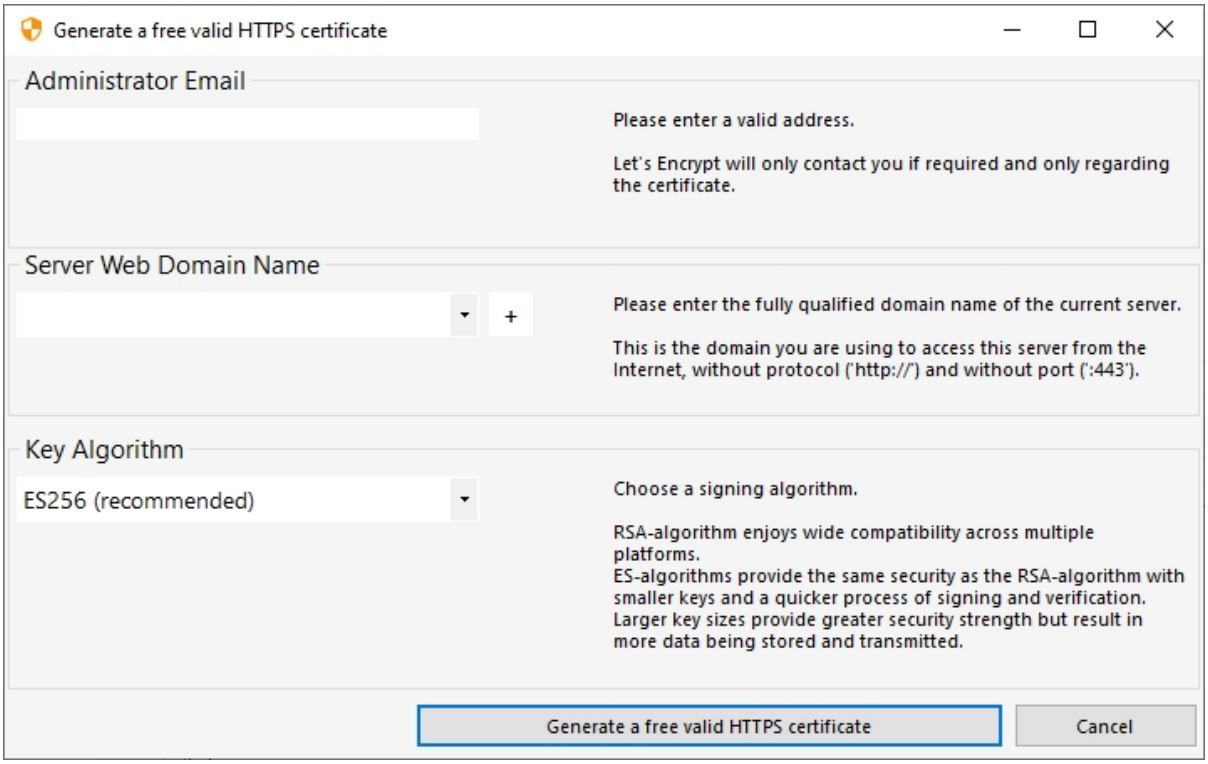
Este es el Nombre de Dominio accesible públicamente por Internet, algo como gateway.tu-empresa.com. También puedes agregar otro nombre de dominio o un nombre de subdominio después de hacer clic en el botón ”+”.

Como se explica en la GUI, no añada un prefijo de protocolo y/o un sufijo de puerto, solo ingrese el nombre de dominio limpio.

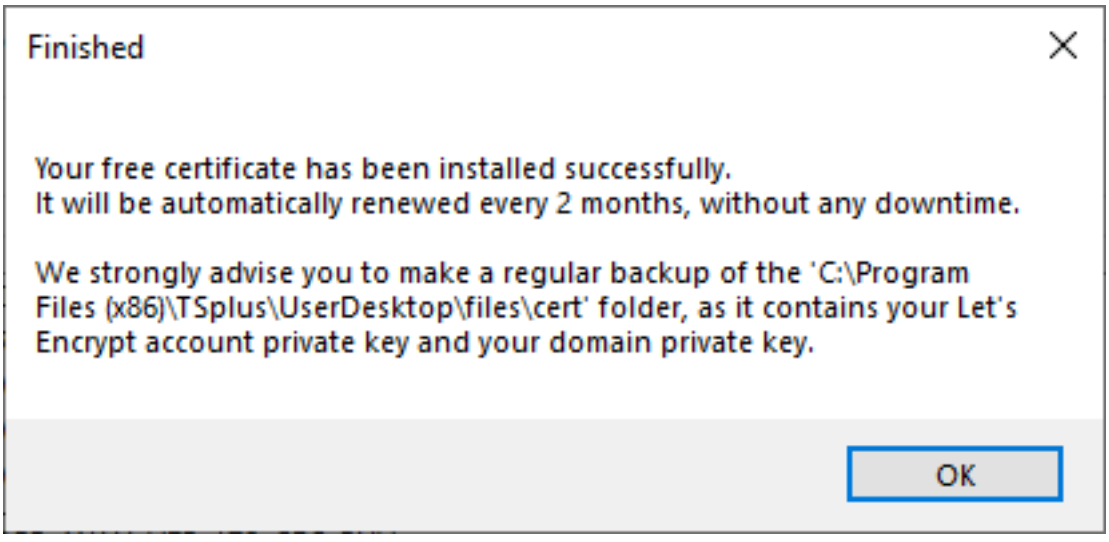
El certificado se generará para este nombre de dominio y solo será válido en una página web alojada en este nombre de dominio. Si sus usuarios se conectan a su Web Portal utilizando https://server1.example.com:1234 entonces debes ingresar "server1.example.com".

Paso 3: Elija un algoritmo de clave

Se utilizará para crear pares de claves y realizar operaciones de firma digital.



¡Disfruta de tu certificado!



TSplus Free Certificate Manager ahora utilizará todos los datos para conectarse con Let’s Encrypt, validar que realmente posees el nombre de dominio que escribiste y obtener el certificado válido correspondiente.

Una vez que el programa recibe el certificado, manejará automáticamente todas las conversiones de formato de archivo requeridas y recargará suavemente el servidor web integrado de TSplus para aplicar el nuevo certificado a cada nueva conexión. El servidor web es

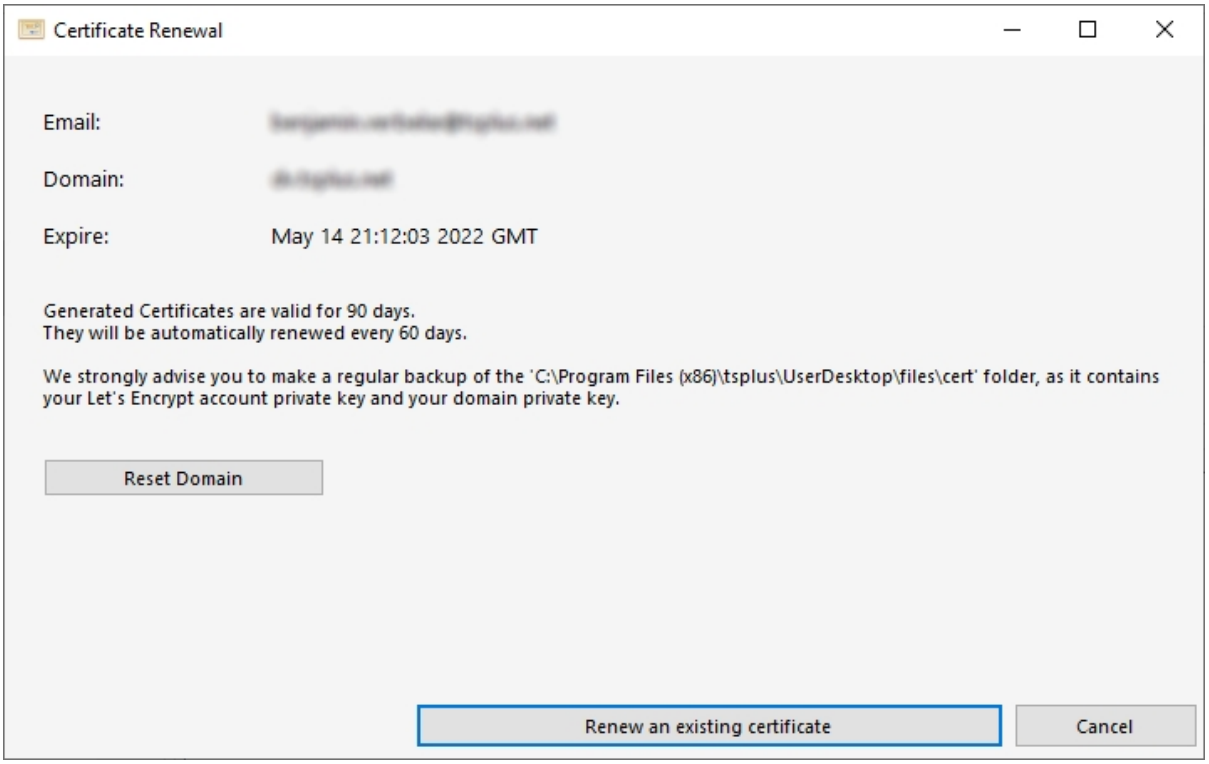
no reiniciado y ninguna conexión está detenida.

Renovación de certificado

Los certificados de Let’s Encrypt son válidos por 90 días. El período de validez se reducirá a la mitad, a 45 días, para 2028, al igual que el resto de la industria.

TSplus renovará automáticamente el certificado cada 15 días por seguridad. Se realiza una verificación en cada reinicio del servidor Windows, y luego cada 24 horas.

Puedes renovar manualmente tu certificado abriendo la herramienta Free Certificate Manager. Mostrará el nombre de dominio del certificado y su fecha de expiración, como se muestra en la captura de pantalla a continuación.



Para renovar manualmente su certificado, simplemente haga clic en el botón "Siguiente".

El botón "Restablecer dominio" en esta ventana elimina el certificado SSL y reconfigura el servidor web a su estado original antes de usar el Administrador de certificados.

Mejores Prácticas

Si no ocurre ningún error, TSplus renovará el certificado automáticamente cada 15 días. Le recomendamos que usted **verifique cada 45 días** que su certificado ha sido renovado automáticamente. Let's Encrypt actualmente emite certificados válidos por 90 días, que se

reducirán a la mitad a 45 días para 2028.

También recomendamos que usted **haga una copia de seguridad al menos una vez al mes** la siguiente carpeta y sus subcarpetas:

C:\Program Files (x86)\TSplus\UserDesktop\files.lego

Esta es una carpeta interna que contiene la clave privada de su cuenta de Let's Encrypt, así como el par de claves de su certificado.

Solución de problemas

En caso de un error por favor, contacte con el soporte y envíeles el siguiente archivo de registro

C:\Program Files (x86)\TSplus\UserDesktop\files.lego\logs\cli.log

Este archivo de registro (y tal vez los otros archivos de registro en la misma carpeta) debería ayudar a nuestro equipo de soporte a investigar y comprender mejor el problema.

Si desea restaurar un certificado utilizado anteriormente ve a la carpeta:

C:\Program Files (x86)\TSplus\Clients\webserver

Contendrá todos los archivos "cert.jks" utilizados. Estos son los archivos de "almacenamiento de claves" y nunca los eliminamos, solo los renombramos con la fecha y hora de su desactivación.

Códigos de error

- Error 801: El Administrador de Certificados Gratuito no pudo registrar su cuenta de Let's Encrypt. Verifique su conexión a Internet. Asegúrese de que su correo electrónico no esté ya registrado en Let's Encrypt. Intente nuevamente con otro correo electrónico.
- Error 802 y Error 803: El Administrador de Certificados Gratuito no pudo recuperar la dirección URL de los Términos de Servicio de Let's Encrypt. Este es un error no bloqueante: aún puedes continuar y aceptar los Términos de Servicio de Let's Encrypt; asegúrate de leerlos primero desde tu navegador, por supuesto.
- Error 804: El Administrador de Certificados Gratuito no pudo validar su acuerdo con los Términos de Servicio de Let's Encrypt con los servidores de Let's Encrypt. Verifique su conexión a Internet. Inténtelo de nuevo.

- Error 805 y Error 806: el Administrador de Certificados gratuito no pudo validar que usted posee el dominio que ingresó durante la creación del certificado (Error 805) o la renovación del certificado (Error 806). Verifique nuevamente todos los requisitos previos. Verifique su conexión a Internet. Verifique que su servidor web esté escuchando en el puerto 80. Verifique que no esté utilizando un servidor web de terceros como IIS o Apache. Verifique que su nombre de dominio sea accesible desde Internet público.

Comando de certificado HTTPS

Preparando el archivo de configuración del certificado

Dentro de la carpeta “C:\Program Files (x86)\TSplus\UserDesktop\files\cert”, crea un archivo llamado “FreeCertificateManager.ini” si aún no existe. Asegúrate de que tu editor de texto y/o el explorador de archivos de Windows no agregue una extensión final “.txt”.

Edita el archivo y escríbelo o actualízalo para que tenga el siguiente formato, luego guárdalo:

configuración

correo = tu.correo@empresa.com

dominio = tu-servidor-nombre-de-dominio.empresa.com

Creando el Certificado

Como administrador del servidor, ejecute el siguiente comando:

C:\Program Files (x86)\TSplus\UserDesktop\files\cert\CertificateManager.exe” /create

Para que este comando sea exitoso:

- El archivo “FreeCertificateManager.ini” debe existir y utilizar el formato esperado.
- Su servidor TSplus Remote Access debe estar en funcionamiento.
- Su portal web de TSplus Remote Access debe estar disponible con el protocolo

HTTP en el puerto 80 desde la red pública de internet, ya que el proveedor de certificados HTTPS de TSplus utilizará eso para validar el nombre de dominio del servidor.

Renovando el Certificado

Una vez que el certificado esté configurado y creado, TSplus Remote Access lo renovará

automáticamente cada dos meses para asegurarse de que nunca expire.

Agregar un certificado de terceros

Dentro de la carpeta “C:\Program Files (x86)\TSplus\UserDesktop\files\cert”, crea un archivo llamado “certpassword.txt” que contenga solo la contraseña del certificado. Como administrador del servidor, ejecuta el siguiente comando:

“C:\Program Files (x86)\TSplus\UserDesktop\files\cert\CertificateManager.exe” /add “tu-ruta-de-certificado”

Si está utilizando TSplus Advanced Security, es posible que deba desactivar temporalmente la función de Protección Geográfica para que funcione. Puede eliminar su archivo de contraseña después de ejecutar el comando.

Evitar el acceso RDP y permitir HTTP en el servidor Gateway

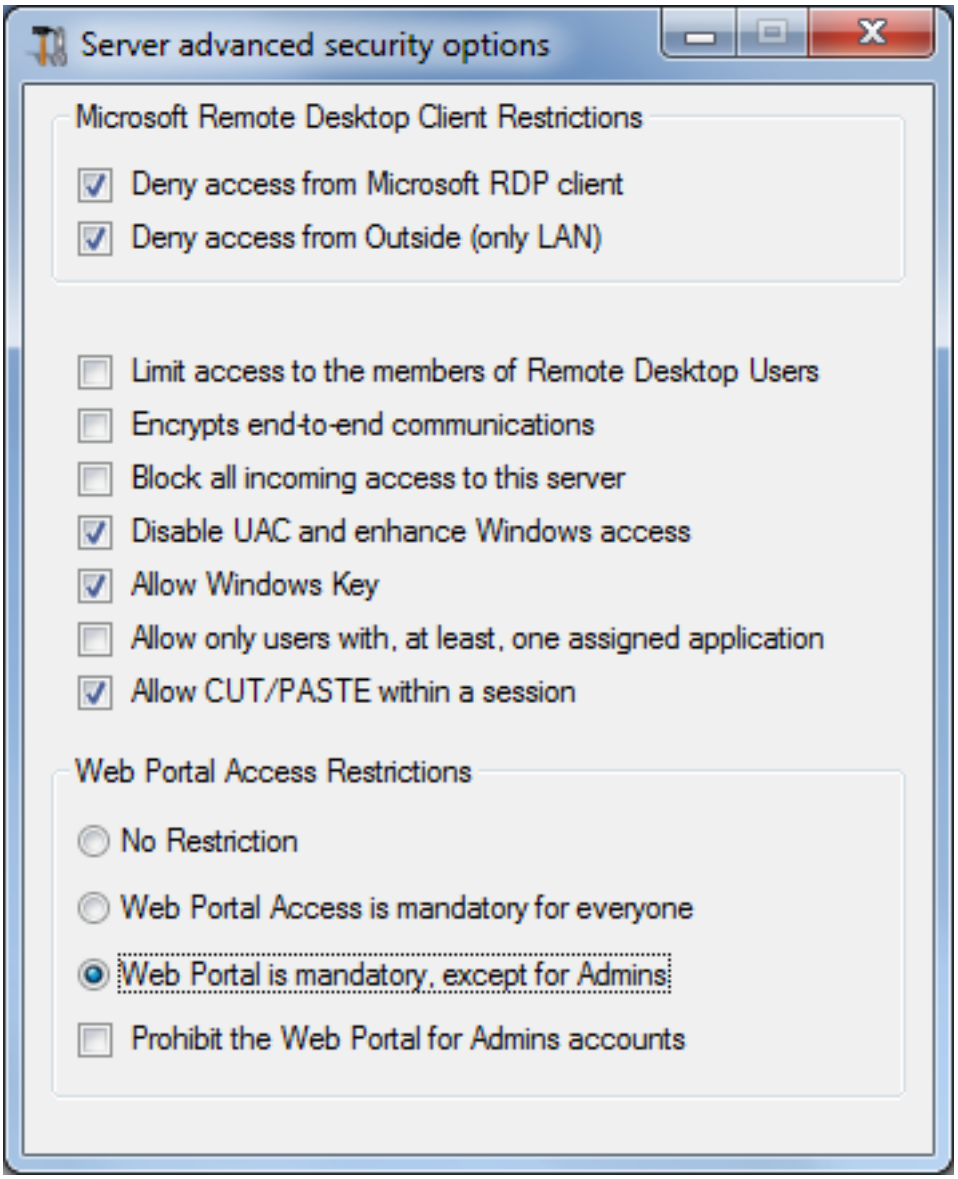
Hay 2 formas de acceder al Servidor Gateway:

- HTML5 / HTML
- Sesión RDP (a través de la IP/DNS del Gateway - Número de puerto)

Cómo BLOQUEAR HTML/HTML5

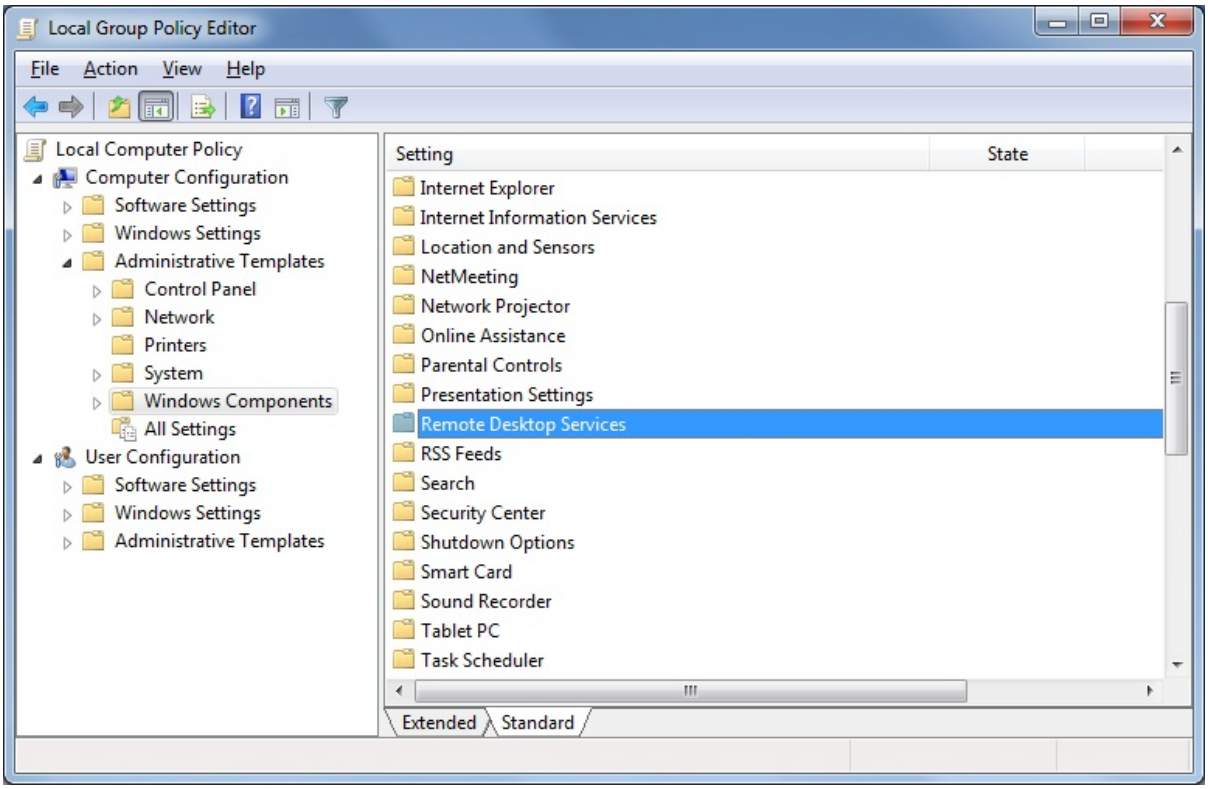
Podemos usar mstsc con un número de PUERTO y RDP en un servidor de aplicación / puerta de enlace de TSplus.

Sin embargo, si utilizamos estas herramientas de seguridad avanzadas ubicadas en la consola de administración de TSplus en el servidor de puerta de enlace, accediendo a la pestaña de seguridad y luego haciendo clic en la opción de seguridad avanzada...

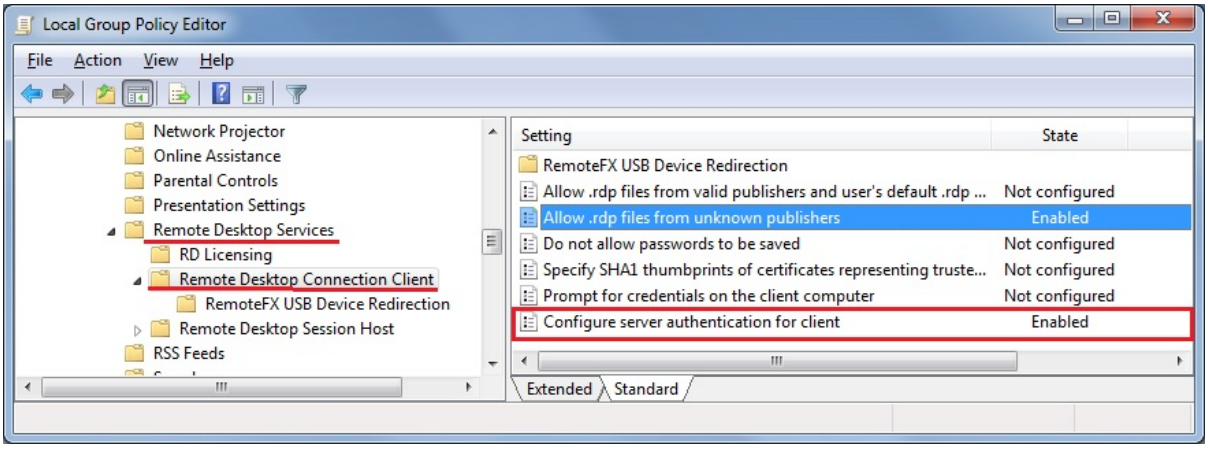


…el acceso se deniega al intentar conectarse con RDP. Para evitar este comportamiento, en el Servidor Gateway, deberá hacer lo siguiente:

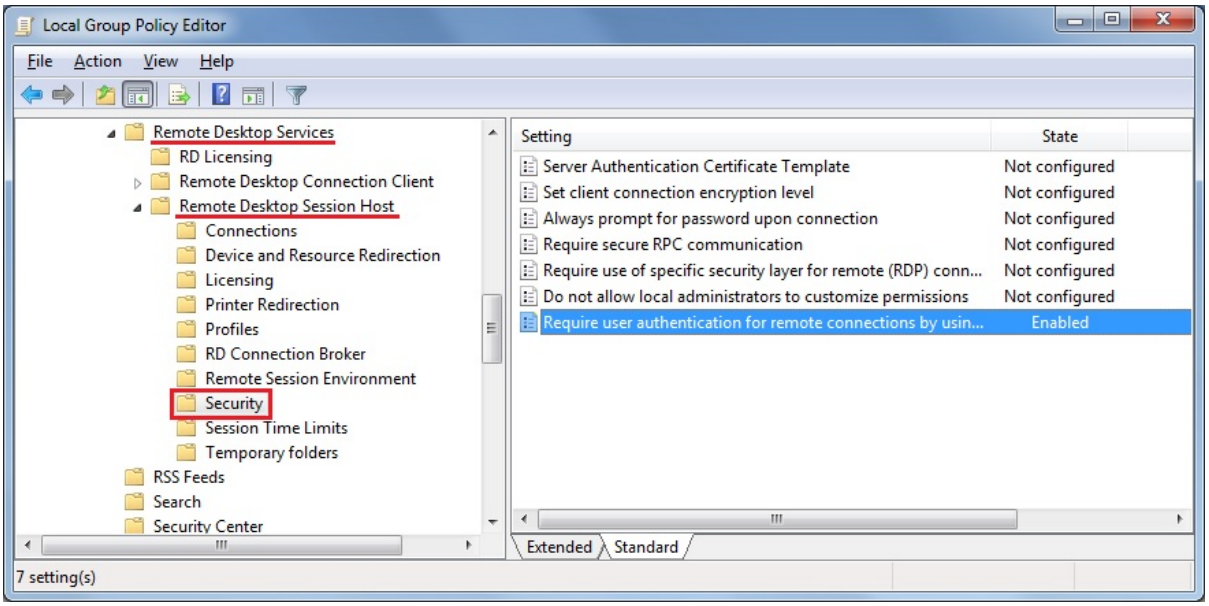
- Ve a Gpedit.msc, luego en Configuración del equipo, haz clic en la carpeta Plantillas administrativas, en la carpeta Componentes de Windows y en Servicios de escritorio remoto:



- Luego, haga clic en la carpeta del Cliente de Conexión de Escritorio Remoto, haga doble clic en la configuración “Permitir archivos .rdp de editores desconocidos” y habilítelo, así como en “Configurar la autenticación del servidor para el cliente”:



- Bajo el menú del Cliente de Escritorio Remoto, haga clic en la carpeta Host de Sesión de Escritorio Remoto, luego en la carpeta Seguridad. Active la configuración "Requerir autenticación de usuario para conexiones remotas utilizando Autenticación a Nivel de Red".

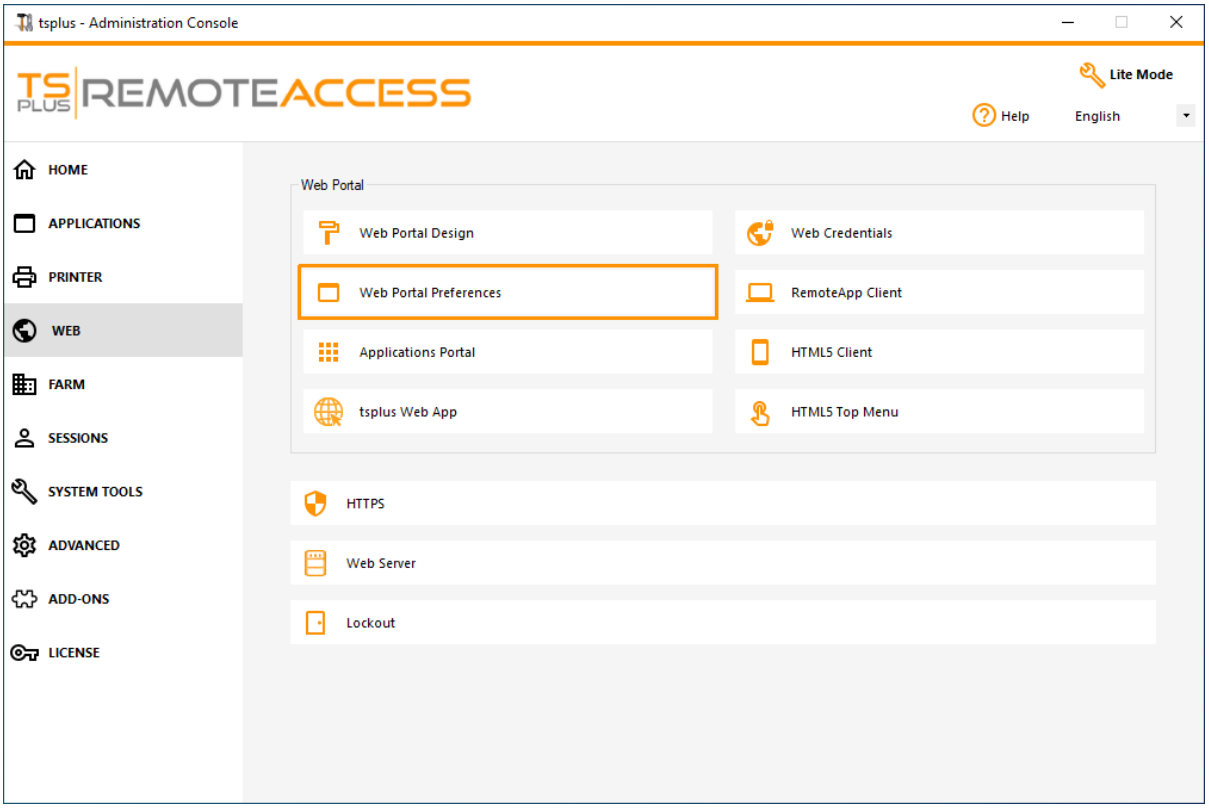

Local Group Policy Editor
File Action View Help
Remote Desktop Services
RD Licensing
Remote Desktop Connection Client
Remote Desktop Session Host
Connections
Device and Resource Redirection
Licensing
Printer Redirection
Profiles
RD Connection Broker
Remote Session Environment
Security
Session Time Limits
Temporary folders
RSS Feeds
Search
Security Center
Setting
State
Server Authentication Certificate Template
Not configured
Set client connection encryption level
Not configured
Always prompt for password upon connection
Not configured
Require secure RPC communication
Not configured
Require use of specific security layer for remote (RDP) conn...
Not configured
Do not allow local administrators to customize permissions
Not configured
Require user authentication for remote connections by usin...
Enabled
Extended
Standard
7 setting(s)

Habilitar/deshabilitar manualmente el servidor de puerta de enlace

Resumen

Basado en la configuración de su granja, el Controlador de Granja cambiará automáticamente su propia configuración del Portal Web para convertirse en un Servidor Gateway. permitiendo a los usuarios conectarse desde el Portal Web de TSplus del Controlador de Granja, no conectarse directamente al Controlador de Granja en sí, sino a uno de los servidores de aplicaciones de la Granja.

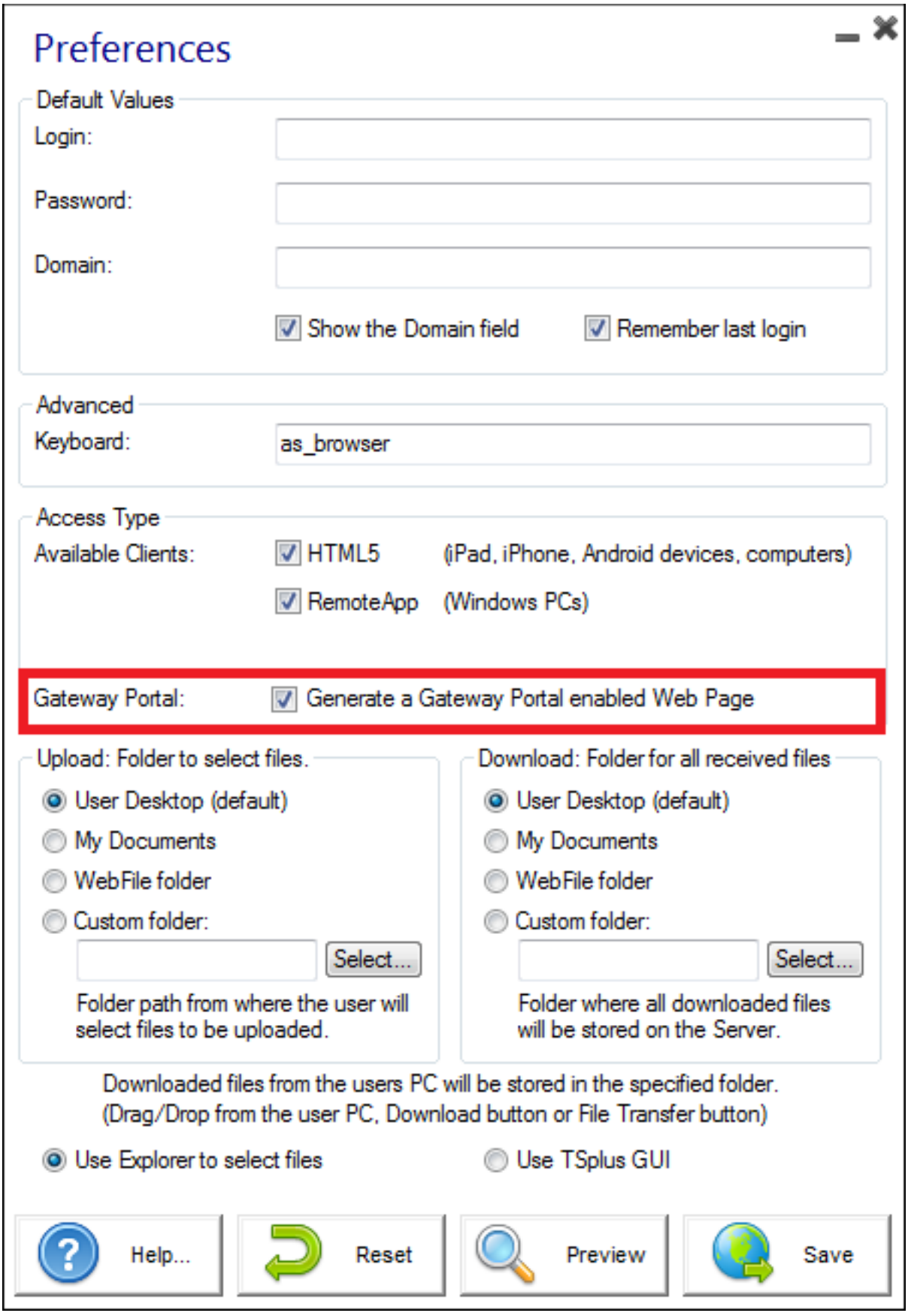
Sin embargo, si desea cambiar este comportamiento manualmente, puede hacerlo haciendo clic en el mosaico "WEB" y luego en el botón de Preferencias del Portal Web.



- Marque la casilla "Generar una página web habilitada para el Portal de Gateway" si desea

que el Portal de Gateway del Controlador de Granja (el servidor actual que está configurando ahora) se convierta en un Servidor de Gateway y redirija a los usuarios a los servidores de aplicaciones de la granja.

- Desmarque la casilla "Generar una página web habilitada para el Portal de Gateway" si desea que el Portal de Gateway del Controlador de Granja redirija al propio Controlador de Granja, eludiendo así cualquier configuración de la granja.



Haga clic en "Guardar" para guardar esta configuración.

Identificador de hardware y servidor clonado

1- Cambio de identificador de hardware.

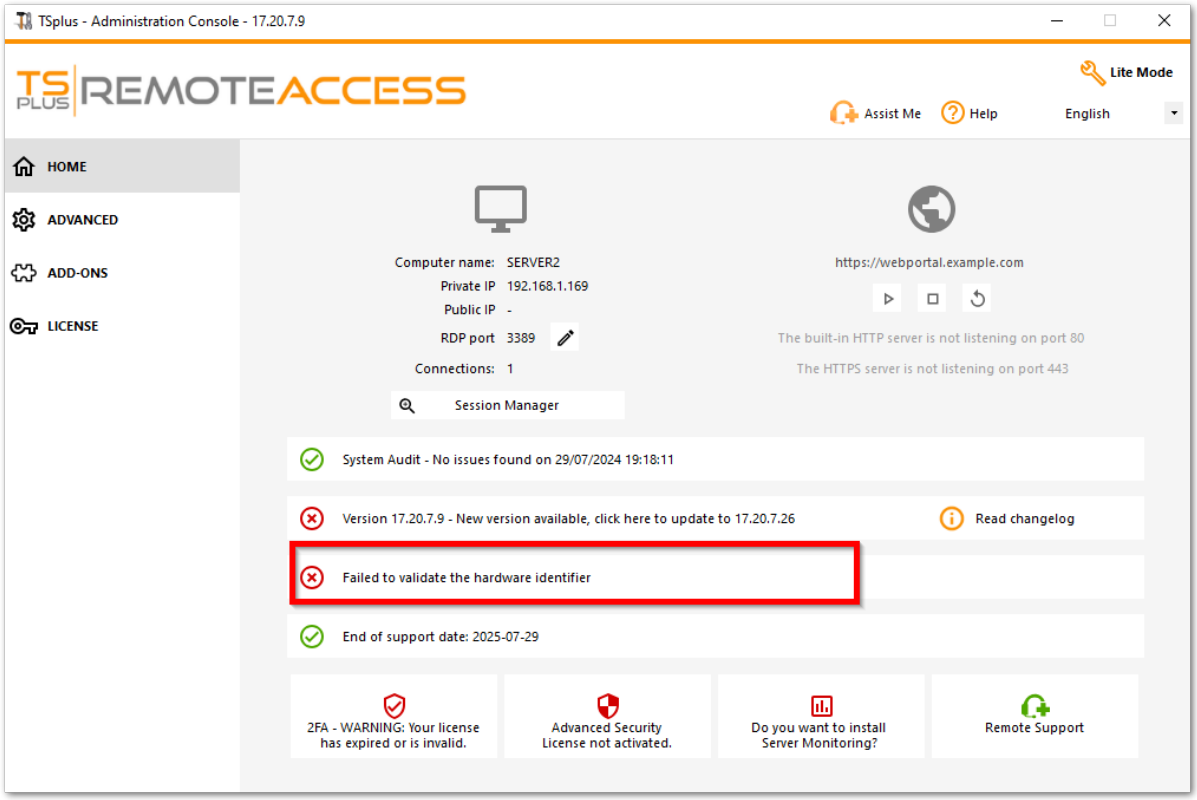
Reparar el identificador de hardware tras la clonación o una actualización.

Advertencia: No se pudo validar el identificador de hardware

Después de migrar un servidor físico a una máquina virtual o una actualización de Kernel de Microsoft, el estado de la licencia cambia a Fallido al validar el identificador de hardware en nuevo hardware.

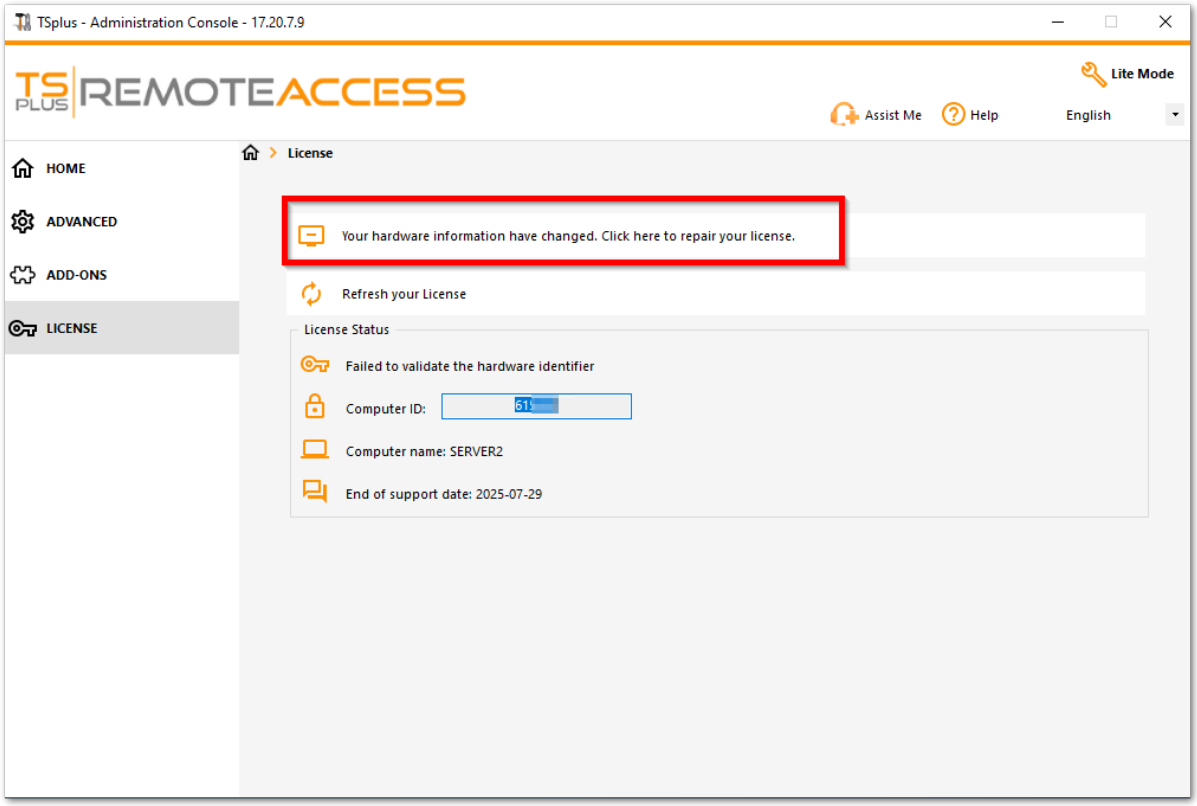
Este mensaje aparece porque TSplus ha detectado un conflicto de licencia copiado de un servidor a otro con el mismo ID de computadora y el mismo nombre.
Ya recomendamos renombrar su nuevo servidor (Ejemplo: SERVER1 > SERVER2)

- Reinicie su servidor



Haz clic en la ventana para llegar a la página de licencia.

Luego haga clic en la pestaña "Su información de hardware ha cambiado. Haga clic aquí para reparar su licencia.



Se abrirá una ventana emergente de "rehospedaje de licencia" para permitirle restaurar su licencia.

Caso 1: ¡No tienes soporte!
La rehosting, por lo tanto, no será posible; tendrás que suscribirte a una suscripción de soporte en el servidor original y comenzar nuevamente la acción de migración.
En caso de problemas, Contact Support y indique su ID de computadora y clave de activación.

Caso 2: ¡Ya has rehosted durante 6 meses!
El mensaje: Ya has reubicado esta computadora en los últimos 6 meses. Por favor, contacta con Soporte si necesitas ayuda para reubicar tu licencia.

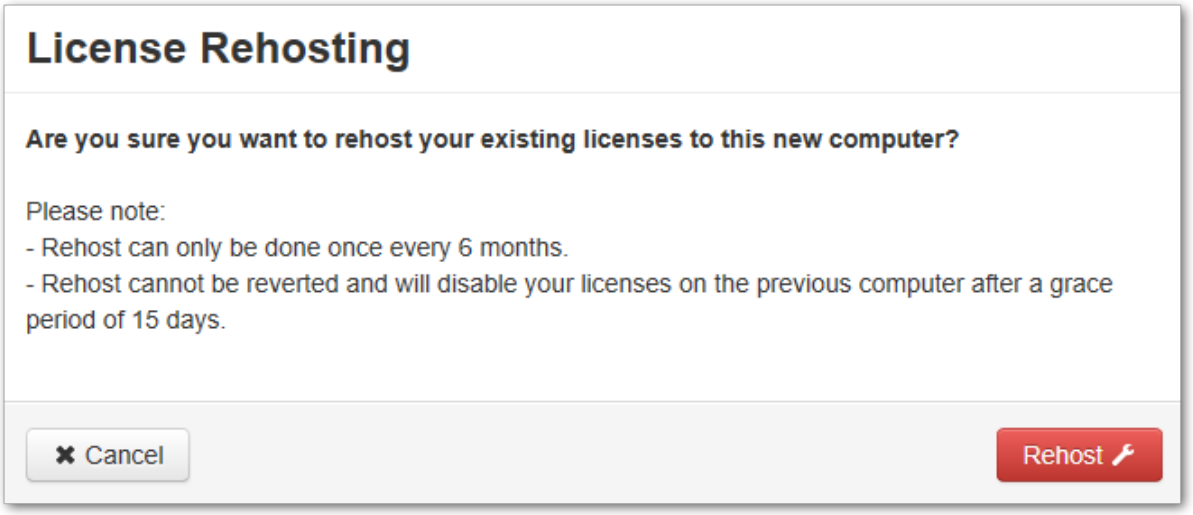
La reubicación, por lo tanto, no será posible, Contact Support y indique su ID de computadora y clave de activación.

Caso 3: ¡Tienes soporte!
El siguiente mensaje aparece: ¿Está seguro de que desea reubicar sus licencias existentes en esta nueva computadora?

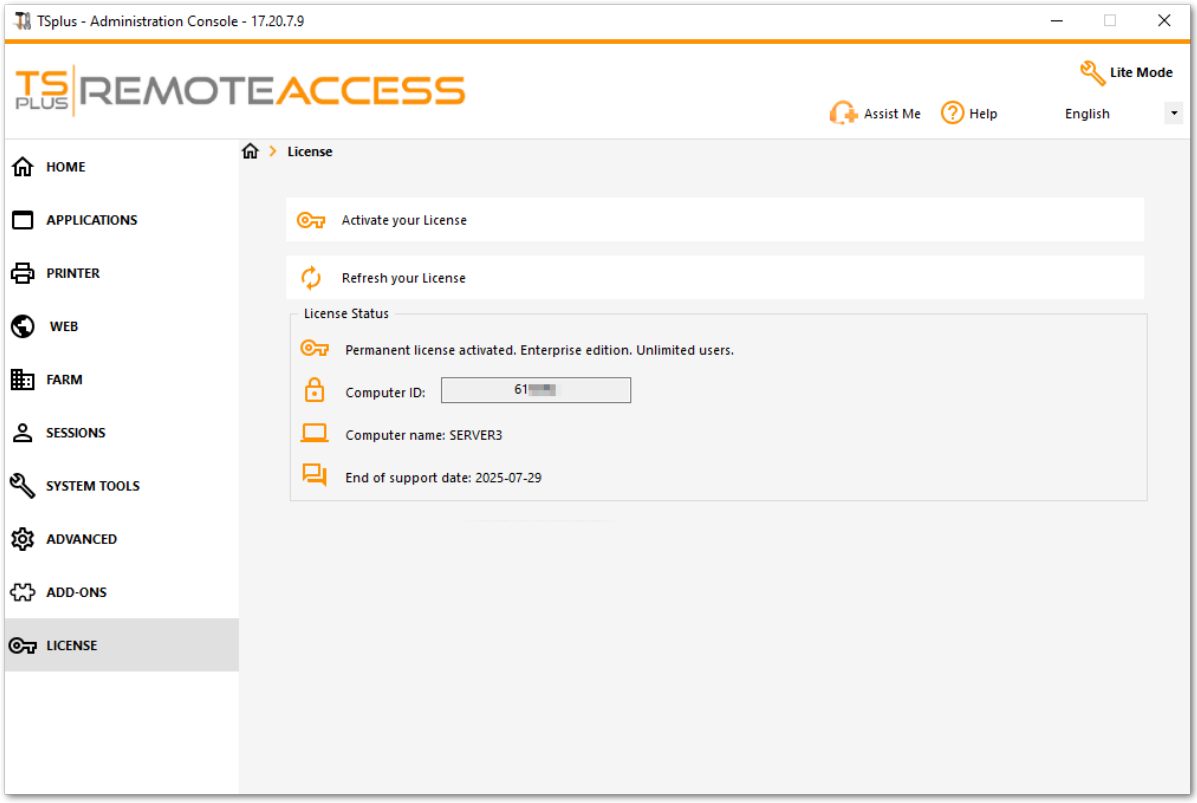
Por favor, tenga en cuenta:

- La reubicación solo se puede realizar una vez cada 6 meses.
- La reubicación no se puede cancelar y desactivará sus licencias en la computadora anterior después de un período de gracia de 15 días.

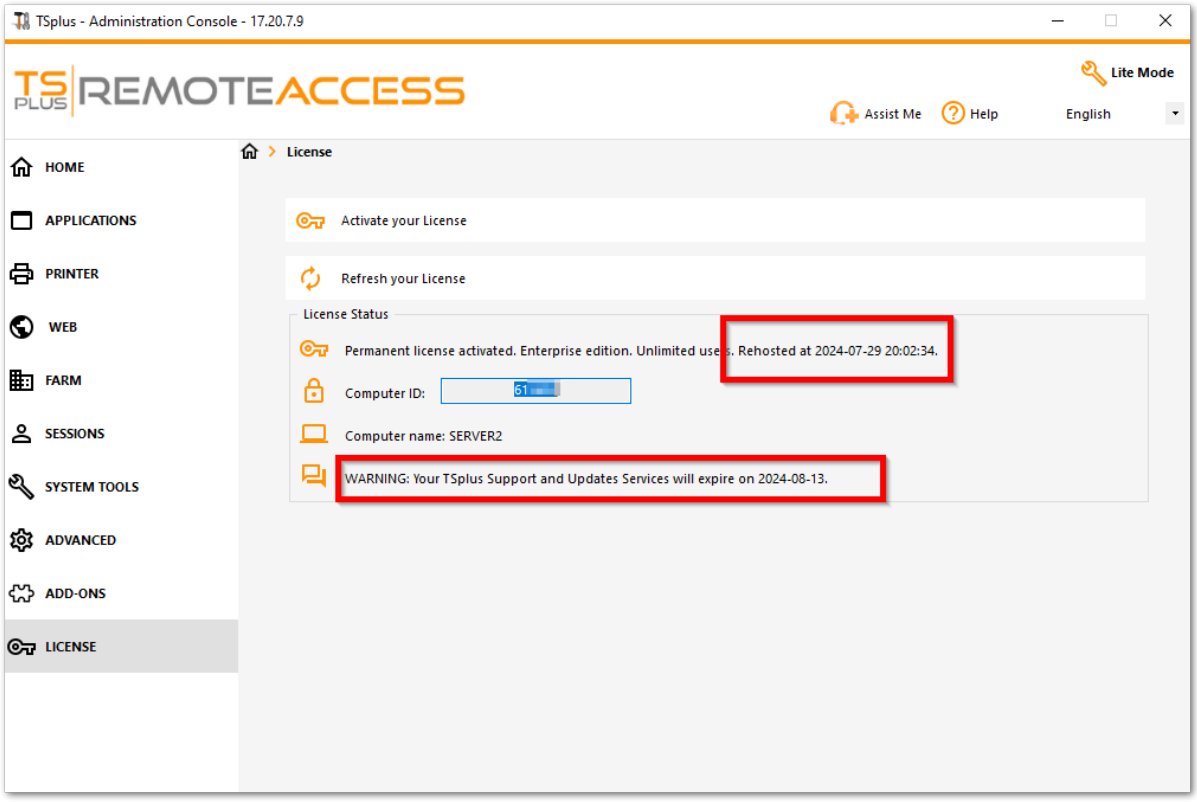
Haga clic en el **"REHOST"** botón



¡Su licencia está reubicada!



Nota: Aparecerá un mensaje en el servidor antiguo con la fecha de rehosting así como la fecha de finalización del período de uso del servidor antiguo (15 días).



Error de actualización:

Ejecute la actualización y verifique si esto ha resuelto su problema después de reiniciar su servidor.

- Descargar el Actualización de la versión

2- Clonar un servidor mientras se mantiene el servidor existente y se activa una nueva licencia.

Requisitos

Al trabajar con máquinas virtuales clonadas, es importante modificar el nombre del equipo y el ID del volumen del disco para garantizar una instalación única de TSplus Remote Access y evitar problemas de licencia.

Consideraciones sobre el nombre del ordenador

El nombre de la computadora se almacena en el registro de Windows dentro de la imagen misma. Si se modifica antes de aplicar la imagen, será sobrescrito por Sysprep cuando Windows se inicie. Sin embargo, puedes predefinir un nombre en un Unattended.xml Archivo de respuesta. Ver Documentación de Microsoft para más detalles.

Para establecer el nombre del equipo, agregue la siguiente sección dentro de Microsoft-Windows-Shell-Setup :

```
    <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
        <ComputerName>%COMPUTERNAME%ComputerName>
    component>
```

Consideraciones sobre el ID de volumen

El ID de volumen está asociado con la partición del disco, no con la imagen del sistema operativo. Se puede cambiar antes de aplicar la imagen, y persistirá. Utilice volumeid.exe de Sysinternals, disponible en Microsoft Sysinternals antes de que Windows se inicie.

Pasos de implementación

Al implementar una nueva máquina virtual a partir de una imagen preparada con sysprep, Windows ingresará a la Experiencia de Configuración Inicial (OOBE) en el primer arranque, solicitando la configuración de ajustes.

Pasos recomendados para la implementación:

1. **Arrancar en WinPE** – Prepare el sistema sin iniciar en Windows.
2. **Establecer el ID de volumen** – Cámbialo antes de aplicar la imagen para que persista.
3. **Desplegar la imagen sysprepped** – Utilice DISM para aplicar la imagen a C: .
4. **Establecer el nombre del equipo sin conexión** – Edite el registro dentro de la imagen montada.
5. **Copiar un Unattended.xml archivo** – Automatizar la configuración OOBE. Este archivo se puede modificar dinámicamente antes de la implementación utilizando un script.
6. **Crear un script de primer arranque** – Asegúrese de que las configuraciones finales se realicen con un solo reinicio.
7. **Reiniciar en Windows** – Windows se finaliza utilizando las configuraciones especificadas.
8. **Restablecer la licencia de acceso remoto** – Ejecute el siguiente comando:

Ventana de terminal

AdminTool.exe /license /reset

Esto restablece la licencia y aplica una nueva licencia.

Script de implementación

Por favor, encuentre a continuación el script de implementación de WinPE relacionado.

Ventana de terminal

```
<# Define variables #>
$ImagePath = "D:\Images\Windows.wim"   # Path to your sysprepped image
$ApplyDrive = "C:"                     # Target drive for deployment
$ComputerName = "REMOTE ACCESS-SERVER-" + (Get-Random -Minimum 1000 -
Maximum 9999)  # Generate a random name (naive implementation)
$VolumeID = "1234-ABCD"                # Desired Volume Serial Number
$UnattendFile = "D:\Unattended.xml"    # Path to the unattended answer file

Write-Host "=== Windows Deployment Automation ==="

<# 1. Set Volume ID before applying the image #>
Write-Host "Setting Volume ID..."
Start-Process -NoNewWindow -Wait -FilePath "volumeid.exe" -ArgumentList "$ApplyDrive
$VolumeID"

<# 2. Apply the Sysprepped Windows image #>
Write-Host "Applying Windows Image..."
dism /apply-image /imagefile:$ImagePath /index:1 /applydir:$ApplyDrive

<# 3. Load Registry Offline to Set Computer Name #>
Write-Host "Modifying Registry to Set Computer Name..."
reg load HKLM\TempSys $ApplyDrive\Windows\System32\Config\SYSTEM
reg add "HKLM\TempSys\ControlSet001\Control\ComputerName\ComputerName" /v
ComputerName /t REG_SZ /d "$ComputerName" /f
reg unload HKLM\TempSys

<# 4. Ensure Unattended Setup is Used #>
Write-Host "Copying Unattended File..."
Copy-Item -Path $UnattendFile -Destination "$ApplyDrive\Windows\Panther\Unattended.xml" -
Force

<# 5. Set the First Boot Script for Final Configurations #>
Write-Host "Creating First Boot Script..."
$FirstBootScript = @"
Write-Host "Finalizing Configuration..."
Rename-Computer -NewName "$ComputerName" -Force
```

```
    Restart-Computer -Force
    "@
    Set-Content -Path "$ApplyDrive\Windows\Setup\Scripts\SetupComplete.cmd" -Value
$FirstBootScript -Encoding ASCII

    Write-Host "Deployment Complete! Rebooting into Windows..."
    Write-Host "================================================"
    Write-Host "  Computer Name: $ComputerName"
    Write-Host "  Volume ID: $VolumeID"
    Write-Host "  Image Applied to: $ApplyDrive"
    Write-Host "================================================"

    <# Reboot into Windows #>
    wpeutil reboot
```

Activación de licencias

Después de la implementación, activar una licencia generará un nuevo ID de computadora para la máquina virtual. Este ID de computadora es creado por el portal de licencias cuando una máquina solicita una prueba o activación de licencia. Para las máquinas virtuales clonadas, la activación de la licencia es obligatoria. Utilice una clave de activación o una clave de licencia por volumen. **Las configuraciones fuera de línea no están permitidas** debido a preocupaciones de seguridad. Para obtener pasos de activación detallados, consulte Lista de comandos de TSplus .

Conclusión

Esta guía describe las consideraciones clave para implementar máquinas virtuales clonadas con TSplus Remote Access. Proporciona pasos esenciales para configurar y licenciar el sistema correctamente y debe adaptarse a sus necesidades y requisitos.

Cómo: Vincular el servidor web a varias tarjetas de red

Resumen

Algunos casos de uso pueden requerir que el servidor web de Terminal Service Plus escuche en más de una tarjeta de red, por ejemplo, si el servidor pertenece a varias redes diferentes.

Esta función responde a esta necesidad específica.

Vinculación del servidor web a varias tarjetas de red

Para vincular el servidor web de Terminal Service Plus a varias tarjetas de red, necesita:

- Crea el archivo “settings.bin” en la carpeta “C:\Program Files (x86)\TSplus\Clients\webserver”
- Agregue la siguiente línea con todas las direcciones IP locales para todas las tarjetas de red que desea vincular, por ejemplo:

  bind_nic=“127.0.0.3”,“127.0.0.4”
- Reinicie el servidor web (AdminTool > Web > Reiniciar servidores web) para aplicar los cambios

El servidor web de Terminal Service Plus ahora escuchará todas las consultas de todas las tarjetas de red vinculadas (en nuestro caso de ejemplo, la vinculación se realizaría automáticamente a 127.0.0.3, 127.0.0.4 y 127.0.0.1).

Cómo: Agregar un encabezado HTTP personalizado

Requisitos

Esta función es muy técnica y esta documentación es solo para expertos técnicos.

Deberías estar familiarizado con el protocolo HTTP así como con los encabezados HTTP.

Resumen

Algunos casos de uso pueden requerir que el servidor web de Terminal Service Plus devuelva uno o más encabezados HTTP personalizados además de los estándar.

Esta función responde a esta necesidad específica.

Configurando un encabezado HTTP personalizado

Para agregar su propio encabezado HTTP personalizado, necesita:

- Crea el archivo “headers.bin” en la carpeta “C:\Program Files (x86)\TSplus\Clients\webserver”
- Agregue los encabezados personalizados separados por nueva línea, por ejemplo: encabezado1=X-Frame-Options
- Reinicie el servidor web (AdminTool > Web > Reiniciar servidores web) para aplicar los cambios

El servidor de Terminal Service Plus ahora responderá a todas las consultas con este encabezado HTTP personalizado además de los estándar.

Páginas HTML y personalización

Puedes editar las páginas HTML proporcionadas con Notepad o Notepad++ para personalizar la interfaz de usuario.

página index.html

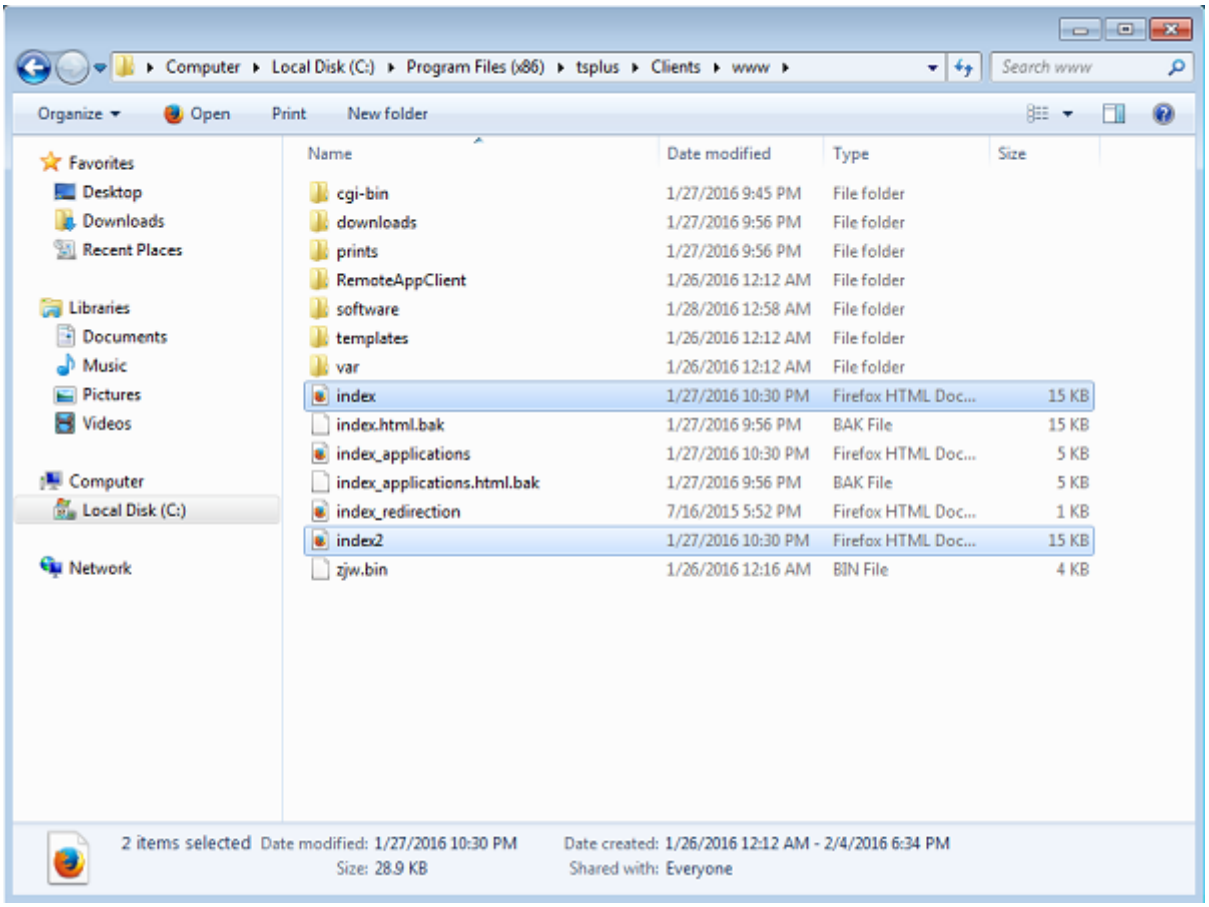
El archivo index.html se encuentra en la ruta de la carpeta raíz del servidor web.

C:\Program Files (x86)\TSplus\Clients\www

La página Index.html es la página web predeterminada. Es como una página de portal de front-end con enlaces a las páginas de conexión que se encuentran en la carpeta \www\.

Esta página web se puede copiar y renombrar para permitir múltiples configuraciones y / o información de inicio de sesión.

Por ejemplo, copiemos y renombremos index.html a index2.html, esta página estará disponible utilizando esta url. http://localhost/index2.html



Tenga en cuenta que si cambia el nombre del archivo “index.html” a “index2.html” y está utilizando el Portal de Aplicaciones Web, entonces debe cambiar la siguiente variable en este archivo: “page_configuration[“applications_portal”] = “index_applications.html” a “index2_applications.html” y luego renombrar el archivo “index_applications.html” a “index_2applications.html”.

El index.html predeterminado incluye todas las opciones posibles:

- Acceso a aplicaciones RemoteApp, conexión fuera del navegador web
- Conexión utilizando HTML5 desde cualquier dispositivo
- Preferencias de impresión local

Podrás cambiar el encabezado y el pie de página en la función de diseño del portal web en el mosaico de preferencias del portal web de la pestaña Web.

Al editar la página web index.html, tendrás acceso a varias configuraciones.

// ---------- Configuración de Acceso ----------

var user = ""; // Inicio de sesión a utilizar al conectarse al servidor remoto (dejar "" para usar el inicio de sesión escrito en esta página)

var pass = ""; // Contraseña a utilizar al conectarse al servidor remoto (dejar "" para usar la contraseña escrita en esta página)

var domain = ""; // Dominio a utilizar al conectarse al servidor remoto (dejar "" para usar el dominio escrito en esta página)

var server = "127.0.0.1"; // Servidor al que conectarse (dejar "" para usar localhost y/o el servidor elegido en esta página)

var port = ""; // Puerto para conectarse (dejar "" para usar localhost y/o el puerto del servidor elegido en esta página)

var lang = "as_browser"; // Idioma a utilizar

var serverhtml5 = "127.0.0.1"; // Servidor al que conectarse, al usar el cliente HTML5

var porthtml5 = "3389"; // Puerto para conectarse, al usar el cliente HTML5

var cmdline = ""; // Texto opcional que se colocará en el portapapeles del servidor una vez conectado

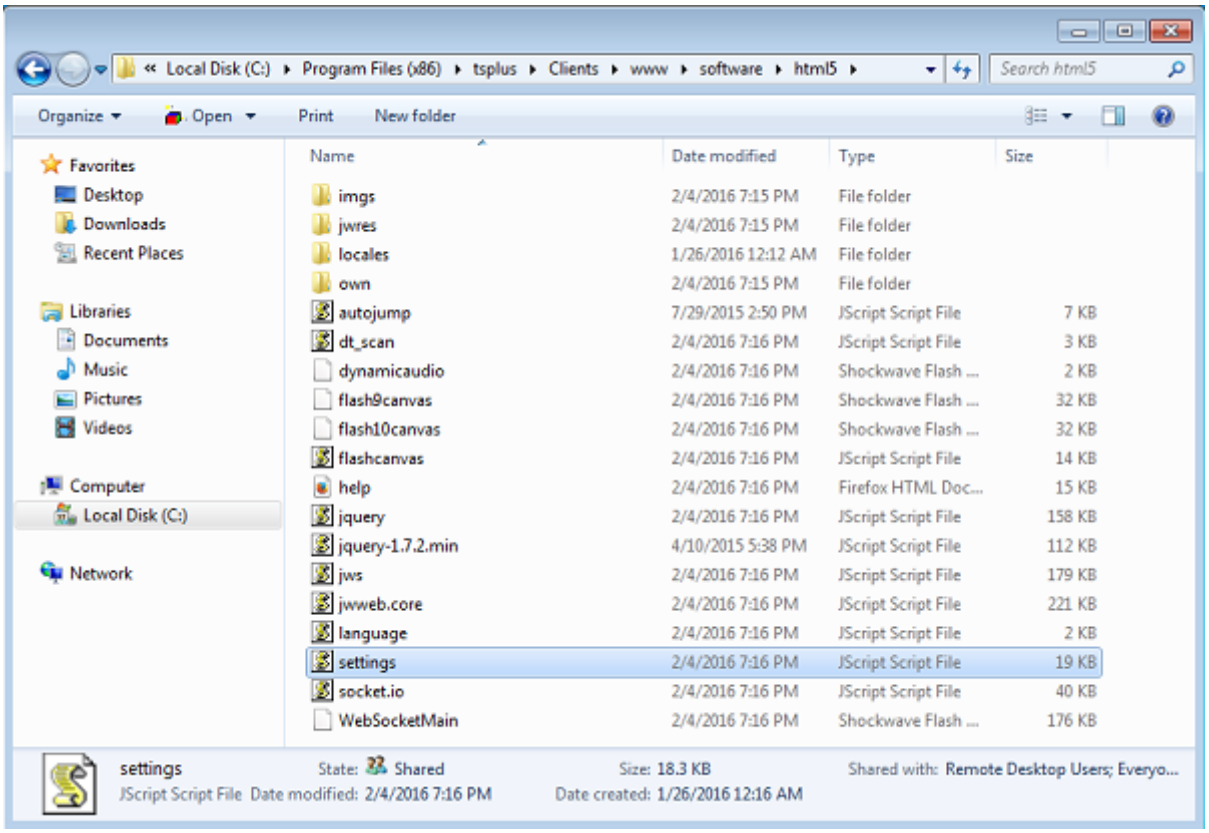
// ---------- Fin de la Configuración de Acceso ----------

Por ejemplo, estableceré demo/Psw como inicio de sesión/contraseña editando:

var user = "Demo"; var pass = "Psw";

Al hacerlo, las credenciales predefinidas son visibles en cada visita al portal.

Otro archivo de configuración muy importante es **settings.js** , ubicado en C:\Program Files (x86)\TSplus\Clients\www\software\html5:



Este archivo contiene varias configuraciones para el cliente web HTML5, como deshabilitar el sonido, el portapapeles o permitir la reconexión de la sesión si se cierra la pestaña del navegador.

- Deshabilitando el portapapeles:

W.clipboard = "sí"; //o "no"

- Desactivar el sonido se realiza con esta configuración:

W.playsound = false;

- Cambiando la resolución predeterminada para dispositivos móviles:

W.viewportwidth = "1024" - La altura se calcula mediante el navegador.

- Forzar HTTPS para conexión remota

W.forcealways_ssl = true;

- Permitir la reconexión de la sesión cuando se cierra la pestaña del navegador:

W.send_logoff = false;

- Agregar un aviso emergente para evitar cerrar la pestaña del navegador:

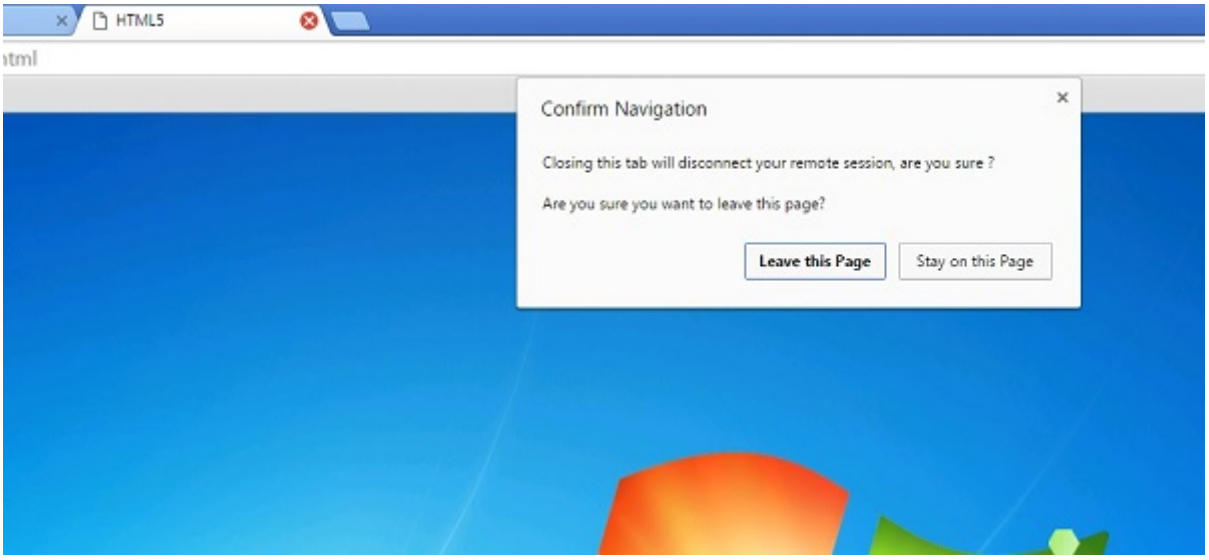
busque el parámetro “W.pageUnloadMessage = "" ”.

He establecido un ejemplo de mensaje que se utilizará a continuación:

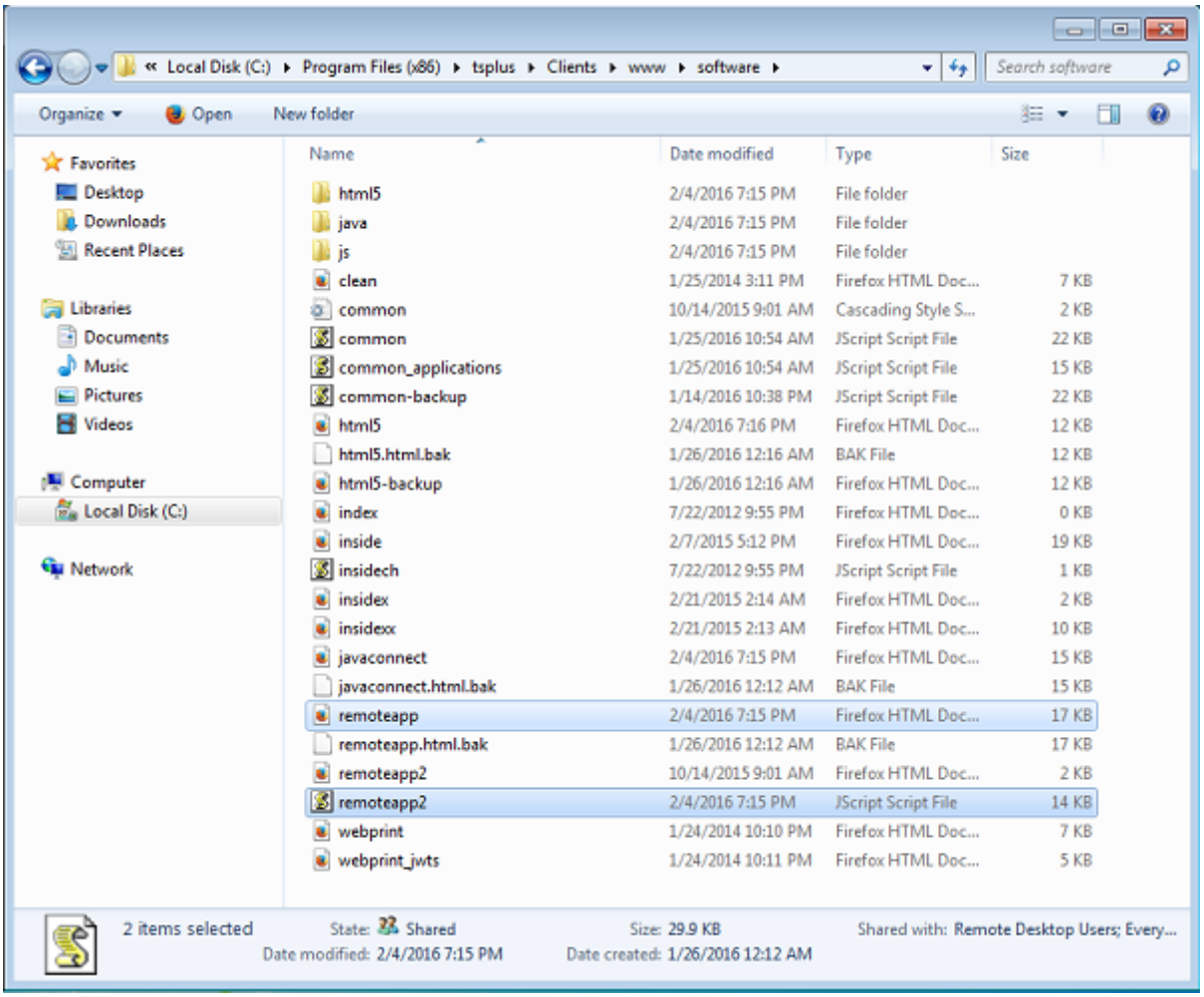
W.pageUnloadMessage = “Cerrar esta pestaña desconectará su sesión remota, ¿está seguro ?”; //Diálogo para devolver cuando se cierra la página.

//1. Aviso importante, los diálogos propios no son compatibles con todos los navegadores.

//2. El estándar HTML no distingue entre la acción de actualizar la página y cerrar la página, el diálogo también aparecerá al actualizar la página.



La configuración general para la página web de RemoteApp se almacena en la carpeta del software, en dos archivos diferentes: **remoteapp.html** y **remoteapp2.js** .



Ejemplo de configuraciones disponibles presentes en **remoteapp2.js** :

// Servidor de Escritorio Remoto

var remoteapp2_server = ''; var remoteapp2_port = '443';

Autenticación de Windows

var remoteapp2_user = ''; var remoteapp2_psw = ''; var remoteapp2_domain = '';

// Parámetros de línea de comandos opcionales

var remoteapp2_apppath = '';

// Modo RemoteApp

var remoteapp2_wallp = 'verde'; var remoteapp2_remoteapp = 'encendido';

// Pantalla

var remoteapp2_color = '32';

```
var remoteapp2_full = '2';

var remoteapp2_width = ”;

var remoteapp2_height = ”;

var remoteapp2_scale = '100';

var remoteapp2_smartsizing = '1';

var remoteapp2_dualscreen = 'apagado';

var remoteapp2_span = 'apagado';

Discos mapeo (requerido para impresión)

var remoteapp2_disk = '1';

// Imprimiendo

var remoteapp2_printer = 'apagado';

var remoteapp2_preview = 'off';

var remoteapp2_default = 'on';

var remoteapp2_select = 'apagado';

// Hardware

var remoteapp2_com = '0';

var remoteapp2_smartcard = '0';

var remoteapp2_serial = 'apagado';

var remoteapp2_usb = 'apagado';

var remoteapp2_sound = 'on';

var remoteapp2_directx = 'off';

// Varios

var remoteapp2_alttab = '0';

var remoteapp2_firewall = '1';
```

```
var remoteapp2_localtb = '32';

var remoteapp2_lock = 'off';

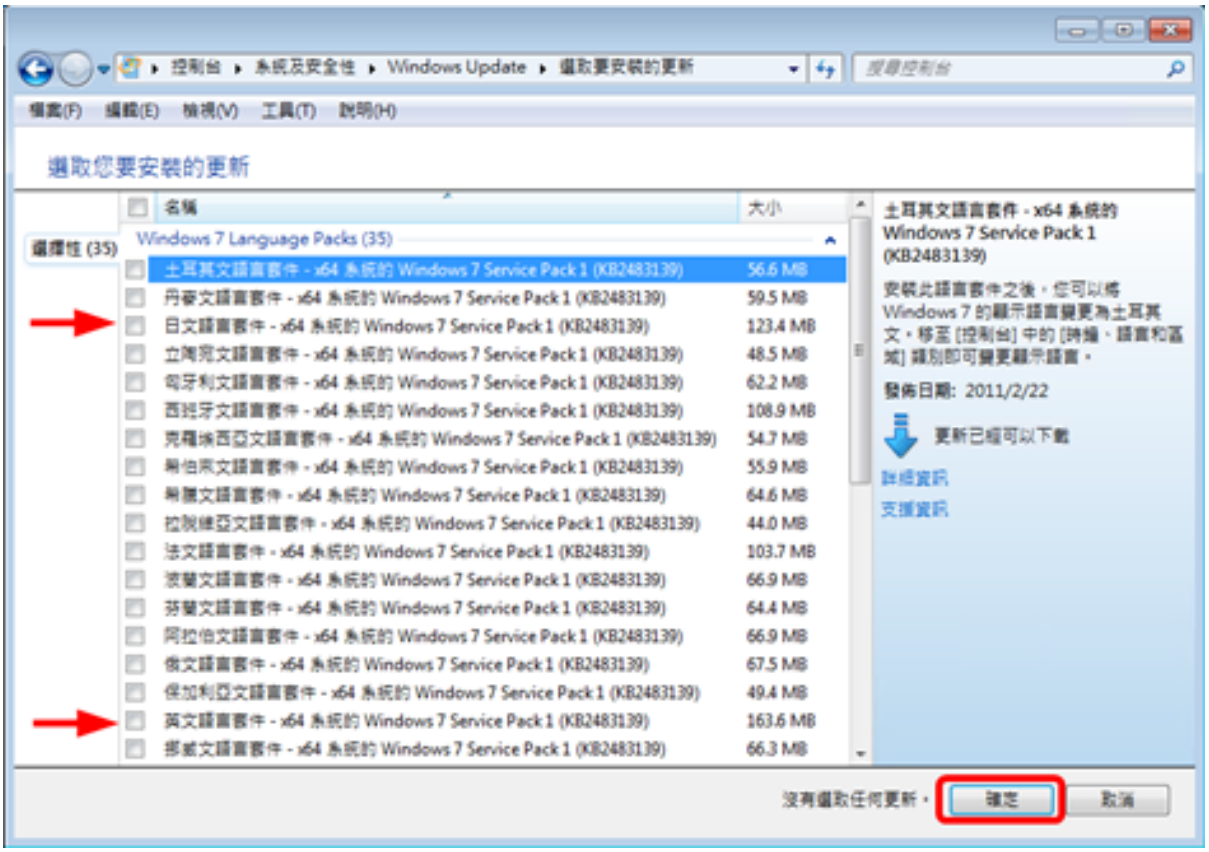
var remoteapp2_rdp5 = 'apagado';

var remoteapp2_reset = 'off';
```

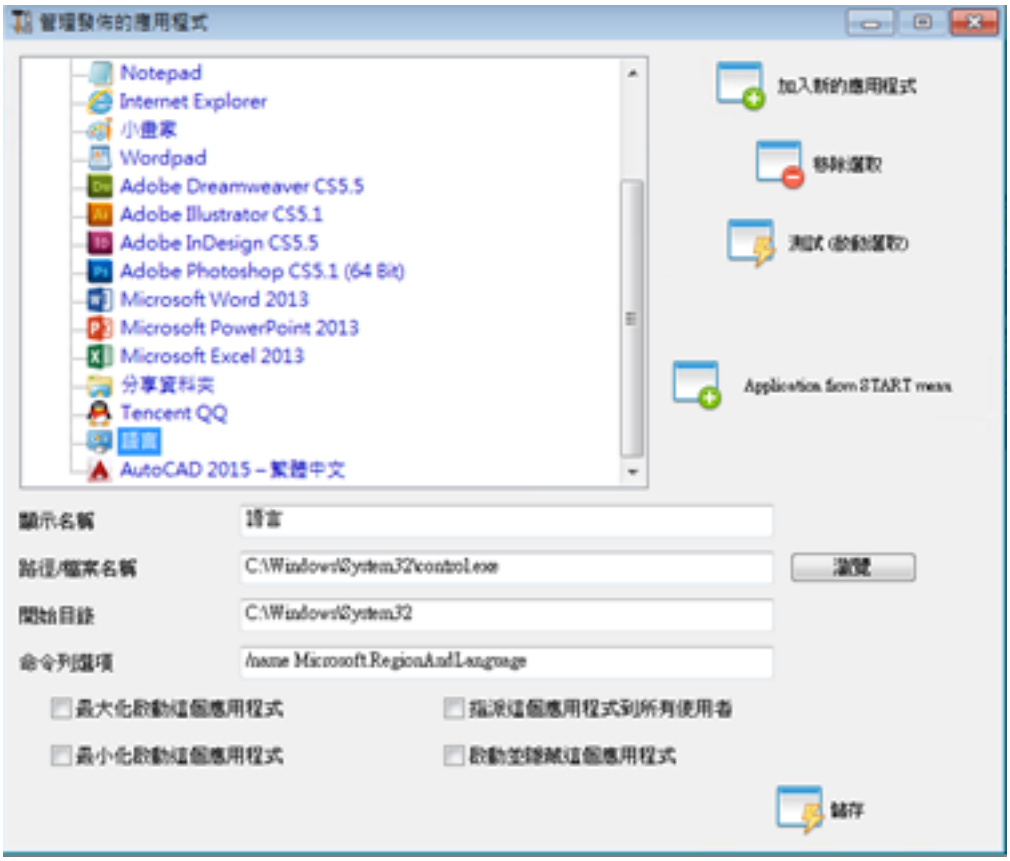
HTML5 : Cambiando el idioma a chino

Necesitas Windows 7 Enterprise o Ultimate / Windows 8 Enterprise o Professional para usar varios idiomas en un solo sistema.

Puedes instalar todos los idiomas en el sistema si lo necesitas.



Podrías publicar un applet de idioma para que los usuarios cambien su propio idioma del sistema operativo de la interfaz de usuario y añadan IME (Editor de Método de Entrada).

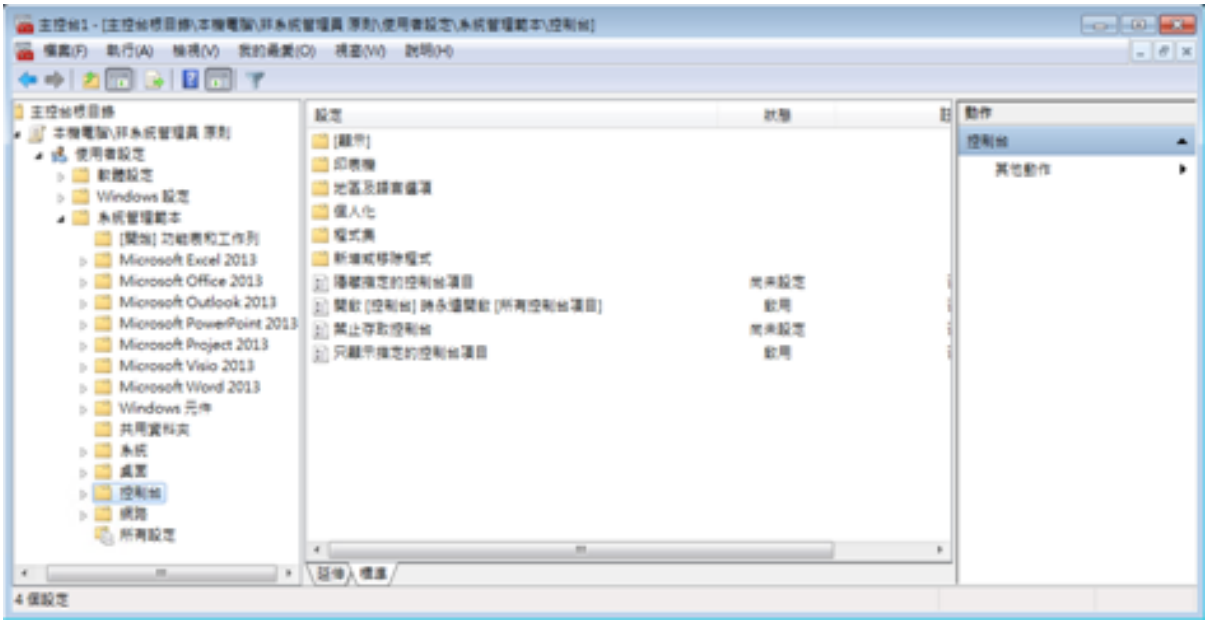


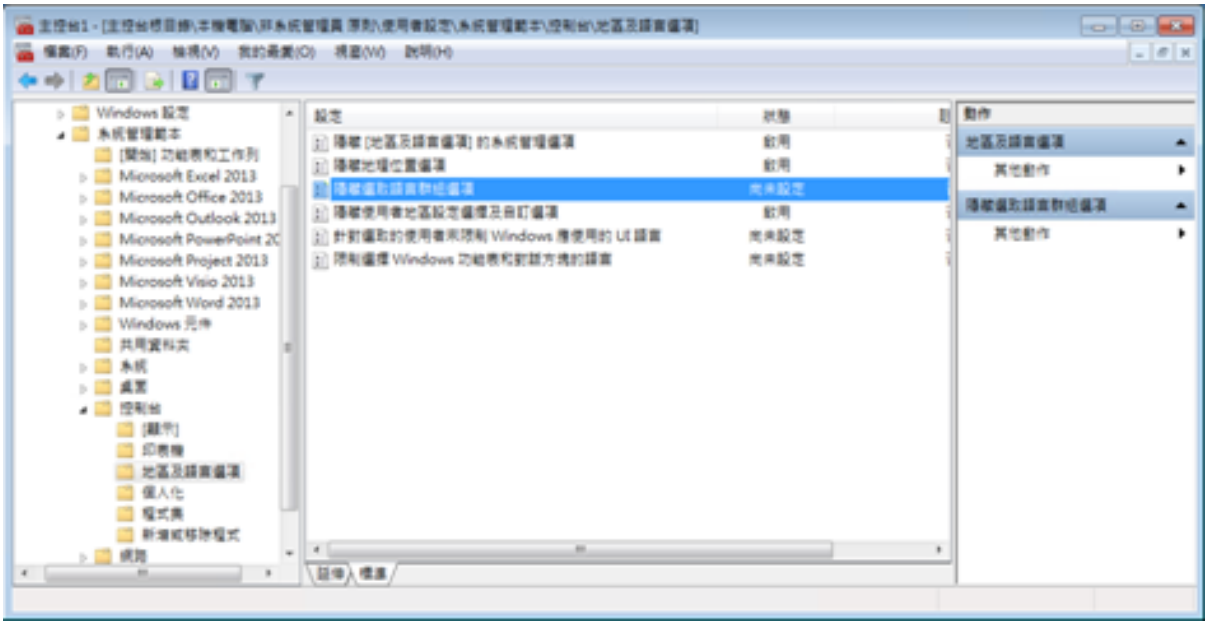
Para Windows 7: control /nombre Microsoft.RegiónYIdioma

Para Windows 8: control /name Microsoft.Language

Lista completa: http://pcsupport.about.com/od/tipstricks/tp/control-panel-applets-list.htm

Opcional: así es como restringir el comportamiento del Panel de Control para los usuarios mediante GPO:

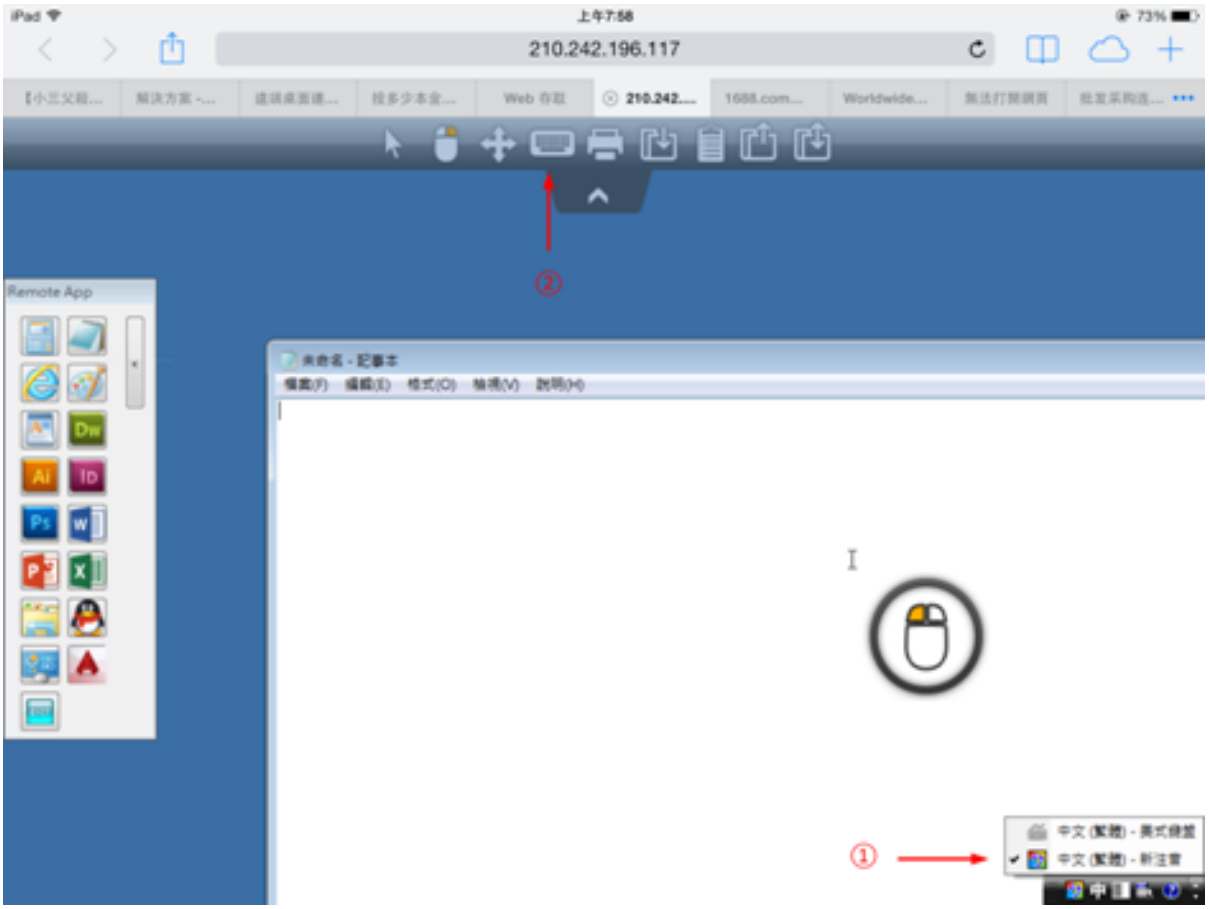




Los usuarios pueden cambiar el idioma del sistema operativo de la interfaz de usuario después de iniciar sesión. (Los usuarios deben cerrar sesión e iniciar sesión nuevamente para que tenga efecto después de cambiar esta configuración)



El usuario debe seleccionar primero el IME chino para ingresar caracteres chinos.


210.242.196.117
Remote App
②
①


210.242.196.117
中文中
中 中文 中國 巾 申 申請 申請人 甲 由 內 內 四 而 p 肉
.?123
上一個
確認
下一個
換行


210.242.196.117
確認
.?123
一聲
.?123

HTML5 Client: ¿Cuál es la diferencia entre Websockets y XHR?

Websockets es la conexión persistente que se puede utilizar para recibir/enviar datos sin un orden secuencial y sin encabezado http.

Xhr-polling crea una nueva solicitud con el encabezado http y espera la respuesta con el encabezado http, también en orden secuencial.

Al hacerlo, el flujo de datos XHR siempre se ve así:

HTTP_HEADER_RESPUESTA -> HTTP_HEADER_RESPUESTA
HTTP_HEADER_RESPUESTA -> HTTP_HEADER_RESPUESTA y así sucesivamente

también antes de que los datos puedan ser descargados, deben ser solicitados con HTTP_HEADER, por lo tanto su nombre: xhr-polling.

El flujo de datos de Websockets puede verse así:

FRAME_DATA_SEND FRAME_DATA_SEND FRAME_DATA_RECEIVE FRAME_DATA_SEND FRAME_DATA_RECEIVE FRAME_DATA_RECEIVE

También se trata de un envío/recepción de datos aleatorios sin un orden secuencial especial y sin ningún dato de encabezado http.

Eso hace que el uso con proxies inversos sea imposible debido a la falta de soporte para Websockets por la mayoría de los proxies inversos conocidos; pero la mitad del transporte xhr puede funcionar con el proxy inverso de Apache.

También vea: Cliente HTML5: Navegadores compatibles

HTML5 Cliente: resolución de sesión RDP en dispositivos móviles

La resolución de pantalla común en la mayoría de los dispositivos, especialmente en teléfonos móviles, es 320x480, pero eso no es suficiente para crear la sesión RDP.

Por lo tanto, la resolución se configuró en 800 de ancho. La altura de la resolución se recalcula mediante la lógica nativa de los navegadores ocultos. Cuanto mayor sea el ancho, mayor será la altura.

- Como ejemplo, la resolución estándar es 320x480, ahora cuando configuras el viewport a 800, el navegador recalcula el valor de la altura, por ejemplo, a 800x904, cuando configuras el ancho a 1280, entonces es 1280x1160, etc.

La altura y el ancho dependen de la vista en paisaje/retrato de su dispositivo, como 800x904 o 904x800, etc. Cada navegador puede recalcularlo según su propia lógica para ajustar la pantalla RDP en el área visible de su dispositivo y puede diferir dependiendo del navegador, incluso cuando se utiliza en el mismo dispositivo.

Si estableces la altura manualmente, romperás la relación de aspecto de tu dispositivo y la sesión RDP final estará fuera de la vista de tu puerto, y para alcanzar estas áreas tendrás que desplazarte a las posiciones deseadas.

- Por lo tanto, se recomienda no establecer la altura manualmente, sino dejar que el dispositivo elija automáticamente la altura.

Si necesitas más altura, ¡aumenta el ancho!

Al probar en dispositivos móviles, el buen valor para el ancho fue 800. Sin embargo, debes prestar atención: los CPU en la mayoría de los teléfonos móviles suelen ser lentos, por lo tanto, cuando aumentas la altura, aumentará la carga del CPU. En dispositivos tablet, los CPU son más rápidos, por lo que se recomienda establecer el ancho en un valor más alto como 1280 y permitir que el dispositivo vuelva a calcular el valor de la altura.

Porque algunos navegadores como FireFox móvil no permiten la configuración del viewport después de cargar la página, este valor se estableció fijo en el archivo Clients\www\software\html5.html:

Por ejemplo, cámbialo a:

para aumentar el ancho y al mismo tiempo la altura recalculada por la lógica interna nativa de los navegadores.

Como segundo ejemplo, cambiándolo a:

rompería el área de visualización y la sesión RDP no se ajustaría a la pantalla.

Cliente HTML5: Parámetros en la dirección URL

Al utilizar el cliente HTML5 de Terminal Service Plus para conectarse a un servidor remoto, puede especificar varios parámetros en la dirección URL para anular los parámetros predeterminados, tales como:

- inicio de sesión de usuario
- contraseña de usuario
- programa para ejecutar
- directorio de inicio para que el programa se ejecute
- línea de comandos para el programa a ejecutar

Ejecutar una aplicación específica

Aquí hay un ejemplo de una dirección URL completa para abrir una sesión remota para el usuario "demo" con la contraseña "demo" y al iniciar el bloc de notas estándar al abrir la sesión:

https://demo.tsplus.net/software/html5.html?user=demo&pwd=demo&program=c:\\windows\\system32\\notepad.exe&startupdir=c:\\windows\\system32¶ms=

Por favor, tenga en cuenta que en la dirección URL todos los caracteres de barra deben repetirse. **4 veces** .

No es necesario especificar todos estos parámetros al mismo tiempo: los parámetros no especificados tendrán su valor configurado por defecto.

Conéctese con credenciales web

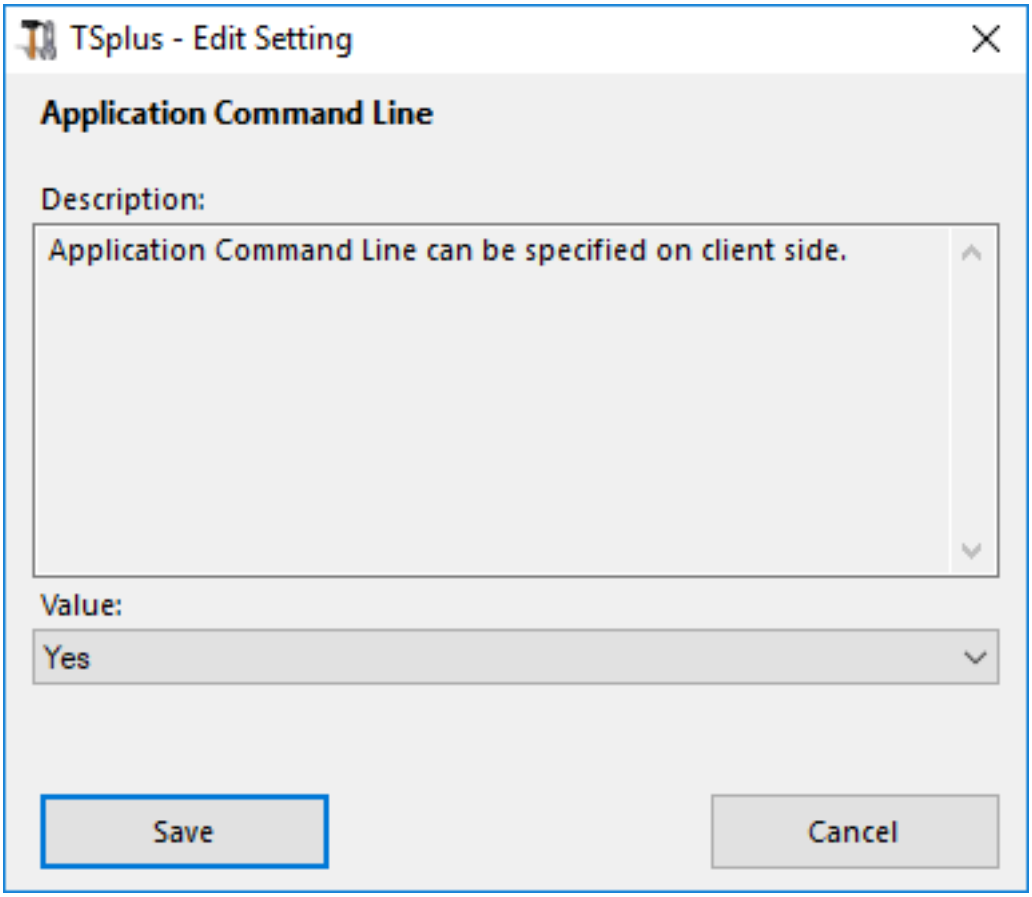
Si deseas utilizar un Credencial Web para conectarse, puede pasarlo en una URL agregando un "@" antes del inicio de sesión web.

Aquí hay un ejemplo de una dirección URL para abrir una sesión remota con el Panel de Aplicaciones para Credenciales Web “1234” con la contraseña “demo”:

https://demo.tsplus.net/software/html5.html?user=@1234&pwd=demo

Restringir este uso a las Aplicaciones Predeterminadas de los Usuarios

Puedes deshabilitar la Línea de Comando de la Aplicación para los usuarios yendo a la **Avanzado —> Pestaña de sesión** del AdminTool, haciendo doble clic en la configuración de "Línea de Comando de Aplicación" y estableciendo el valor en "No".



Cliente HTML5: Navegadores compatibles

Si su navegador muestra una advertencia roja al iniciar al usar el cliente HTML5

Significa que su navegador no es compatible con Websockets o su navegador no es compatible con Canvas.

Los navegadores que no son compatibles con estas tecnologías son IE6, IE7, IE8, IE9 y necesitan FLASH para emular estas funciones.

Navegadores que soportan Websocket y Canvas

Navegadores	Lona	Websocket
FireFox	Completo	Versión completa a partir de la 4
Chrome	Completo	Completo en la mayoría de las versiones conocidas en PC.
Ópera	Completo	Completo en las versiones más recientes
IE6	Flash	Flash (emulado y sin soporte de proxy)
	Flash	XHR (con soporte de proxy)
IE7	Flash	Flash (emulado y sin soporte de proxy)
	Flash	XHR (con soporte de proxy)
IE8	Flash	Flash (emulado y sin soporte de proxy)
	Flash	XHR (con soporte de proxy)
IE9	Flash	Flash (emulado y sin soporte de proxy)
	Flash	XHR (con soporte de proxy)
IE10	Completo	Completo
nativo de Android	Completo	XHR
Opera móvil	Completo	Completo en las versiones más recientes
Firefox móvil	Completo	Completo
Safari móvil	Completo	Completo en las versiones más recientes hasta iOS4, de lo

		contrario emulado a través de XHR

También vea: ¿Cuál es la diferencia entre websockets y XHR?

Si su navegador recarga automáticamente las páginas a la dirección HTTPS

Significa que el transporte de Websockets no es compatible. Este es el caso en varios navegadores móviles nativos de Android.

Se debe a que el navegador cambia automáticamente al transporte XHR.

Pero debido a que este transporte se realiza a largas distancias con el protocolo HTTP, cada solicitud crea una nueva conexión. Es muy lento e inestable crear nuevas conexiones (hasta 20 nuevas conexiones por segundo), por lo tanto, para evitar esta inestabilidad, el programa está concebido para que la página se recargue automáticamente a la dirección HTTPS para forzar la conexión HTTPS.

Físicamente, también obtienes una conexión segura mayormente persistente y mucho más estable en largas distancias. Así que la lógica del navegador reutiliza la conexión SSL ya establecida en lugar de crear una nueva conexión como lo hace el uso del protocolo HTTP.

Este comportamiento se puede cambiar mediante la siguiente opción en el archivo setting.js ubicado en la carpeta del programa TSplus bajo esta ruta: Clients\www\software\html5\settings.js:

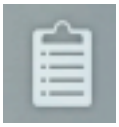
forcesslforxhr = false;

Pero no se recomienda en absoluto deshabilitar el uso de SSL en modo XHR.

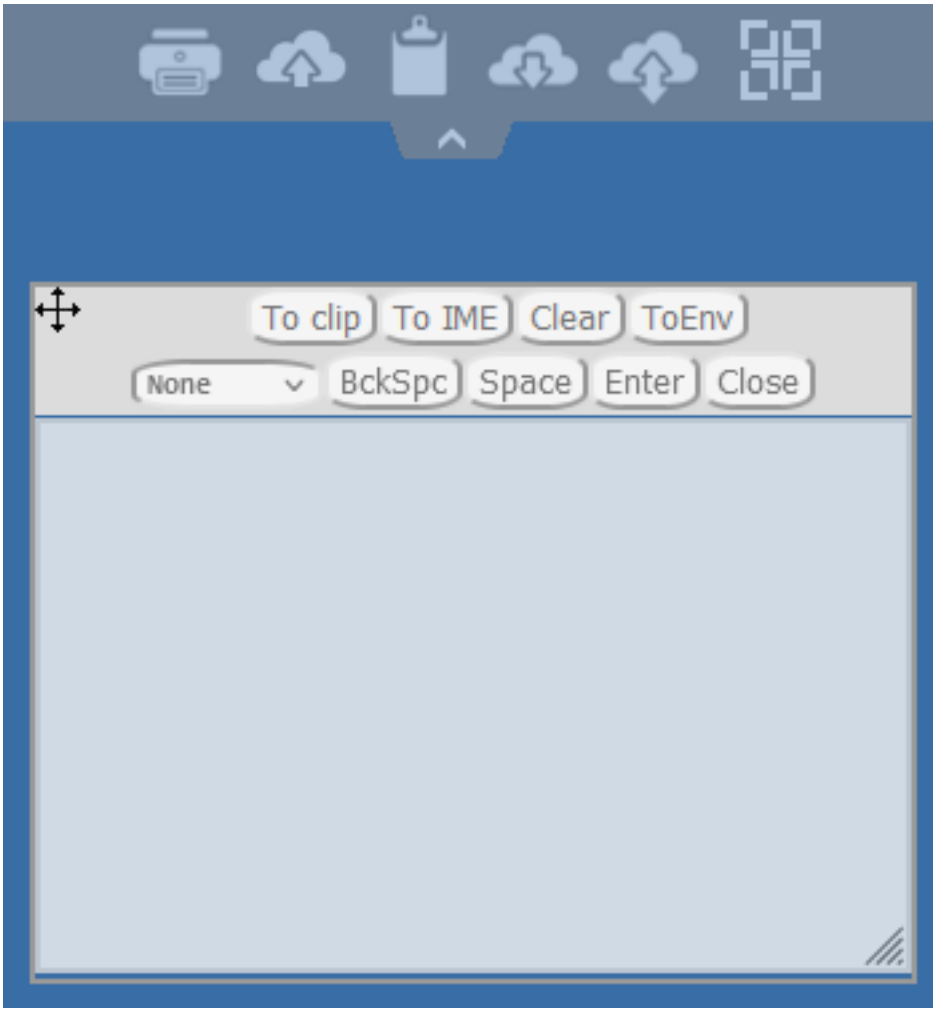
Si no tiene un archivo llamado “settings.js” en la carpeta “C:\Program Files (x86)\TSplus\Clients\www\software\html5”, entonces su versión de TSplus es más antigua y esta documentación no se aplica. Por favor, actualice su sistema primero o contacte con el soporte.

Cliente HTML5: Usando el portapapeles

El portapapeles se puede encontrar en el menú superior de HTML5, con este ícono:



La mayoría de los navegadores, excepto los navegadores MSIE más antiguos, no admiten la lectura y escritura directa del portapapeles debido a razones de seguridad.



Aquí están las diferentes acciones:

- **Para recortar** envía al RDP SESSION el contenido del ÁREA DE TEXTO y produce Ctrl+V al final para poner el texto DENTRO DEL RDP SESSION (¡tu PROPIO ENTORNO no se toca!)

- **Para IME** convierte caracteres de TEXT AREA a pulsaciones de teclas y las envía como si hubieras utilizado el teclado. (este botón es necesario cuando deseas colocar el texto donde la entrada de texto del portapapeles no es compatible dentro de la aplicación de sesión rdp)

- **Para el entorno** TRATA de poner texto del ÁREA DE TEXTO en tu PROPIO PORTAPAPELES fuera de tu navegador (no en la sesión RDP, sino en tu PROPIO ENTORNO!!!!) Debido a que agregar texto a tu propio portapapeles es una acción privilegiada, debe ejecutarse con un clic.

- **Para recortar** como se mencionó, maneja la colocación de texto en la acción rdp-clip+ctrl/v sin agregar texto fuera de su propio navegador debido a la seguridad, ya que sería bastante tonto poner texto dentro de su propio portapapeles cuando realmente no se desea hacerlo, así que úselo para "ToEnv", este comportamiento se mantendrá así y no se cambiará ya que se solicitó.

- **BckSpc** envía el comando del botón BACKSPACE a la sesión RDP (tu aplicación debe estar enfocada y soportar la acción del botón Backspace)

- **Espacio** envía a la sesión RDP el comando del botón Espacio (tu aplicación debe estar enfocada y soportar la acción del botón Espacio)

- **Entrar** envía el comando del botón Enter a la sesión RDP (tu aplicación debe estar enfocada y soportar la acción del botón Enter)

Para copiar el texto de la sesión al portapapeles, usa Ctrl+C y para insertar el texto del portapapeles, usa Ctrl+V.

Pero presta atención cuando copies el texto con Ctrl+C, espera un tiempo antes de soltar los botones Ctrl+C presionados, porque si el texto del portapapeles solicitado llega después de que sueltes esta combinación de teclas, el texto no se añadirá al portapapeles de tu entorno. De esta manera se utiliza un soporte nativo de copia del portapapeles del navegador iniciado por Ctrl+C.

Alternativamente puedes **usar el menú del portapapeles** copiar desde y para insertar el texto en el portapapeles de la sesión RDP.

Ahí puedes simplemente insertar el texto en el portapapeles de la sesión RDP o agregarlo al portapapeles e iniciar automáticamente Ctrl+C en el lado de la sesión RDP para insertar el texto. El menú del portapapeles se puede abrir a través del menú de acciones o Shift + F11.

- Cuando copias el portapapeles con el mouse dentro de una sesión RDP, el texto se envía al navegador y tan pronto como sales del enfoque del navegador, el menú del portapapeles aparece automáticamente para informarte que había un texto en el portapapeles y que no lo agregaste a tu entorno de portapapeles.

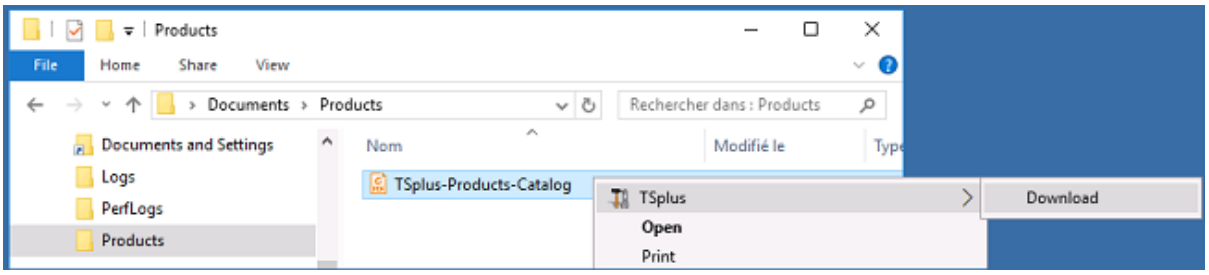
Para evitar este comportamiento, establezca la siguiente línea en la carpeta Clients, por defecto, la ruta es: C:\Program Files(x86)\tsplus\Clients\www\software\html5\settings.js :

openonclipblur = false;

Si no tiene un archivo llamado “settings.js” en la carpeta “C:\Program Files (x86)\TSplus\Clients\www\software\html5”, entonces su versión de TSplus es más antigua y esta documentación no se aplica. Por favor, actualice su sistema primero o contacte con el soporte.

Cliente HTML5: Usando Transferencia de Archivos

La transferencia de archivos se puede realizar de múltiples maneras en TSplus: desde la versión 12.50, **un menú contextual está disponible para descargar archivos del servidor al pc local** :



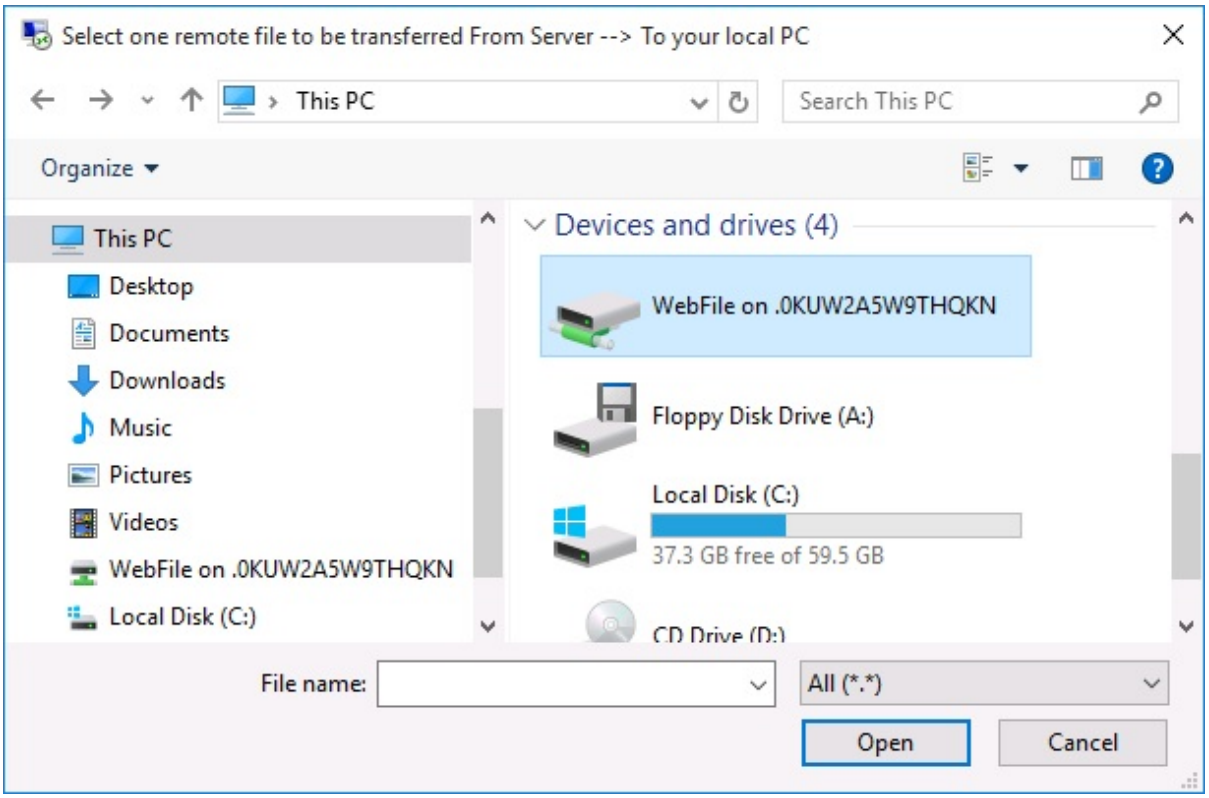
Más información se puede encontrar en esta documentación .

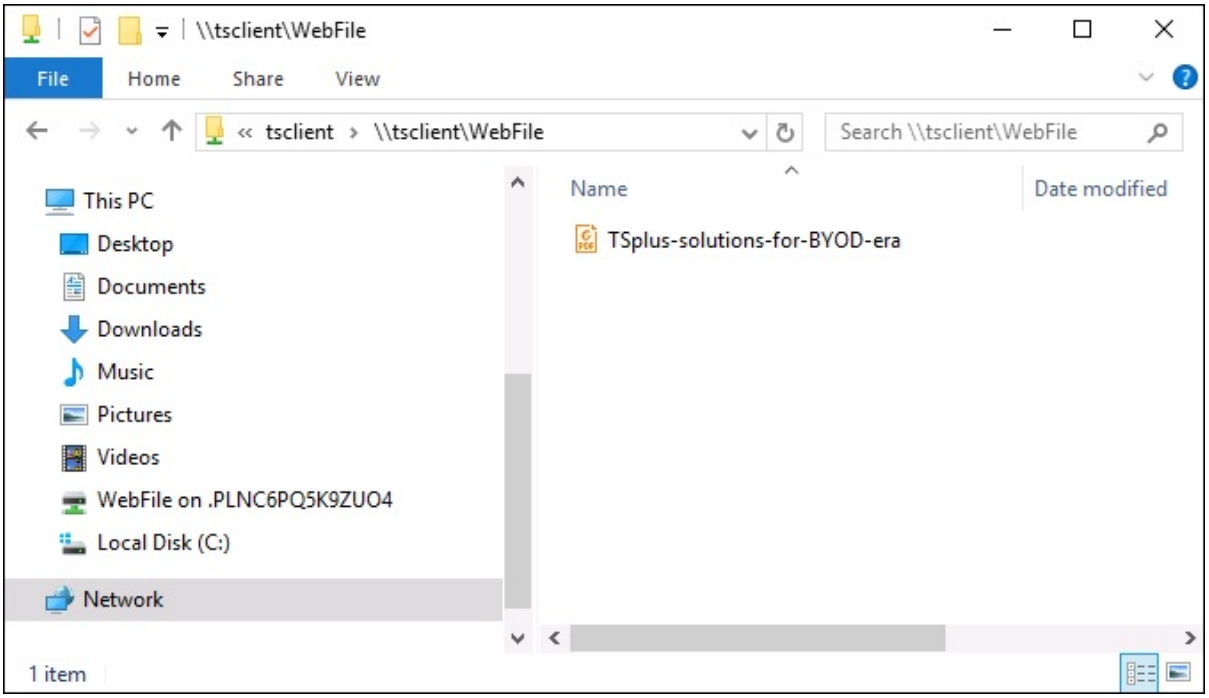
Usando el menú superior para la transferencia de archivos:



A diferencia de una sesión RDP real, los navegadores no permiten acceder directamente a los discos duros, la transferencia de archivos se emula.

La subcarpeta del gateway se monta como un dispositivo WebFile en tu sesión RDP. Dentro de la sesión RDP, puedes acceder a ella a través del Explorador haciendo clic en "WebFile" o llamando directamente a "\\tsclient\WebFile".

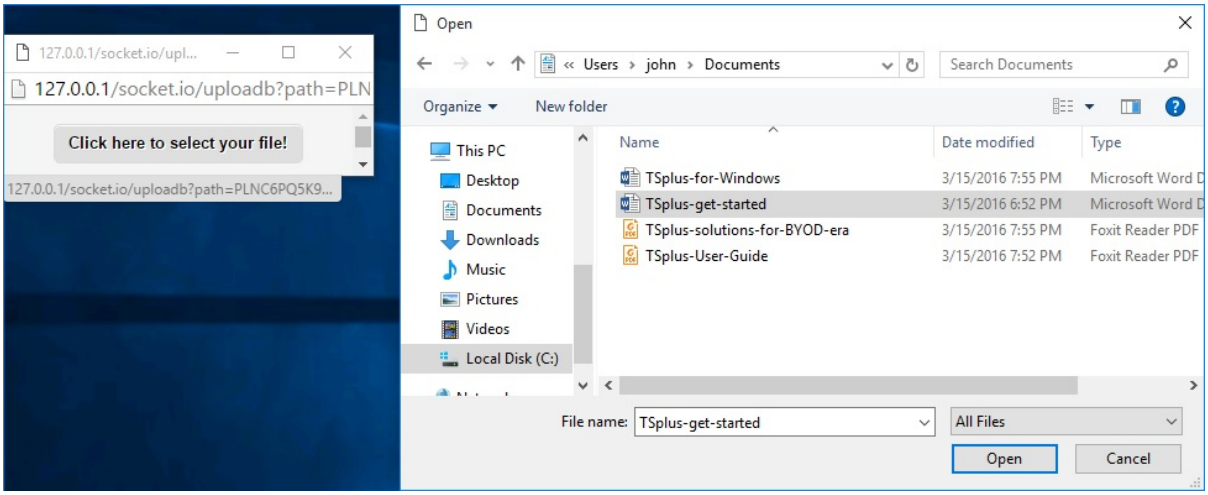




Hay 3 posibilidades diferentes para transferir un archivo:

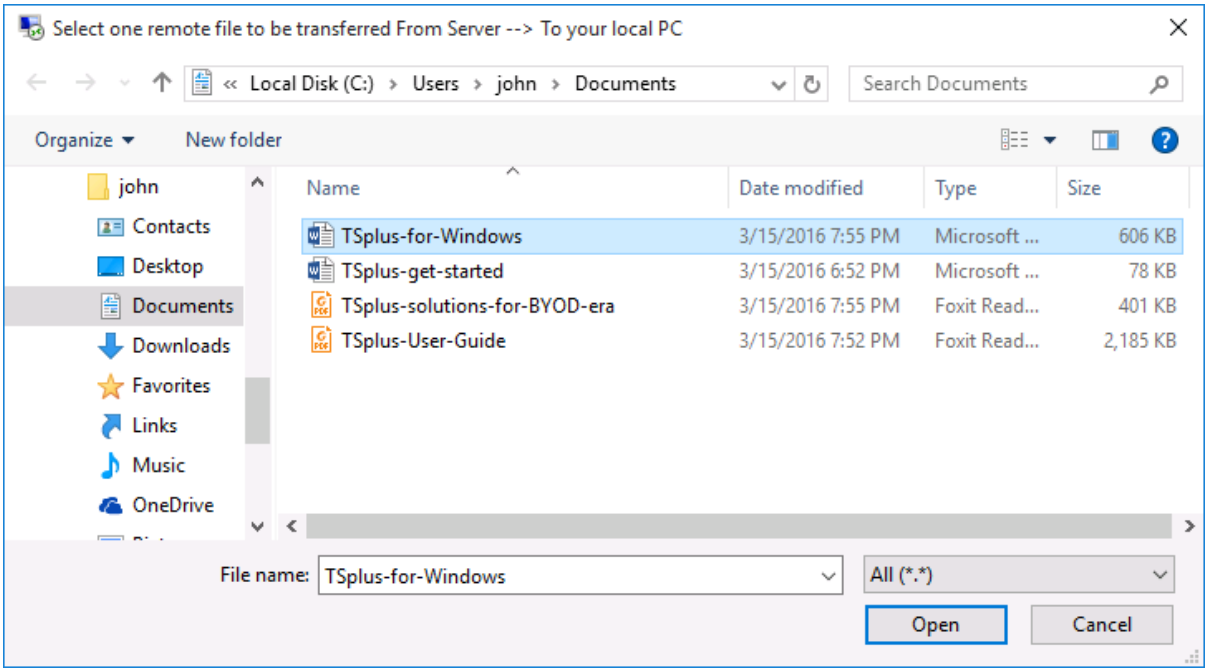
- Desde la computadora local hasta el servidor:



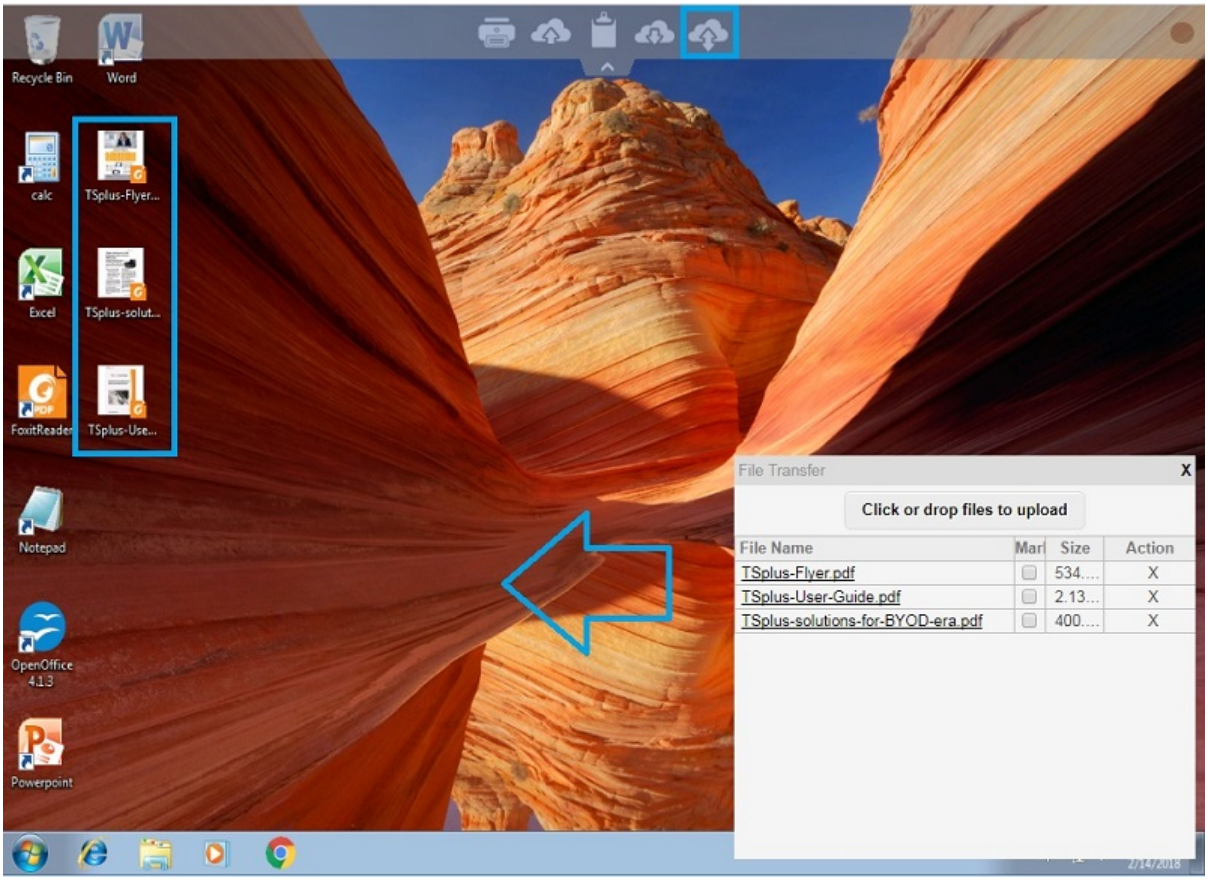


- Desde el servidor hasta la computadora local:



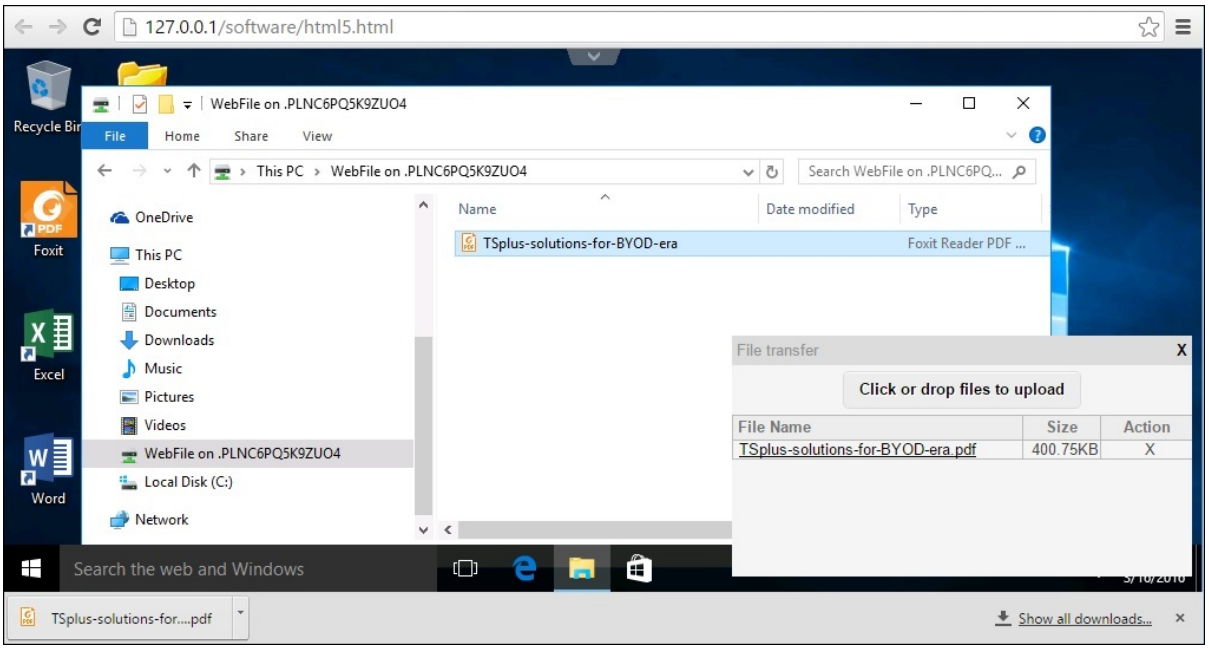


- El administrador de archivos que le permite transferir archivos desde el ordenador local al servidor, con un historial de los archivos transferidos:

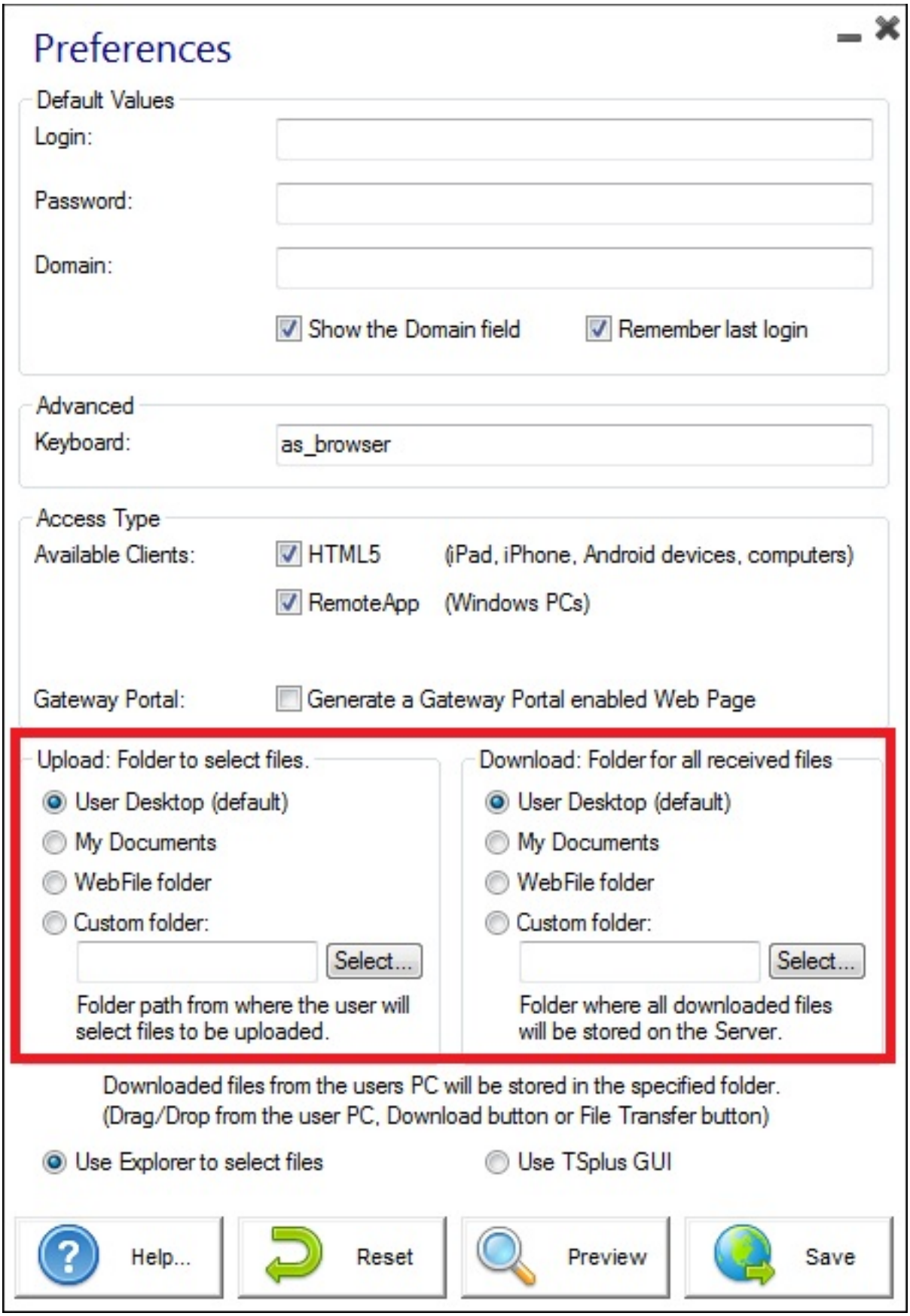


En el lado del navegador, los archivos se muestran dentro del menú de lista del navegador. Se pueden abrir a través del menú de acciones o con Shift + F12.

- Cuando copias archivos con el Explorador en la carpeta WebFile, esto activa automáticamente el evento sobre la creación de un nuevo archivo en la carpeta WebFile y el menú del navegador se abre/actualiza automáticamente para mostrar el nuevo archivo.



Al utilizar una carpeta personalizada, asegúrese de que esta carpeta exista en los lados del cliente y del servidor. Puede establecer la carpeta de destino de carga/descarga en el mosaico de preferencias del Portal Web en la pestaña web de la Herramienta de Administración.



Si deseas evitar este comportamiento, establece la siguiente línea en el archivo setting.js cuyo camino es por defecto: C:\Program Files (x86)\tsplus\Clients\www\software\html5\settings.js :

dropboxonnewfile = 0;

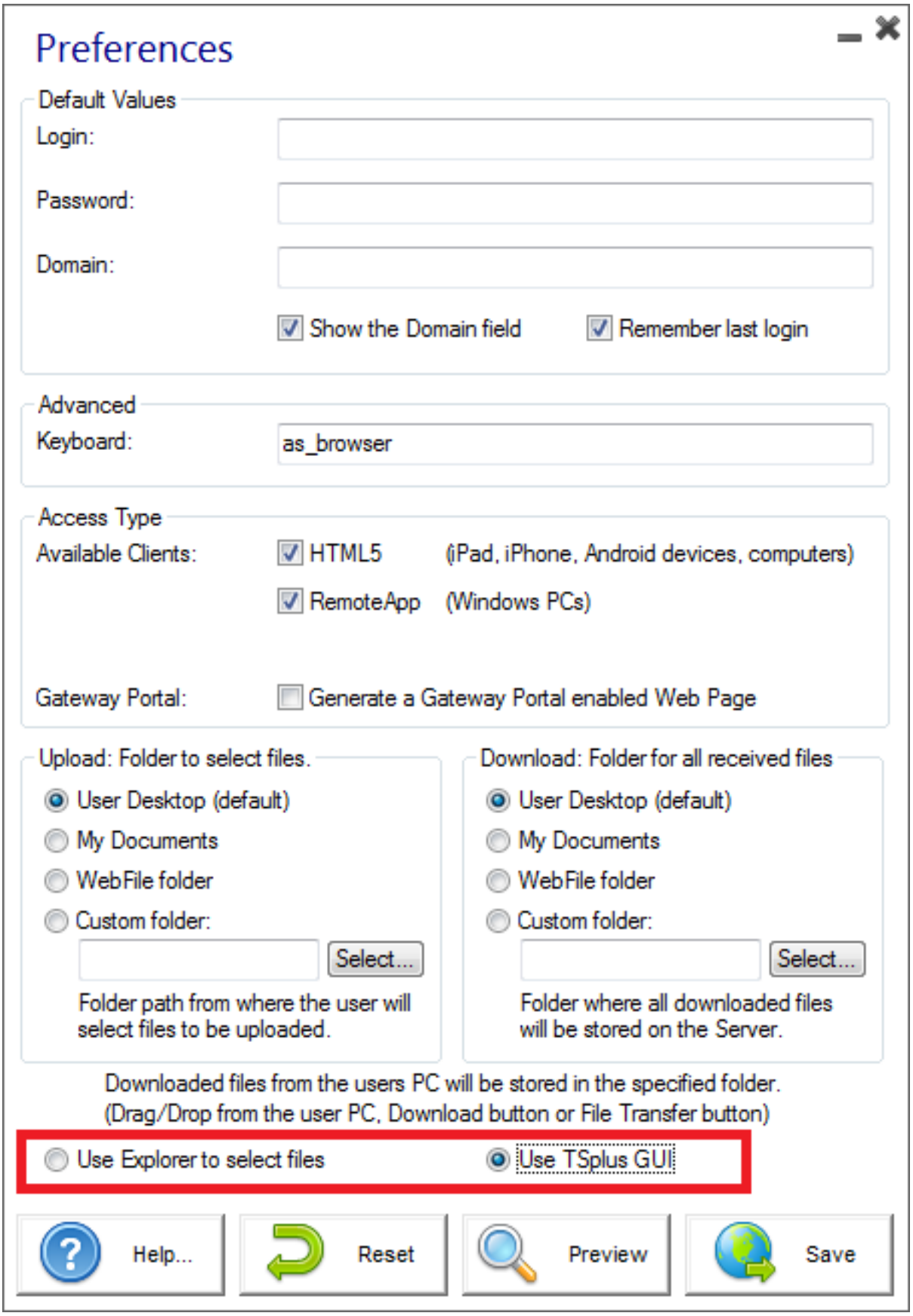
Además, puedes configurar:

sharedfolder = "sí";

para mostrar la carpeta compartida y compartir tus archivos con otros usuarios (deshabilitado por defecto).

Si no tiene un archivo llamado “settings.js” en la carpeta “C:\Program Files (x86)\TSplus\Clients\www\software\html5”, entonces su versión de TSplus es más antigua y esta documentación no se aplica. Por favor, actualice su sistema primero o contacte con el soporte.

- Por defecto, se utiliza el explorador para transferir archivos. También puedes descargar directamente tus archivos del servidor al cliente marcando "usar la interfaz gráfica de TSplus" y copiar cualquier archivo en la carpeta webfile:


Preferences
Default Values
Login:
Password:
Domain:
Show the Domain field
Remember last login
Advanced
Keyboard:
as_browser
Access Type
Available Clients:
HTML5
(iPad, iPhone, Android devices, computers)
RemoteApp
(Windows PCs)
Gateway Portal:
Generate a Gateway Portal enabled Web Page
Upload: Folder to select files.
User Desktop (default)
My Documents
WebFile folder
Custom folder:
Select...
Folder path from where the user will select files to be uploaded.
Download: Folder for all received files
User Desktop (default)
My Documents
WebFile folder
Custom folder:
Select...
Folder where all downloaded files will be stored on the Server.
Downloaded files from the users PC will be stored in the specified folder.
(Drag/Drop from the user PC, Download button or File Transfer button)
Use Explorer to select files
Use TSplus GUI
Help...
Reset
Preview
Save

Cliente HTML5: Usando gestos en dispositivos móviles (táctil)

Usando el área de la pantalla:

1. Toque fácil en la pantalla = movimiento del mouse a la posición tocada y clic izquierdo del mouse
2. Doble toque rápido en la pantalla = movimiento del mouse a la posición tocada y doble clic izquierdo del mouse
3. Toque y mantenga durante un segundo en la pantalla = movimiento del mouse a la posición tocada y clic derecho del mouse
4. Tocar y mover fuera del área del cursor = desplazamiento del marco de sesión visible (este es el comportamiento nativo de los navegadores para el desplazamiento, especialmente después de hacer zoom con pellizco)
5. Tocar en el área del cursor y mover = el cursor del mouse se mueve solo
6. Toque dos veces dentro del área del cursor y muévase = botón izquierdo del mouse presionado y movimiento del mouse. Útil para mover ventanas, mover elementos, redimensionar.
7. Toque dos veces en la pantalla (fuera del área del cursor) y mueve el dedo hacia abajo/arriba = desplazamiento del mouse medio. Útil para desplazarse por páginas o ver archivos pdf.
8. Pinch zoom con dos dedos = hacer zoom en el marco de la sesión RDP (este es el comportamiento nativo de los navegadores)

Usando el área del mouse pad - funciones adicionales en el punto medio del mouse pad:

1. Toque fácil en el medio = clic izquierdo del ratón
2. Doble toque en el medio = doble clic del ratón izquierdo
3. Tocar y mover en el medio = movimiento del mouse y movimiento del pad del mouse
4. Toque y mantenga durante un segundo = clic derecho

Modo de teclado activado:

1. Toque fácil en la pantalla = pérdida de enfoque, teclado deshabilitado (este es el comportamiento nativo de los navegadores) pero esto activará el movimiento del mouse y el clic izquierdo del mouse.
2. Doble toque rápido = movimiento del mouse y clic izquierdo del mouse (sin desactivar el teclado) Útil para reposicionar el cursor, establecer el enfoque en un carácter diferente y permanecer al mismo tiempo en modo teclado.

3. Funciones del mouse pad descritas arriba

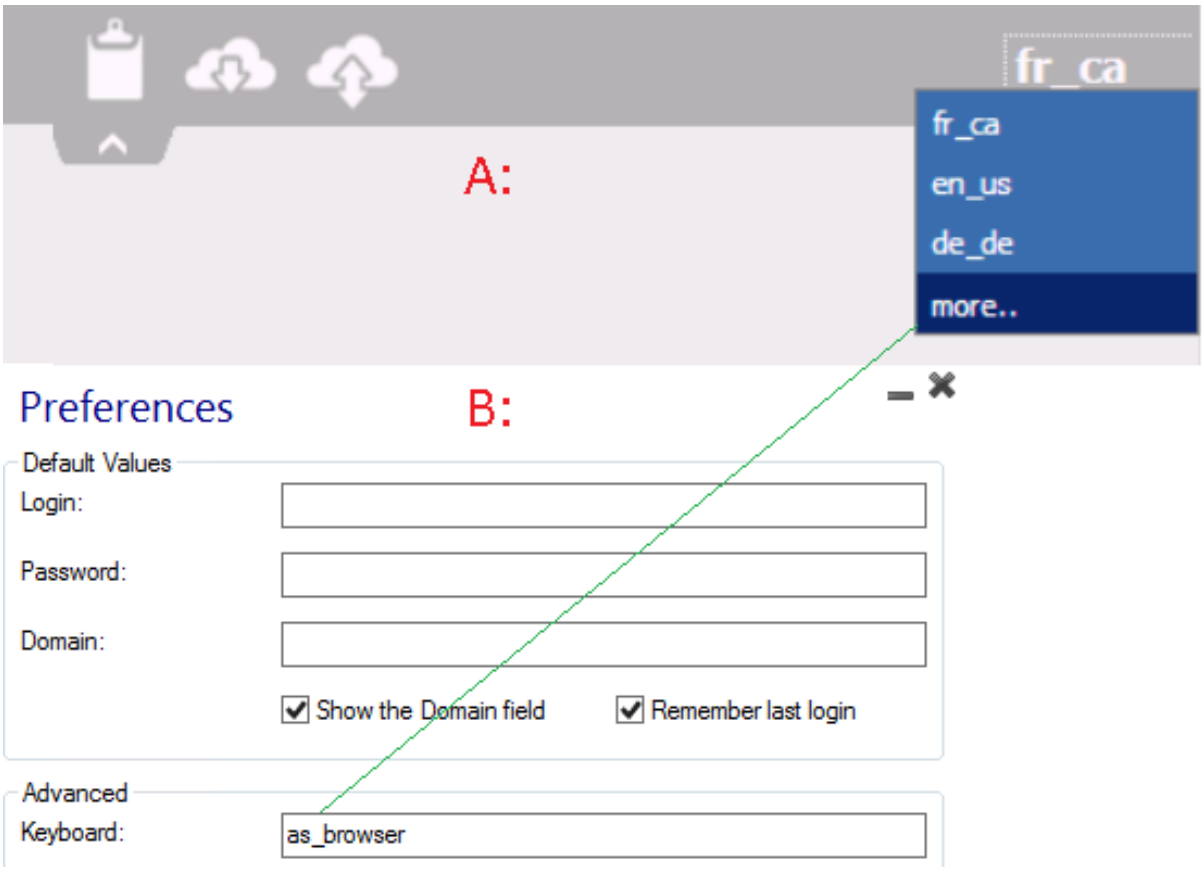
Cliente HTML5: Usando dos idiomas

Por defecto, el cliente HTML5 intenta reconocer el idioma predeterminado del navegador y luego usarlo dentro de la sesión RDP. Este comportamiento está controlado por la etiqueta "as_browser". Sin embargo, puede encontrar la lista completa de etiquetas de idioma disponibles en http:// tu_servidor /software/language.html bajo "Locale"

Tienes la opción de establecer un idioma fijo. **A:** por cliente directamente desde el menú superior de HTML5.

	Language	Locale	Value
○	Portal	as_portal	
○	Browser	as_browser	
○	Gateway	as_gateway	
○	Arabic	ar_ar	1025
○	Arabic (Algeria)	ar_dz	5121
○	Assamese	as_as	1101
○	Azeri (Cyrillic)	az_cy	2092
○	Azeri (Latin)	az_lt	1068
○	Belarusian	be_be	1059
○	Bulgarian	bg_bg	1026
○	Bengali	bn_bn	1093
○	Tibetan	bo_bo	1105
○	Bosnian (Cyrillic)	bs_cy	8218
○	Bosnian (Latin)	bs_lt	5146
○	Catalan	ca_ca	1027
○	Czech	cs_cs	1029
○		cs_cz	1029
○	Welsh	cy_gb	1106
○	Danish	da_da	1030
○		da_dk	1030
○	German (Swiss)	de_ch	2055
○	German	de_de	1031
○	Divehi	dv_dv	1125
○	Greek	el_el	1032
○		el_gr	1032
○	English (Canada)	en_ca	1105

B: o desde el portal configurándolo en la interfaz de AdminTool, lo que será efectivo para todos.



Deberías reiniciar la sesión si configuras otro idioma como principal.

Recuerda: al usar **cliente HTML5** en un escenario de múltiples idiomas, asegúrese de que el idioma utilizado dentro de la sesión Web-HTML5-RDP esté sincronizado con el idioma realmente configurado en su PC/Laptop/Mac, etc. De lo contrario, algunos caracteres que se representan y cruzan en cada mapa de idioma pueden producir caracteres incorrectos al enviar el código de escaneo actual para otro idioma. Esto también significa que, si cambió el idioma de inglés a alemán dentro de la sesión web, entonces cámbielo a alemán en su PC/Laptop/Mac también.

HTML5 Client: Cómo maximizar la ventana del navegador

Resumen

El protocolo RDP no permite cambiar el tamaño mientras está conectado sin una reconexión.

Tenga en cuenta que obtendrá la mejor experiencia posible del cliente HTML5 de Terminal Service Plus al conectarse con un navegador maximizado **.**

Sin embargo, si deseas forzar la ventana del navegador a ser lo más grande posible, puedes intentar “forzar” la ventana HTML5 a abrirse con el tamaño máximo (pero no como una ventana “maximizada”, debido a las limitaciones de seguridad de los navegadores de internet).

Maximizando la ventana del navegador

Deberá modificar el archivo “Clients\www\software\common.js” ubicado en su directorio de Terminal Service Plus. Le aconsejamos que utilice un editor de texto como Notepad++ (haga no usa Word).

Para tener una ventana del navegador que utilice toda la pantalla, tendrás que modificar la(s) línea(s) que contengan "window.open" y agregar el siguiente texto:

Ventana de terminal

"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(screen.availHeight-(55))

Esto permite que IE/Chrome/Firefox/Safari abra la ventana con un tamaño de pantalla (menos la barra de Windows). Desafortunadamente, no es posible forzar a un navegador web a "maximizar" la ventana en un tipo de Windows "pantalla completa".

Abre el archivo y busca “window.open(”

Luego agrega el nuevo al final antes de los corchetes, por ejemplo:

Ventana de terminal

```
window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);
```

se convertirá en:

Ventana de terminal

```
window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse,
"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(sc
reen.availHeight-(55)));
```

Y de nuevo:

Ventana de terminal

```
tmpwin = window.open(p, '_blank'); //Chrome needs _blank
```

se convertirá en:

Ventana de terminal

```
tmpwin = window.open(p, '_blank',
"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(sc
reen.availHeight-(55))); //Chrome needs _blank
```

Y de nuevo:

Ventana de terminal

```
success = window.open(p, k);
```

se convertirá en:

Ventana de terminal

```
success = window.open(p, k,
"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(sc
reen.availHeight-(55)));
```

Y finalmente :

Ventana de terminal

```
cpwin = window.open("about:blank", n);
```

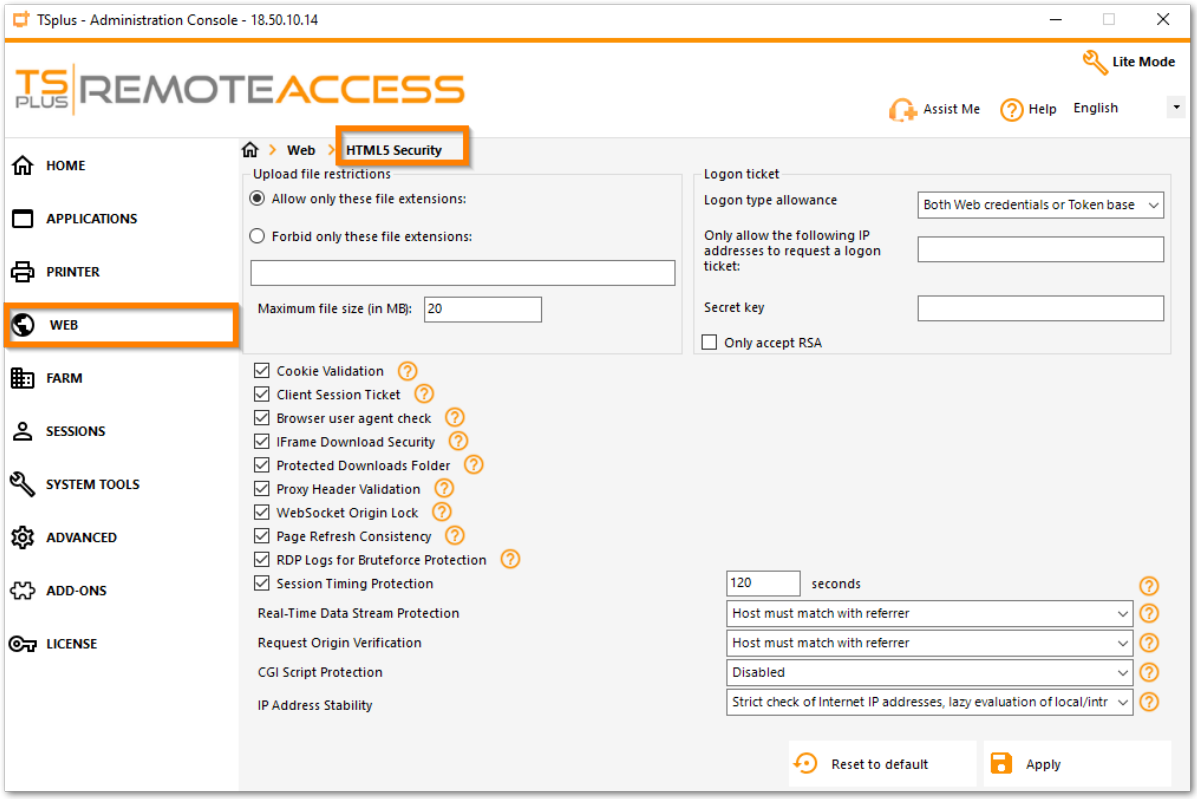
se convertirá en:

Ventana de terminal

```
cpwin = window.open("about:blank", n,
"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(sc
reen.availHeight-(55)));
```

Seguridad HTML5

En la pestaña de Seguridad HTML5, puedes gestionar la configuración web.



Si necesita seguridad adicional, puede ver y descargar nuestro Advanced Security .

Uso de memoria del servidor HTML5

El servidor HTML5 de Terminal Service Plus se ejecuta en JAVA. Comprender cómo JAVA maneja la memoria ayuda a entender el uso de memoria del servidor HTML5 de Terminal Service Plus.

Memoria asignada

Cuando Java se ejecuta, intenta asignar el 25% de la memoria física del ordenador. Esta memoria está "asignada" pero no se utiliza directamente; no es el uso real de la memoria que se puede ver en el Administrador de tareas de Windows.

plataforma JAVA: 32 bits vs 64 bits

Hay una gran diferencia entre estas dos plataformas:

- JAVA de 32 bits no puede manejar más de 4 GB de RAM por definición. Dado que asignará el 25% de toda la memoria disponible, asignará como máximo 1 GB, asumiendo que hay 4 GB de memoria física. Si solo hay 2 GB de memoria física, solo asignará 500 MB, etc.
- JAVA de 64 bits puede manejar mucho más de 4 GB (teóricamente hasta 16 exa bytes), por lo que la memoria asignada dependerá únicamente de la memoria física.

Gestión de memoria JAVA

JAVA es una "máquina virtual". Esto significa que JAVA gestiona la memoria por su cuenta. Una vez que JAVA asigna memoria, incluso cuando ya no la necesita, no la devolverá automáticamente al sistema. Esto es por razones de rendimiento, ya que la asignación y desasignación de memoria son tareas intensivas para la CPU.

JAVA generalmente esperará hasta que tenga un gran bloque de memoria no utilizada antes de devolverlo al sistema. El tamaño de este gran bloque depende directamente del tamaño de la memoria física del ordenador. Cuanta más memoria física tenga un ordenador, más memoria será asignada por JAVA.

Uso de memoria del servidor HTML5 de Terminal Service

Plus

Todos estos detalles técnicos son la razón por la cual uno puede abrir el Administrador de tareas de Windows y pensar que Terminal Service Plus HTML5 Server utiliza mucha memoria, o que JAVA de 32 bits utiliza menos memoria que JAVA de 64 bits.

En realidad, la memoria realmente utilizada por el servidor HTML5 de Terminal Service Plus está directamente relacionada con el número de sesiones HTML5 abiertas. Cuanta más memoria disponible haya en la computadora, más sesiones HTML5 podrás abrir.

Uso de memoria de sesión HTML5

La memoria utilizada por una sesión HTML5 depende de las actividades del usuario (aplicaciones y programas utilizados, Word/Excel frente a programas intensivos en gráficos) y del método de conectividad establecido entre el servidor HTML5 de Terminal Service Plus y la computadora cliente.

En el caso de uso general, una sesión HTML5 utilizará 30 MB de memoria (uso estándar, conectividad de websockets binarios). En el peor de los casos, una sesión utilizará hasta 100 MB de memoria (uso intensivo, conectividad de "XHR" de respaldo para navegadores más antiguos).

Pérdida de la escucha del servidor HTTP y HTTPS

Cada registro de error de Java indica suficiente memoria nativa para la operación.

El problema es en realidad bastante simple.
Cuando comienza la sesión HTML5, hay suficiente memoria según los valores reportados.
Luego, dentro de la sesión RDP, inicia un programa desconocido y roba toda la memoria nativa para sí mismo.

Cuando Java lo solicita de nuevo, de repente ya no está disponible, causando este error de memoria insuficiente.

- No hay suficiente memoria para que el entorno de ejecución de Java continúe.
- La asignación de memoria nativa (mmap) no pudo mapear 234881024 bytes. Detalles del error: espacio virtual G1# Posibles razones:
- El sistema se ha quedado sin RAM física o espacio de intercambio# Este proceso se está ejecutando con Compressed Oops habilitado, y el montón de Java puede estar bloqueando el crecimiento del montón nativo.

Posibles soluciones:

- Reduce la carga de memoria en el sistema

- Aumentar la memoria física o el espacio de intercambio# Verificar si el almacenamiento de soporte de intercambio está lleno
- Disminuir el tamaño del heap de Java (-Xmx/-Xms)
- Disminuir el número de hilos de Java # Disminuir el tamaño de la pila de hilos de Java (-Xss)
- Establecer un caché de código más grande con -XX:ReservedCodeCacheSize=

La JVM se está ejecutando en modo Zero Based Compressed Oops, en el cual el montón de Java se coloca en el primer espacio de direcciones de 32 GB. La dirección base del montón de Java es el límite máximo para el crecimiento del montón nativo.
Por favor, use **-XX:HeapBaseMinAddress**

Potencialmente, podrías asignar más memoria nativa a Java desde el principio y obligarlo a dejar de devolver memoria al sistema, asignándola así a sí mismo.
Sin embargo, en este caso, te encontrarás con el siguiente problema: los programas que se ejecutan en una sesión RDP pueden quedarse sin memoria, y todo el sistema podría fallar.

Pero aún puedes intentarlo.

1. Abre y edita el siguiente archivo con el Bloc de notas: *\Clients\webserver\runwebserver.ini

2. Allí, encontrará la siguiente configuración de línea de comandos, así:

Ventana de terminal

-Djdk.tls.ephemeralDHKeySize=matched -Djdk.tls.rejectClientInitiatedRenegotiation=true -Dorg.jboss.netty.epollBugWorkaround=true -XX:+UseG1GC -XX:MinHeapFreeRatio=10 -XX:MaxHeapFreeRatio=10 **********
and so on

3. Elimina toda la línea de runwebserver.ini y añade lo siguiente en su lugar:

Ventana de terminal

```
-server -javaagent:"%~dp0httpwebs.jar" -Djdk.tls.ephemeralDHKeySize=matched -
Djdk.tls.rejectClientInitiatedRenegotiation=true -Dorg.jboss.netty.epollBugContourn=true --add-
opens java.prefs/java.util.prefs=ALL-UNNAMED --add-opens java.base/java.lang.reflect=ALL-
UNNAMED --add-opens java.base/sun.security.ssl=ALL-UNNAMED --add-opens java.base/
java.nio=ALL-UNNAMED --add-opens java.base/jdk.internal.ref=ALL-UNNAMED --add-exports
java.prefs/java.util.prefs=ALL-UNNAMED ---add-exports java.base/java.lang.reflect=ALL-
UNNAMED --add-exports java.base/sun.security.ssl=ALL-UNNAMED --add-exports java.base/
jdk.internal.ref=ALL-UNNAMED --add-exports java.base/java.nio=ALL-UNNAMED
```

4. Reinicie el servidor HTML5 a través de la interfaz gráfica de AdminTool para aplicar los cambios.
   Pero antes de hacerlo, asegúrate de que el archivo web server\runwebserver.bat no tenga un atributo de solo lectura establecido en sus propiedades. De lo contrario, la interfaz gráfica de AdminTool no podrá adaptar runwebserver.bat después de un reinicio.

En la mayoría de los casos, esto debería ser suficiente. Una vez que Java utiliza memoria, la asignará a otros usos en lugar de devolverla al sistema. Por lo tanto, el uso de memoria de html5service.exe podría alcanzar potencialmente el 70% de la memoria disponible del sistema. En este caso, Java debería dejar de fallar. Sin embargo, si otro programa está consumiendo una gran cantidad de memoria, podría fallar en su lugar. En ese caso, somos impotentes; debes asegurarte de que haya suficiente memoria para ejecutar un servidor HTML de Java, así como otros programas.

Hay una opción en Java llamada -XX:+AggressiveHeap que podría mejorar la asignación de memoria para la Máquina Virtual de Java, y por lo tanto el contenido final de *\webserver\runwebserver.ini.

Podría verse algo así:

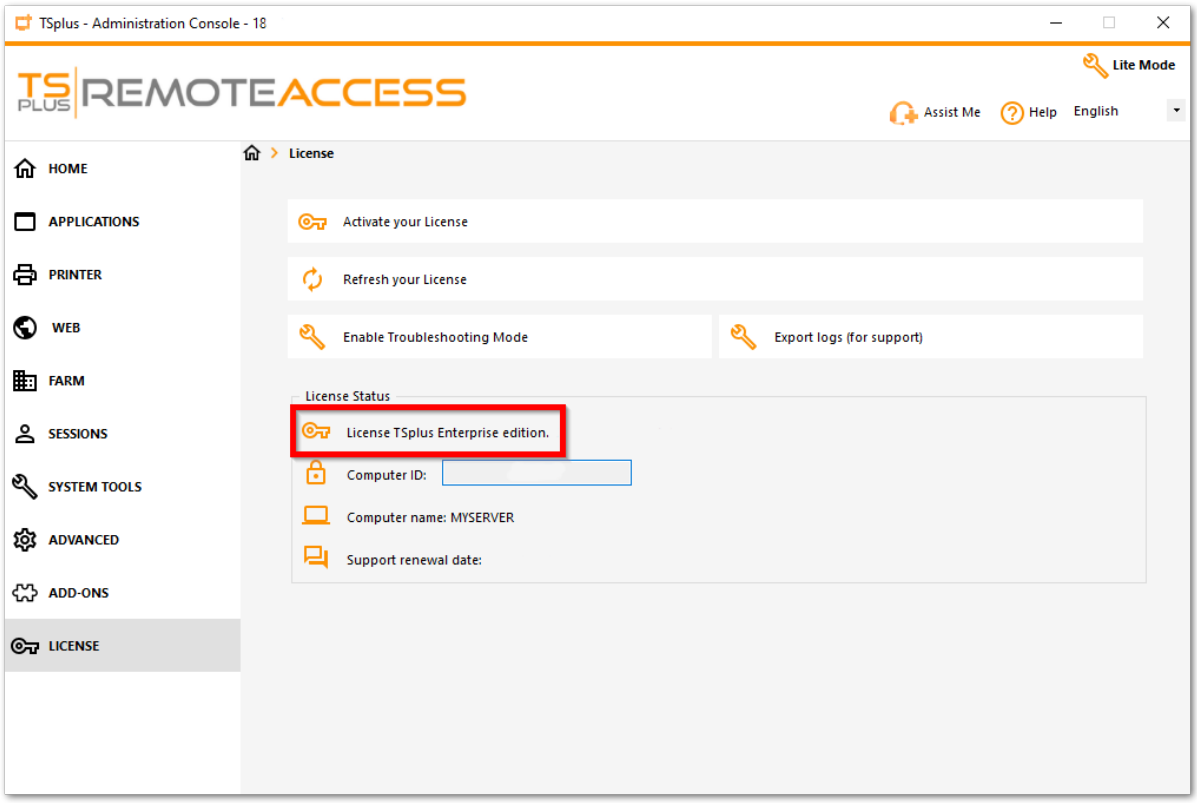
Ventana de terminal

```
-XX:+AggressiveHeap -server -javaagent:"%~dp0httpwebs.jar" -
Djdk.tls.ephemeralDHKeySize=matched -Djdk.tls.rejectClientInitiatedRenegotiation=true -
```

Dorg.jboss.netty.epollBugWorkaround=true --add-opens java.prefs/java.util.prefs=ALL-UNNAMED --add-opens java.base/java.lang.reflect=ALL-UNNAMED --add-opens java.base/sun.security.ssl=ALL-UNNAMED --add-opens java.base/java.nio=ALL-UNNAMED --add-opens java.base/jdk.internal.ref=ALL-UNNAMED --add-exports java.prefs/ java.util.prefs=ALL-UNNAMED --add-exports java.base/java.lang.reflect=ALL-UNNAMED --add

Cómo identificar su Edición de TSplus

En la ficha de licencia bajo el número de serie, puedes ver el tipo de licencia que compraste, así como tu número de usuarios junto al número de conexiones.



TSplus ha fusionado licencias antiguas en una sola para obtener más claridad. Las ediciones de Sistema e Impresora se han migrado a **Desktop Edition** .

Desktop Edition

Características básicas:

- TSplus Administrator Tool (AdminTool),

- Soporte de conexiones concurrentes,
- Control de aplicaciones por usuario y/o por grupos,
- TSplus Remote Taskbar y/o TSplus Floating Panel,
- Acceso a Escritorio Remoto,
- TSplus Portable Client Generator,
- Cliente de conexión RemoteApp,
- Totalmente compatible con el protocolo RDP,
- Soporte de pantalla dual, sonido bidireccional, RemoteFX cuando sea compatible con la versión de Windows,
- Soporte de conexión local y remota,
- Soporte para usuarios de Workgroup y Active Directory,
- Redirección de dispositivo/disco.
- Virtual Printer, le permite imprimir desde cualquier ubicación, sin tener que instalar ningún controlador específico y permite la redirección de impresoras.

Edición Web Móvil

Permite que usted (además de todas las características de las ediciones de Sistema y Impresora) pueda:

-

Conéctese desde cualquier navegador web con TSplus HTTP Web Server,

- Conexión completamente segura desde cualquier navegador web con TSplus HTTPS Web Server y servidor SSH,
- Páginas HTML incluyen clientes de acceso web de Windows y HTML5,
- Conéctese fácilmente desde dispositivos iPhone/iPad y Android, también con el TSplus Mobile App ,
- Personaliza la página de inicio de sesión web con el kit de herramientas de Webmaster fácil de usar de TSplus,
- Con TSplus Web Applications Portal, los usuarios pueden acceder a su lista de aplicaciones dentro de su navegador web,
- En lugar de las credenciales de Windows, las credenciales web de TSplus permiten a los usuarios conectarse solo con un correo electrónico o un código PIN,
- Universal Printer te permite imprimir desde cualquier ubicación, sin necesidad de instalar ningún controlador de impresora específico,

Enterprise Edition

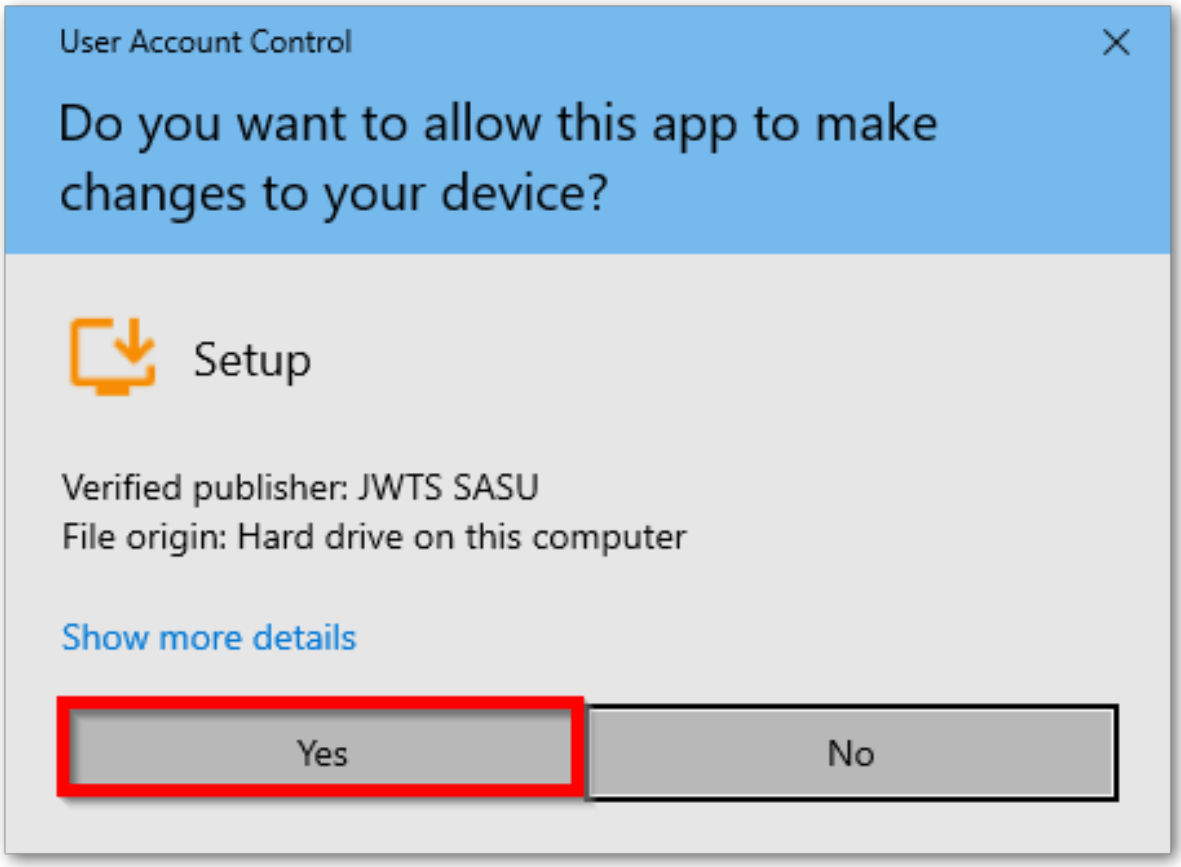
Incluye todas las características anteriores más estas:

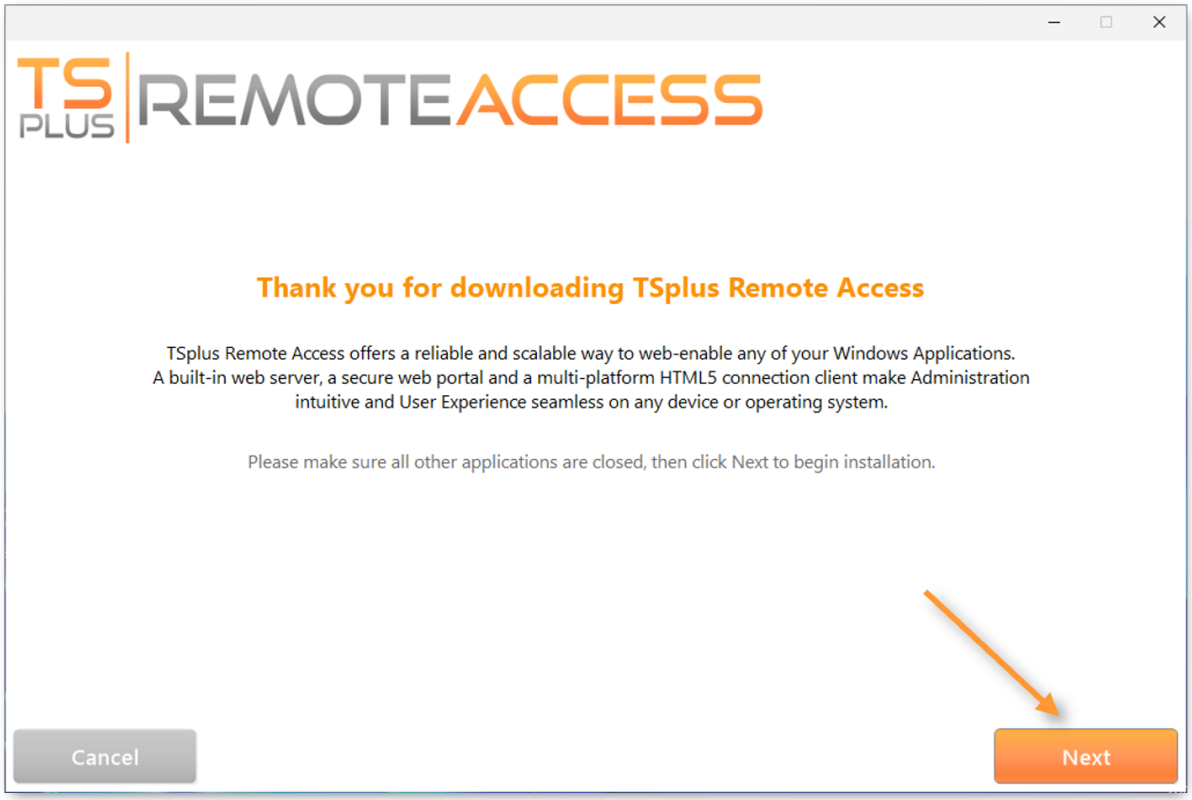
- Soporte a un número ilimitado de servidores dentro de cada granja de TSplus (se requiere una licencia por servidor),
- Miles de usuarios trabajando simultáneamente en una arquitectura escalable con balanceo de carga,
- Portal único de empresa para acceder a todos tus servidores TSplus,

- Capacidad para asignar uno o varios Servidores de Aplicaciones a usuarios o grupos de usuarios,
- Soporte de balanceo de carga y conmutación por error incluido.
- La posibilidad de agregar una capa adicional de seguridad con el TSplus 2FA Add-On .

TSplus Remote Access v19 Instalación

Ejecutar TSplus Remote Access Setup program y luego **siga los pasos de instalación** .
Se requiere la contraseña de administrador local después del primer reinicio de TSplus Remote Access.





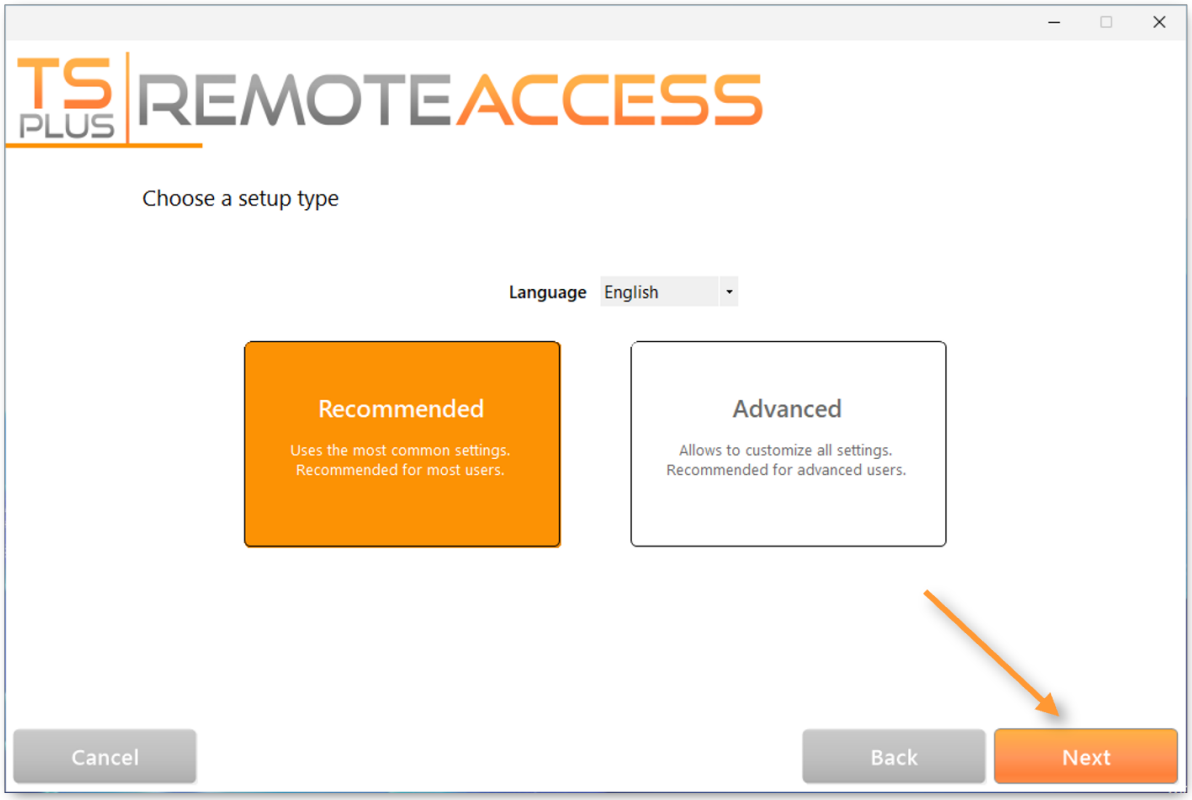
Puedes seleccionar tu idioma (posible cambiarlo más tarde)

Puede seleccionar luego dos opciones personalizadas marcando las casillas correspondientes: **Recomendado** o **Avanzado**

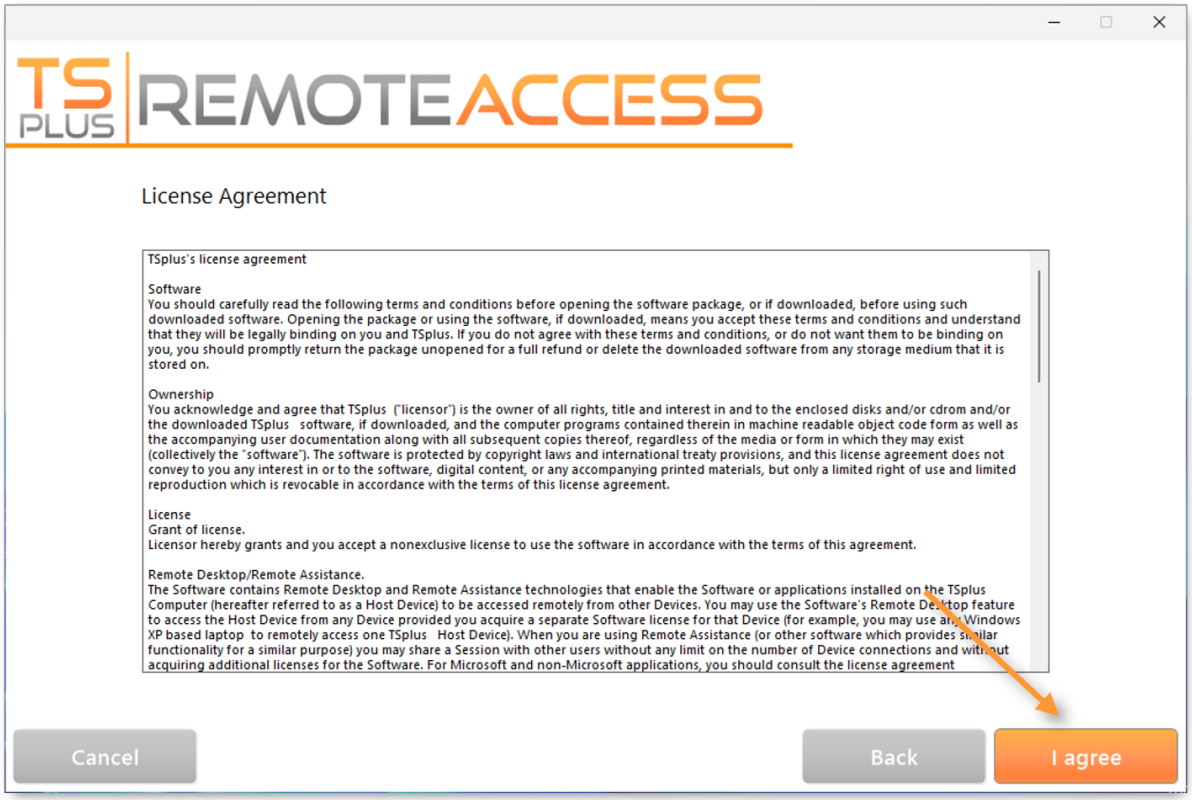
La opción Avanzada le permite:

- No instalar TSplus Advanced Security.
- Utilice configuraciones de proxy personalizadas.
- Descargue solo el instalador, que no instala TSplus.
- Cambiar puertos predeterminados (no recomendado).

Haga clic en Siguiente.



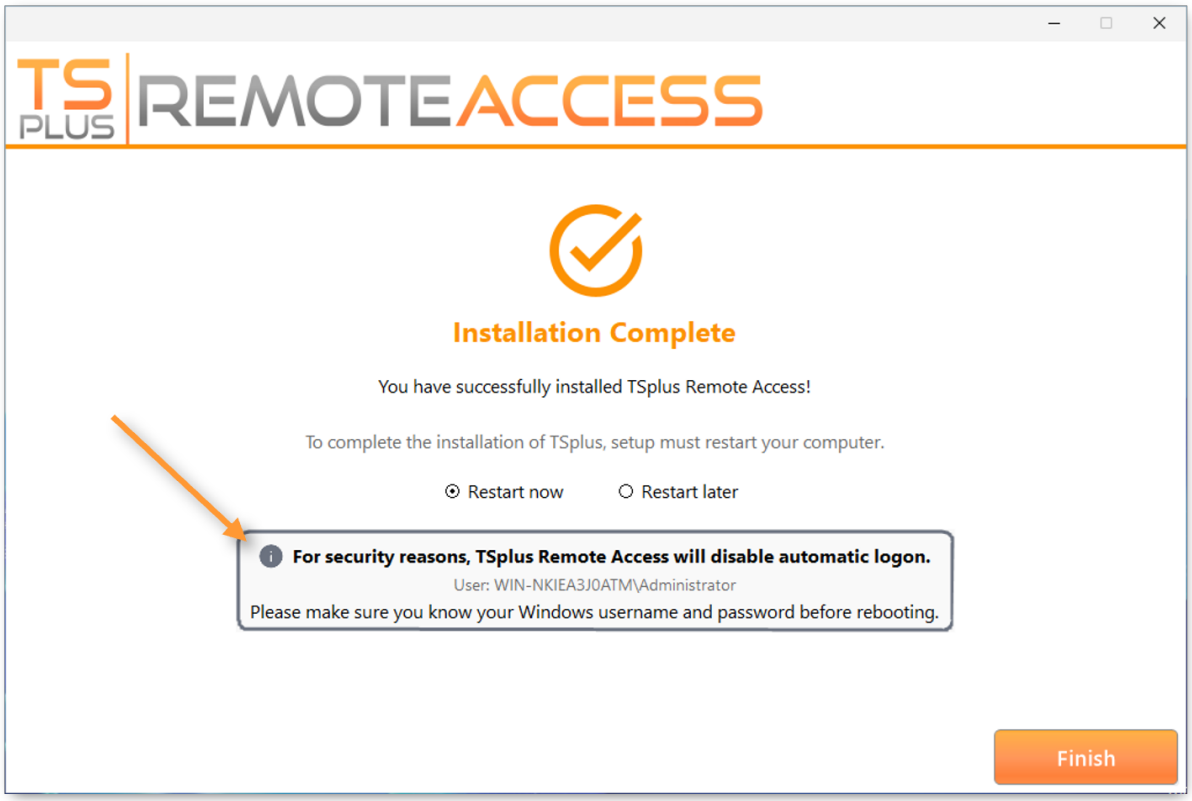
Haga clic en Acepto el acuerdo.



Por favor, espere, descargando e instalando el programa



Luego, aparece el logo de TSplus y una ventana te informa sobre la finalización de la instalación.

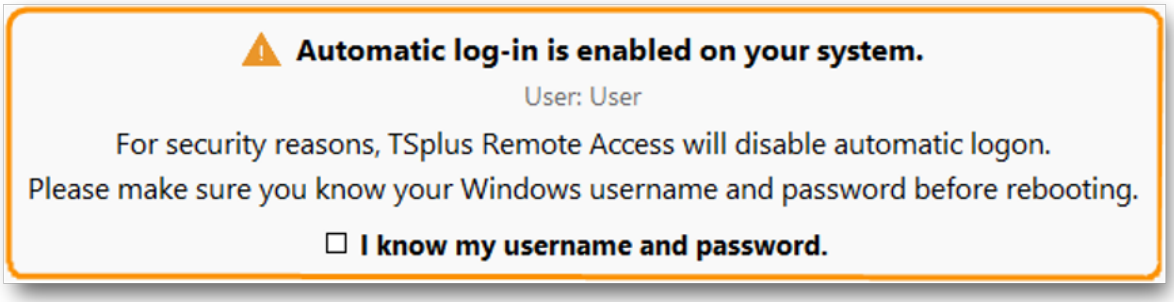


☐ **Aviso Importante**

Por razones de seguridad, **TSPlus Remote Access** requerirá que ingreses manualmente tu nombre de usuario y contraseña en cada inicio de sesión.

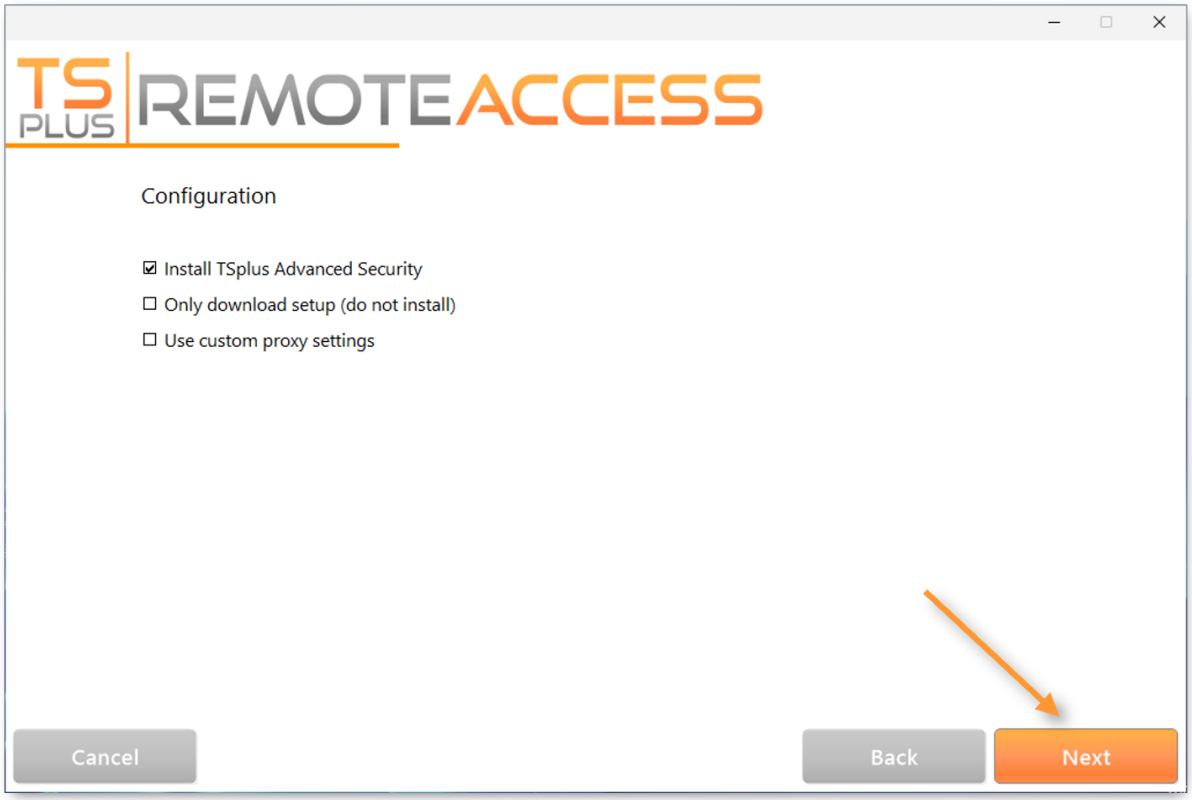
Asegúrate de conocer tus credenciales antes de reiniciar el sistema para evitar quedarte fuera.

Si
autologon
está habilitado en el sistema, el instalador mostrará un mensaje de advertencia pidiéndole que confirme que conoce su nombre de usuario y contraseña.



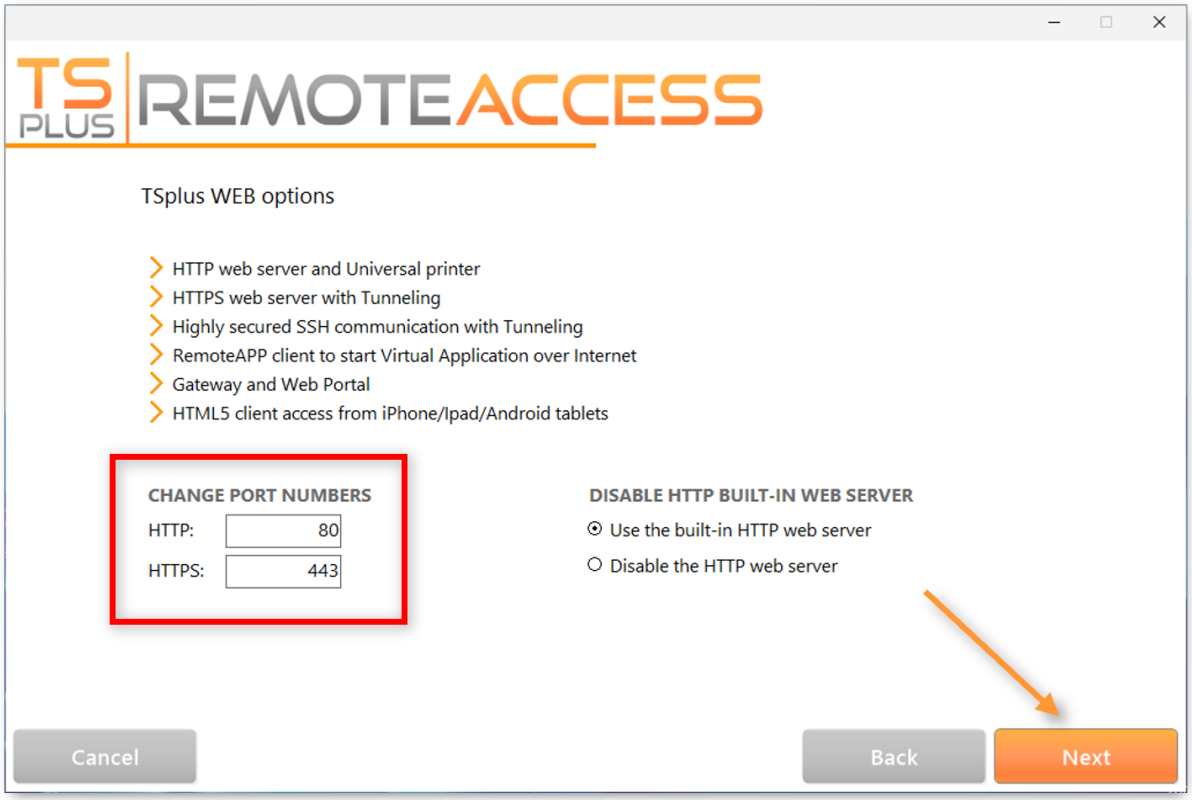
Para usar TSplus, debes reiniciar tu sistema. El período de prueba ofrece un producto completo durante 15 días y 5 usuarios concurrentes.

Los pasos a continuación solo si selecciona instalar TSplus Remote Access en **Modo avanzado** .

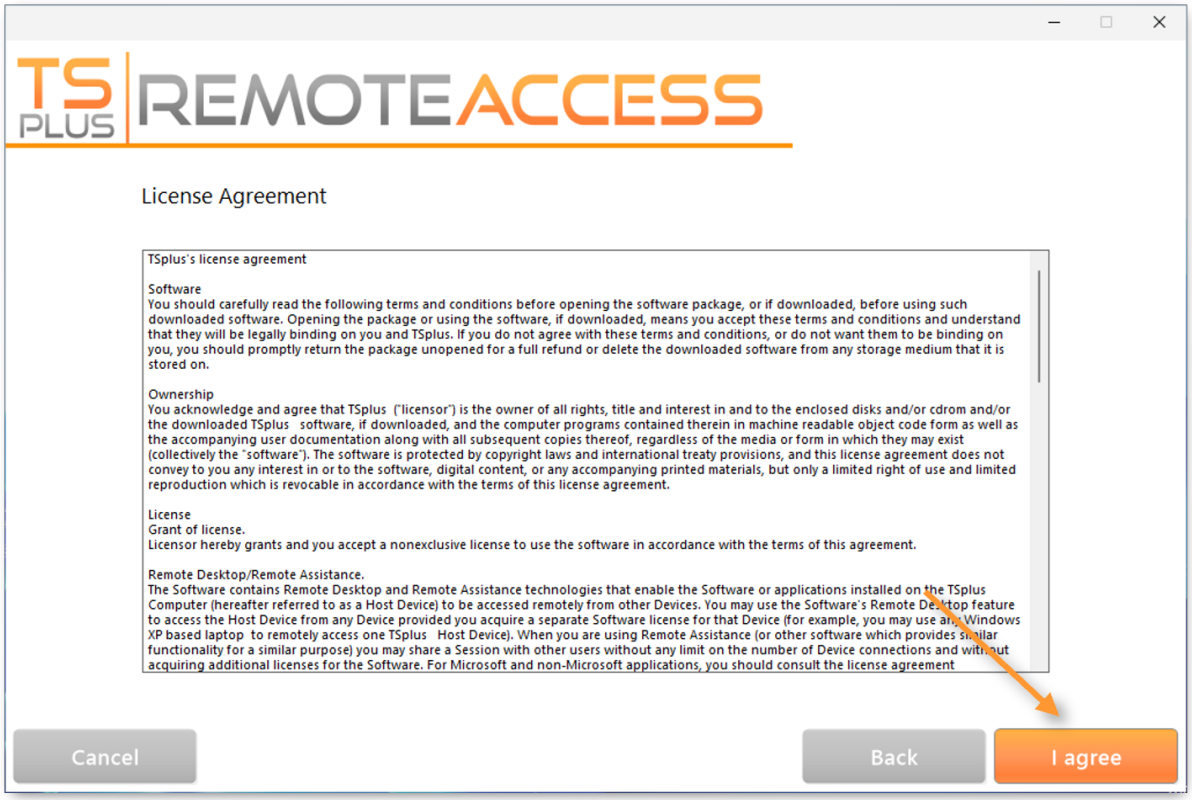


Los servidores web están escuchando en los puertos 80 y 443 por defecto. Recomendamos que acepte nuestra configuración de instalación predeterminada de TSplus. Según nuestra experiencia, la mayoría de los problemas de producción se deben a las características de seguridad de Windows.

Puedes seguir modificando estos puertos si lo deseas durante la instalación o en cualquier momento en el Gestión del servidor web incorporado de AdminTool Asegúrate de que los puertos definidos estén disponibles y que Java esté instalado en el servidor.



Haga clic en Acepto el acuerdo.



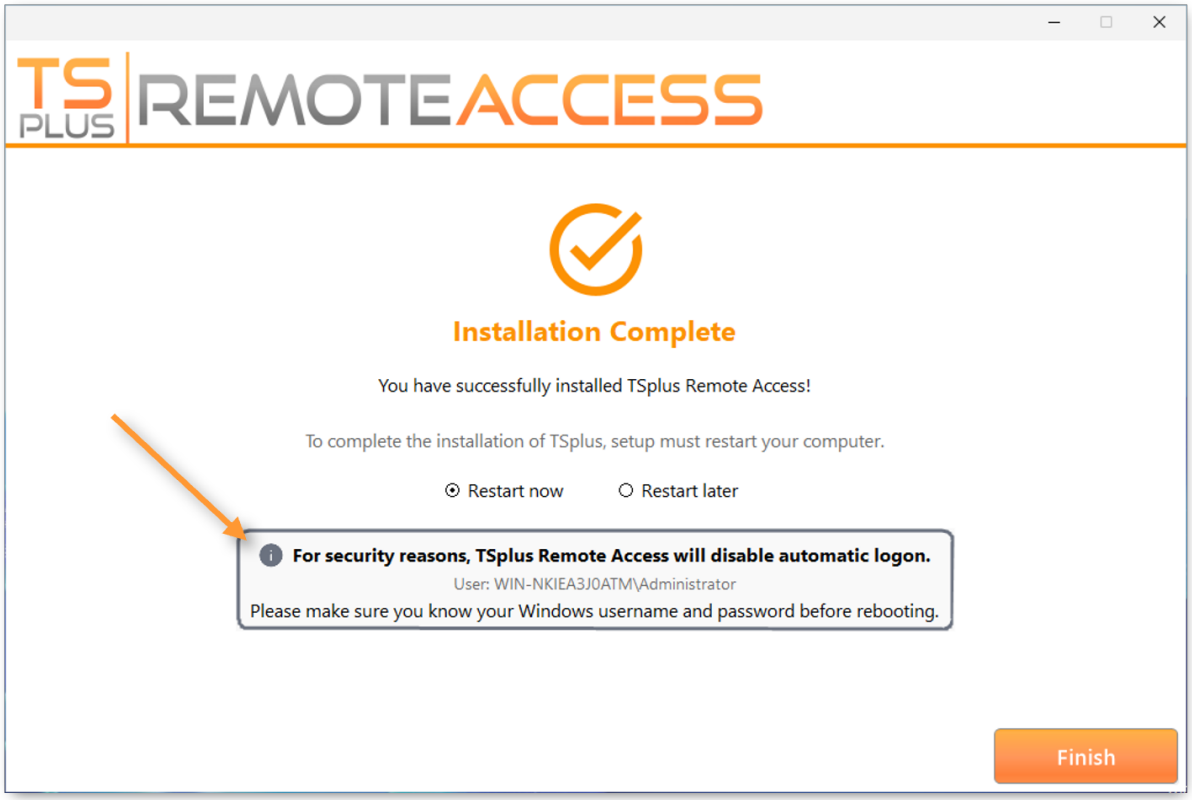
La barra de progreso aparece y te permite seguir el avance del proceso:



- Desde la versión 11.40 de TSplus, tendrás la opción de instalar TSplus Advanced Security nuestra poderosa Adición de Seguridad, en su versión de prueba Ultimate (todas las funciones de seguridad gratis para usar durante 2 semanas) a su sistema TSplus:

Para más información sobre este producto, consulte las páginas sobre TSplus Advanced Security. documentación .

Luego, aparece el logo de TSplus y una ventana te informa sobre la finalización de la instalación.

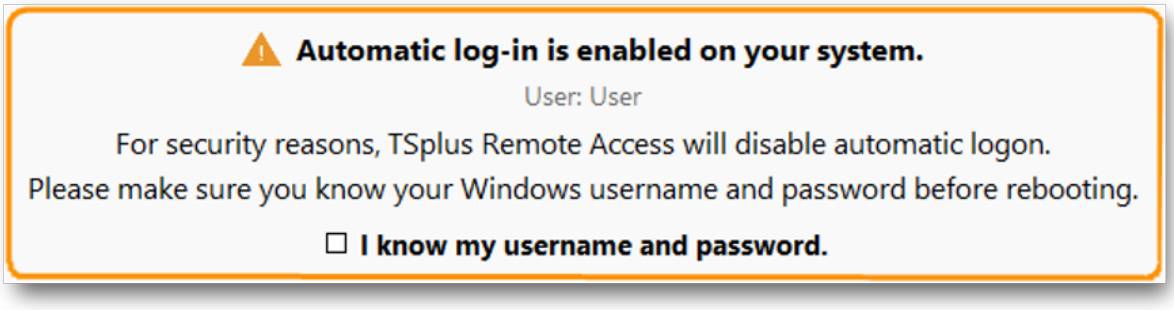


☐ **Aviso Importante**

Por razones de seguridad, **TSPlus Remote Access** requerirá que ingreses manualmente tu nombre de usuario y contraseña en cada inicio de sesión.

Asegúrate de conocer tus credenciales antes de reiniciar el sistema para evitar quedarte fuera.

Si
autologon
está habilitado en el sistema, el instalador mostrará un mensaje de advertencia pidiéndole que confirme que conoce su nombre de usuario y contraseña.



Para usar TSplus, debes reiniciar tu sistema. El período de prueba ofrece un producto completo durante 15 días y 5 usuarios concurrentes.

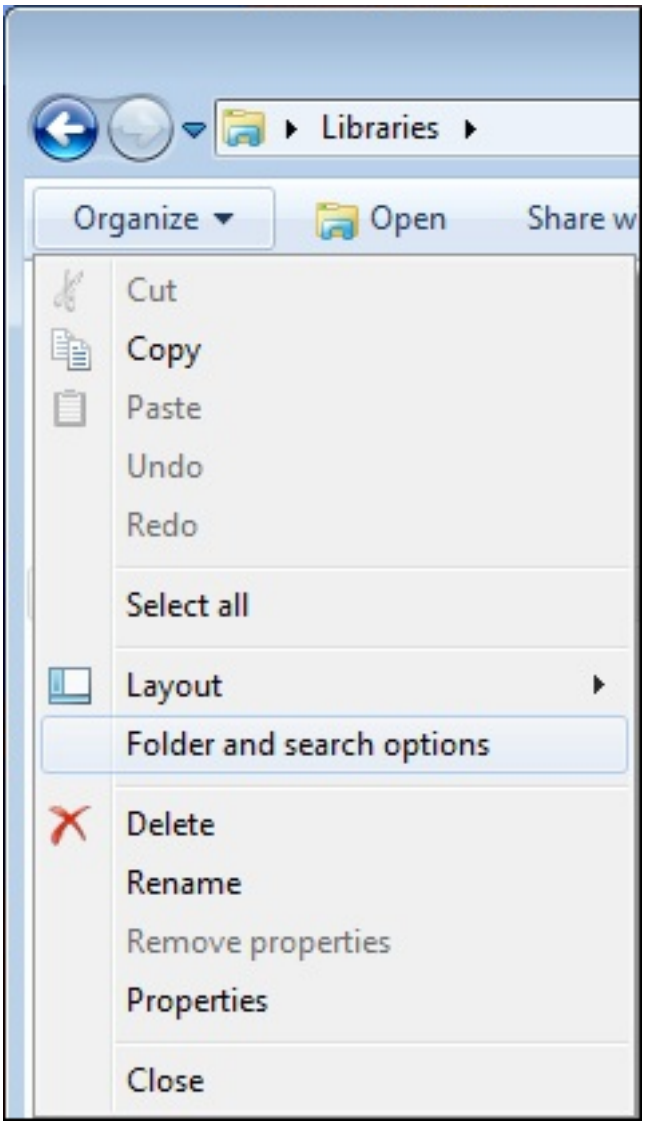
Cómo montar una unidad lógica dentro de una sesión de TSplus

Este tutorial cubrirá los siguientes aspectos:

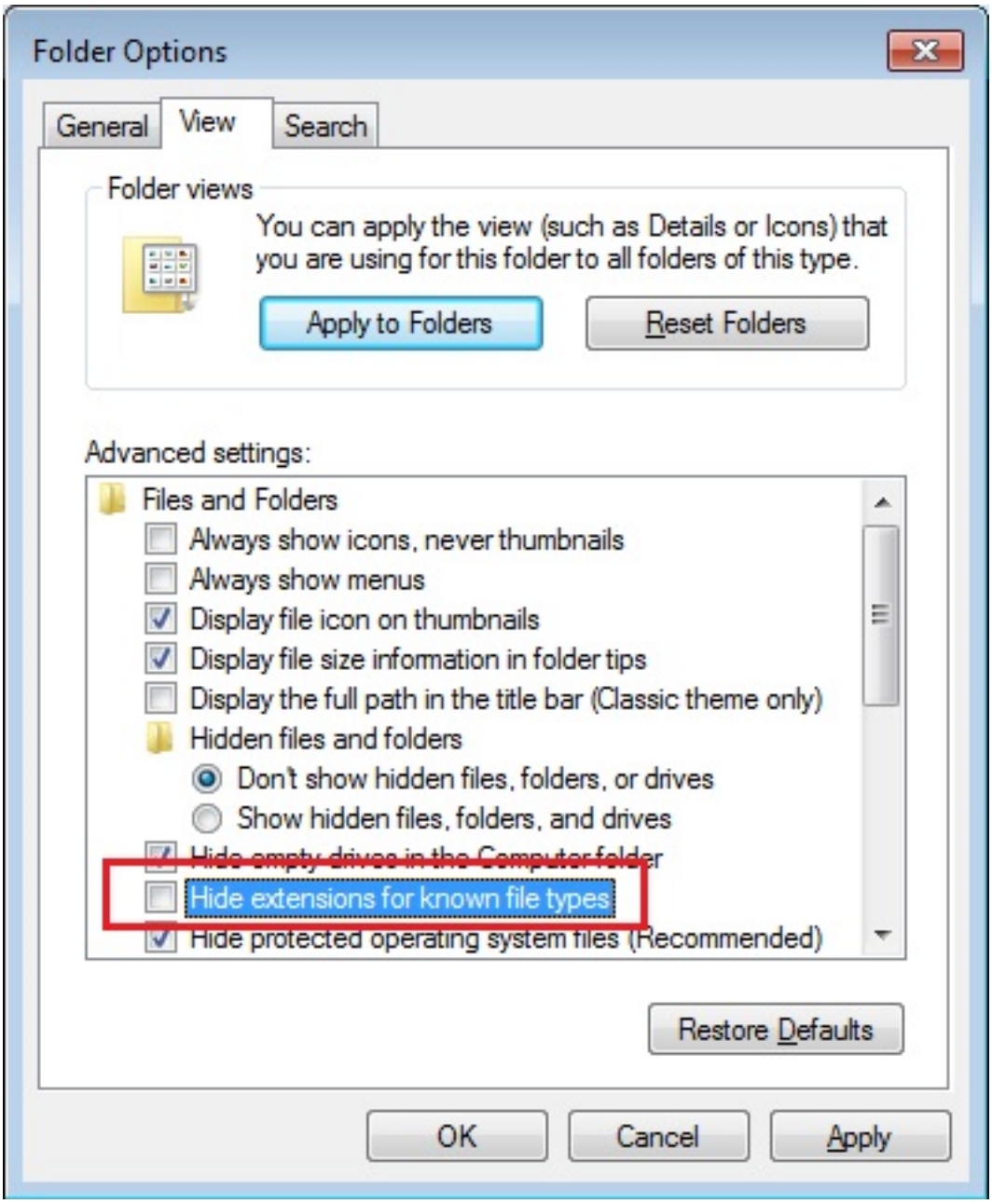
- Cómo implementar un script de inicio de sesión y tener múltiples escenarios de scripts de inicio de sesión.
- Montando una carpeta específica dentro de una sesión desde el lado del cliente o del servidor.

Si desea publicar una carpeta en una unidad virtual lógica para sus usuarios, simplemente siga este procedimiento:

Antes de crear el script, abre el explorador de Windows y haz clic en "Opciones de carpeta y búsqueda".



Luego, haz clic en la pestaña de vista y desmarca la casilla "Ocultar extensiones para tipos conocidos":

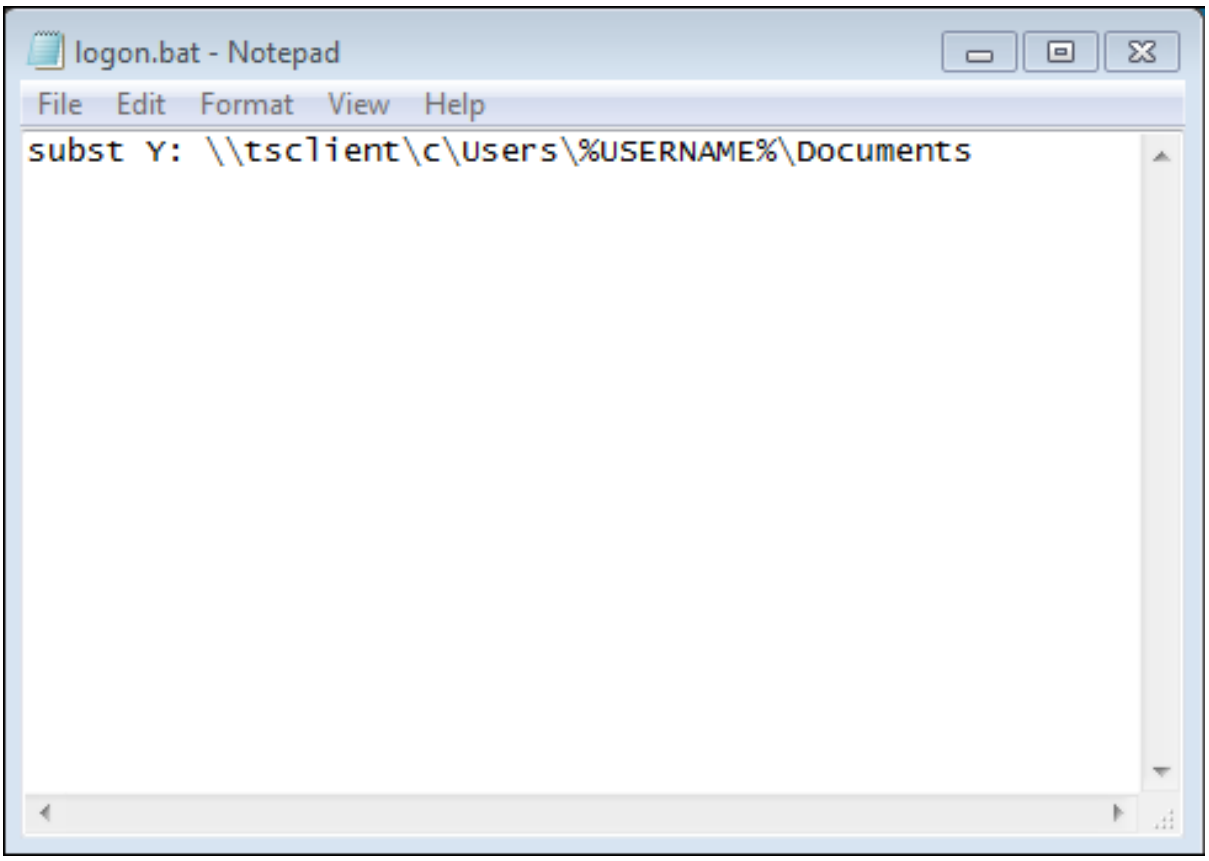


Crea un documento de texto y modifica la extensión nombrándolo “logon.bat”:



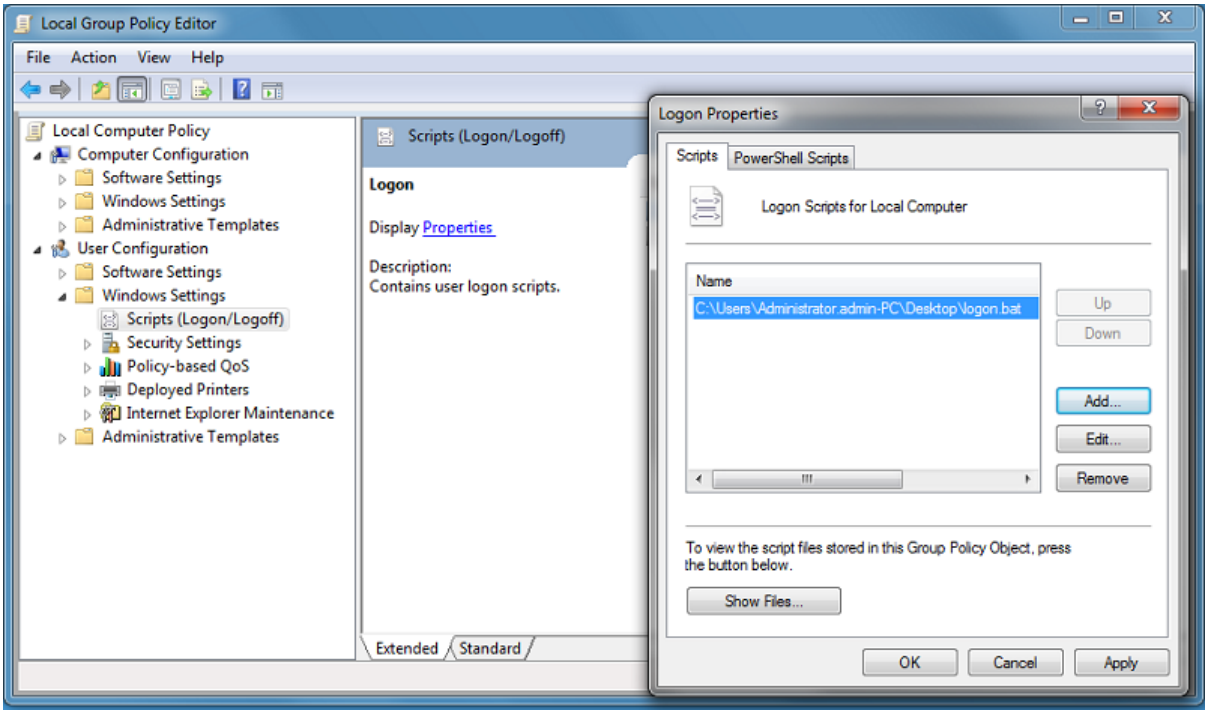
Dentro del archivo, ingrese por ejemplo este comando para publicar la carpeta Folder.exe:

subst Y: \tsclient\C\Users%USERNAME%\Documents

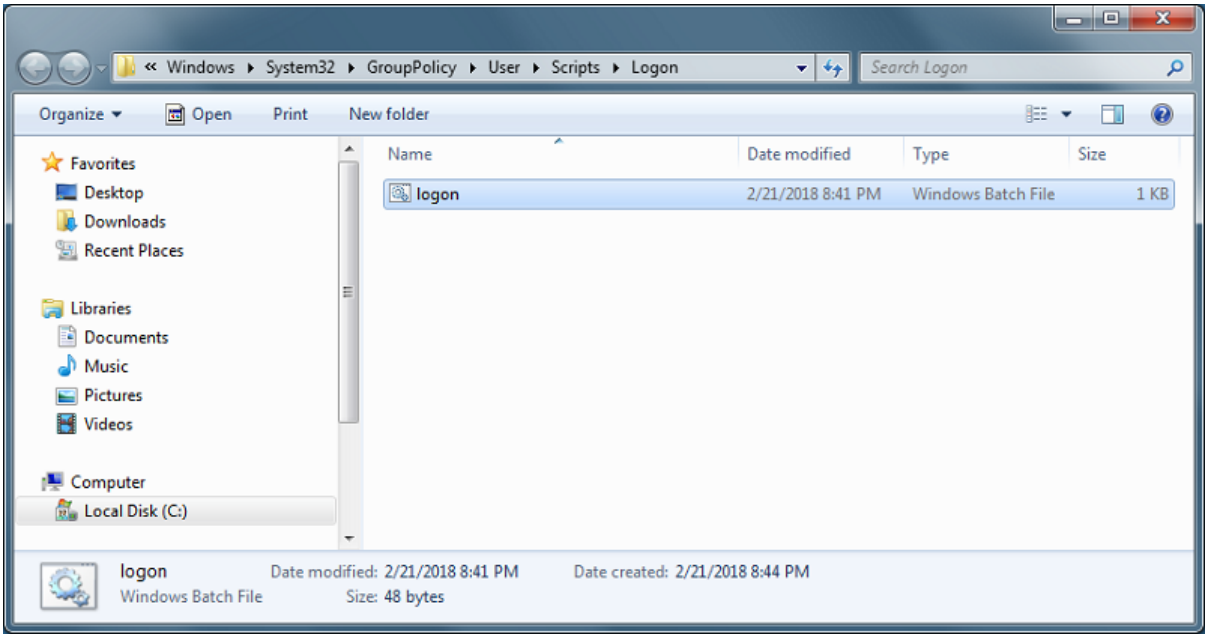


Luego, en el menú de inicio, escribe gpedit.msc en la barra de tareas de búsqueda. Vamos a utilizar la política local para que cada usuario que se conecte a este servidor ejecute el script.

Ve al menú de configuración del usuario, luego a la configuración de Windows y finalmente a Scripts (Inicio/Cierre de sesión). Haz doble clic en el script de inicio de sesión, luego haz clic en "Agregar" y después en "Examinar".

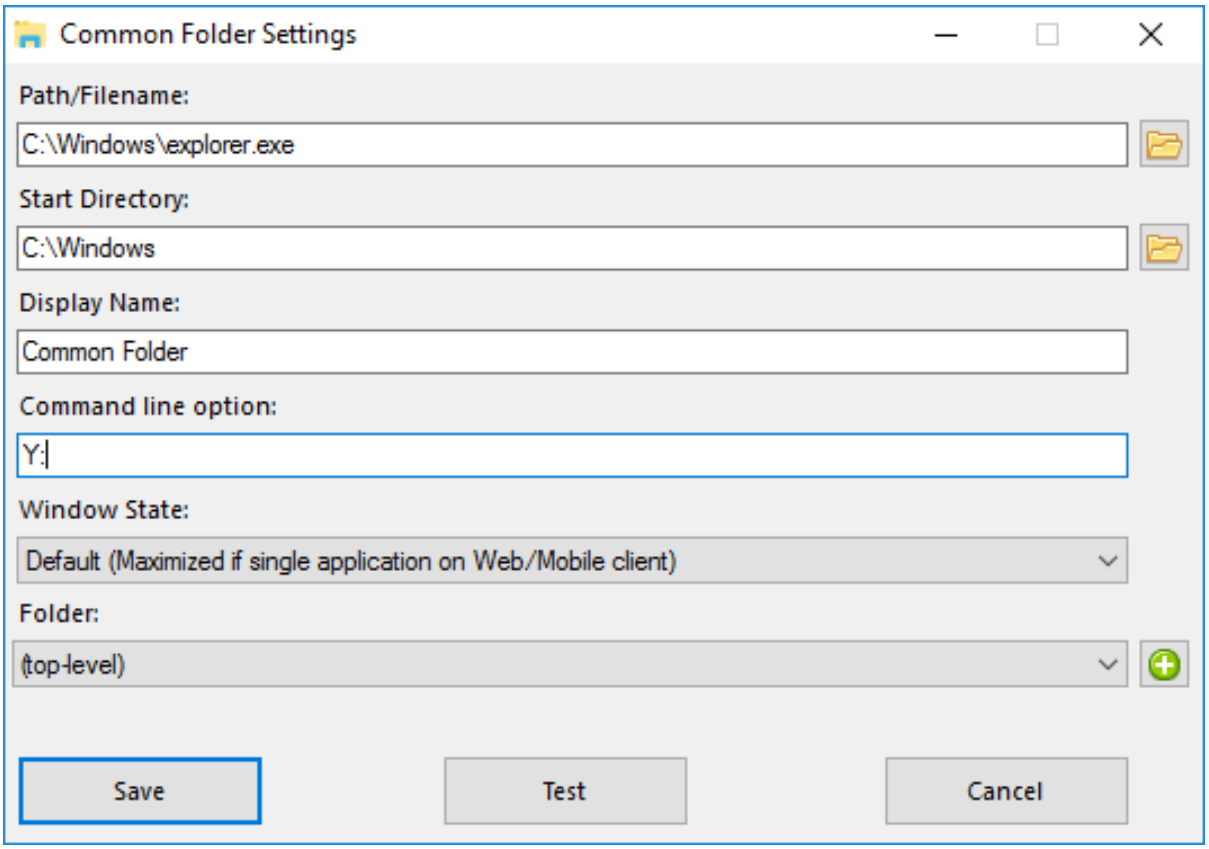


Luego, haga clic en el botón "Mostrar archivos" en la ventana de propiedades de inicio de sesión y copie su script logon.bat en la ruta proporcionada por el Editor de políticas, es decir: "C:\Windows\System32\GroupPolicy\User\Scripts\Logon"



- Puedes copiar este archivo logon.bat en C:\ProgramData si deseas que este script se ejecute para todos tus usuarios.
- Si necesita un script de inicio de sesión específico para cada usuario, copie el script en C:\Users\Username\AppData\Roaming

Ahora, ¿cómo hacemos que esta unidad Y aparezca en la sesión del usuario? Hay muchas maneras de lograr esto. Puedes crear una nueva aplicación dentro de la herramienta de administración y asignarla a tus usuarios; al hacerlo, el acceso directo aparecerá en la sesión.


Common Folder Settings
Path/Filename:
C:\Windows\explorer.exe
Start Directory:
C:\Windows
Display Name:
Common Folder
Command line option:
Y:
Window State:
Default (Maximized if single application on Web/Mobile client)
Folder:
(top-level)
Save
Test
Cancel


CommonFolder

Si te conectas a una sesión con mstsc.exe, no olvides ir al menú de opciones, y en la pestaña Recursos locales, bajo Dispositivos y recursos locales, haz clic en "Más", luego marca la casilla "Unidades".

Si desea asignar este script solo a usuarios no administradores, siga esto tutorial .

Si desea asegurar el acceso a una carpeta, consulte nuestra documentación para publicar un carpeta asegurada .

Ticket de inicio de sesión y balanceo de carga

Creación de Ticket de Inicio de Sesión en el Servidor Gateway

Puedes crear un ticket de inicio de sesión en el portal con:

/socket.io/LPW?WinUser=DOMINIO\INICIO DE SESIÓN&WinPassword=CONTRASEÑA

Pero solo te permitirá conectarte en el servidor de puerta de enlace mismo.

Creación de Ticket de Inicio de Sesión en un Servidor de Aplicaciones

También puede crear un ticket de inicio de sesión en un servidor de aplicaciones con proxy inverso con:

/srv4/socket.io/LPW?WinUser=DOMINIO\INICIO DE SESIÓN&WinPassword=CONTRASEÑA

asumiendo que ~~srv4 es el nombre interno del servidor de aplicaciones según lo configurado en TSplus reverse-proxy

Pero solo te permitirá conectarte a este servidor de aplicaciones específico.

Ticket de inicio de sesión y balanceo de carga

Así que si deseas utilizar tickets de inicio de sesión y balanceo de carga, es posible que desees realizar una solicitud HTTP adicional primero:

https://your-gateway-server.com/cgi-bin/hb.exe?action=lb&l=LOGIN&d=DOMAIN&t=TIMESTAMP

Esto devolverá una respuesta como esta.

loadbalancing-on|SERVIDOR DE APLICACIONES 4|your-gateway-server.com/~~srv4|https|443|

Puedes analizar esta respuesta para recuperar el servidor de aplicaciones en el que TSplus Load-Balancer te recomendaría conectar a este usuario específico.

es decir, recomendará el servidor menos cargado en su granja de TSplus, si las sesiones persistentes están habilitadas en su portal de TSplus, tendrá en cuenta las sesiones activas existentes, etc.

Puedes crear un ticket de inicio de sesión en este servidor de aplicaciones específico y conectarte a él.

Esto es precisamente la solicitud http realizada en la página de inicio de sesión del portal web de TSplus.

Usando un Ticket de Inicio de Sesión para Abrir una Sesión de Usuario

Ahora que tiene un ticket de inicio de sesión válido, puede abrir una sesión de usuario utilizando este ticket abriendo una ventana del navegador a esta URL:

https://your-gateway-server.com/~~srv4/software/html5.html?user=*xxxxxxxx

donde “xxxxxxxx” es el ticket de inicio de sesión.

Versiones de Soporte a Largo Plazo

Clientes que se han suscrito a los Servicios de Soporte y Actualización de TSplus y no están interesados en las últimas características y mejoras de TSplus pueden instalar una versión LTS (Soporte a Largo Plazo) de TSplus.

TSplus LTS (Soporte a Largo Plazo) extiende el período de mantenimiento del software; también reduce la frecuencia de las actualizaciones del software para disminuir el riesgo, el costo y la interrupción del despliegue del software, al tiempo que promueve la confiabilidad del software.

Además, TSplus LTS (Soporte a Largo Plazo) no recibe nuevas funciones.

TSplus ciclo de vida

Las versiones estándar de TSplus se publican con bastante frecuencia y la última versión siempre es la mejor solución disponible para nuestros clientes: todos los errores conocidos se corrigen y las nuevas funciones están disponibles con mucha frecuencia.

Se lanza una nueva versión importante de TSplus al comienzo de cada año.

A partir de enero de 2019, TSplus también está disponible en una versión de Soporte a Largo Plazo, llamada "LTS". Cada nueva versión principal, TSplus publicará una versión LTS estable de la versión anterior que será compatible durante 2 años.

Beneficios y limitaciones de TSplus LTS

TSplus LTS tiene varios beneficios:

- No hay actualizaciones excepto para correcciones de seguridad y compatibilidad con actualizaciones de Windows.
- Sin cambios en el comportamiento y sin cambios en las características cuando actualizas.
- Menos riesgo al actualizar entre dos versiones menores de un LTS dado
- Compatible durante al menos 2 años

TSplus LTS también tiene limitaciones y restricciones:

- El cliente debe adquirir los Servicios de Soporte y Actualización (una licencia no se puede

activar sin Servicios de Soporte y Actualización activos).
- No hay nuevas características en absoluto (en comparación con la versión estándar de TSplus que recibe constantemente muchas actualizaciones y nuevas características)

Recomendamos a nuestros clientes que utilicen la versión estándar de TSplus para beneficiarse de nuestra solución de vanguardia.

TSplus LTS Enlaces

TSplus LTS 18 soportado desde 2026-01 hasta 2028-01:

- Historial de cambios
- Configuración para instalar TSplus en un nuevo servidor
- Actualización de lanzamiento para actualizar una instalación existente de TSplus
- Documentación de LTS18

TSplus LTS 17 soportado desde 2025-01 hasta 2027-01:

- Historial de cambios
- Configuración para instalar TSplus en un nuevo servidor
- Actualización de lanzamiento para actualizar una instalación existente de TSplus
- LTS17 Documentación

TSplus LTS 16 (compatible desde 2024-01 hasta 2026-01): **Fin del soporte**

TSplus LTS 15 (compatible desde 2023-01 hasta 2025-01): **Fin del soporte**

TSplus LTS 14 (compatible desde 2021-12 hasta 2023-12): **Fin del soporte**

TSplus LTS 12 (compatible desde 2019-12 hasta 2022-12): **Fin del soporte**

TSplus LTS 11 (compatible desde 2018-12 hasta 2021-12): **Fin del soporte**

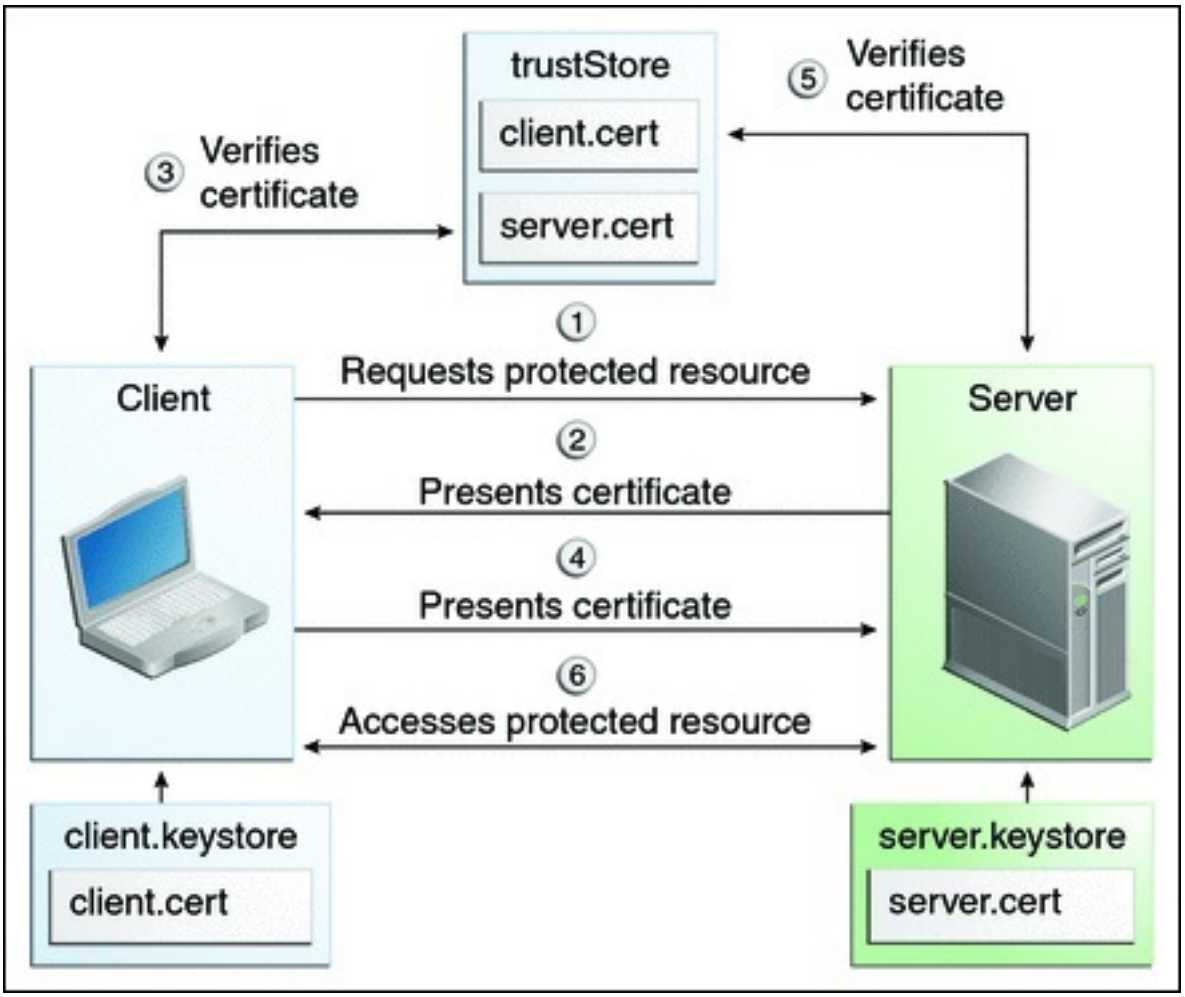
Activando la autenticación SSL mutua

¿Qué es la autenticación mutua?

Muchas personas están esperando una seguridad adicional y la autenticación mutua ya es compatible con Terminal Service Plus. Generalmente, es implementada por bancos o entidades gubernamentales.

Para entender qué es eso, podemos compararlo con un proceso estándar de SSL donde agregarás una verificación adicional para confirmar si el navegador web del usuario permite la conexión SSL. Sabes cuál es tu certificado SSL del lado del servidor. Imagina que el certificado se importa en el navegador web para asegurar que este navegador web específico sea de confianza para crear una conexión. En el primer paso de la comunicación, el navegador web actúa como un cliente y en el segundo paso, es al revés. Al final, ambos lados, el navegador web del cliente y el servidor web, han aceptado la autoridad y la conexión puede comenzar.

Una definición más completa: La autenticación mutua SSL o la autenticación mutua basada en certificados se refiere a que dos partes se autentican mutuamente mediante la verificación del certificado digital proporcionado, de modo que ambas partes estén seguras de la identidad de la otra. En términos tecnológicos, se refiere a un cliente (navegador web o aplicación cliente) que se autentica ante un servidor (sitio web o aplicación de servidor) y ese servidor también se autentica ante el cliente mediante la verificación del certificado de clave pública/certificado digital emitido por las Autoridades de Certificación (CAs) de confianza. Debido a que la autenticación se basa en certificados digitales, las autoridades de certificación como Verisign o Microsoft Certificate Server son una parte importante del proceso de autenticación mutua.



Activándolo en TSplus

TSplus el servidor web integrado permite configurar la autenticación mutua.

Para habilitar la autenticación mutua, siga este proceso:

Tendrás que instalar el último Kit de Desarrollo de Java (JDK), disponible en http://java.com > Descargas > JDK.

1. Crea y edita con Notepad el siguiente archivo: C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin

Agrega estas 3 líneas:

disable_http_only=true disable_print_polling=true force_mutual_auth_on_https=true

2. Eliminar cert.jks

En “C:\Program Files (x86)\TSplus\Clients\webserver” verás el archivo cert.jks. Copíalo en “C:\Program Files (x86)\TSplus\Clients”. Elimina “C:\Program Files (x86)\TSplus\Clients\webserver\cert.jks”.

3. Crear el archivo por lotes

En ‘C:\Program Files (x86)\TSplus\Clients’ crea un archivo por lotes, por ejemplo “createcertuser.bat” con estas configuraciones:

@rem descomentar la siguiente línea, si desea generar un nuevo cert.jks autofirmado @rem keytool -genkey -v -alias jwts -keyalg RSA -validity 3650 -keystore cert.jks -storepass secret -keypass secret -dname “CN=localhost, OU=my_ou, O=my_org, L=my_city, ST=my_state, C=MY” @keytool -genkey -v -alias AliasUser1 -keyalg RSA -storetype PKCS12 -keystore forBrowserUser1.p12 -dname “CN=some_name, OU=some_ou, O=some_org, L=Paris, ST=FR, C=FR” -storepass mypassword -keypass mypassword @keytool -export -alias AliasUser1 -keystore forBrowserUser1.p12 -storetype PKCS12 -storepass mypassword -rfc -file forCertUser1.cer @keytool -alias AliasCertUser2 -import -v -file forCertUser1.cer -keystore cert.jks -storepass secret @del forCertUser1.cer

Esto importará automáticamente el par de claves del certificado desde el navegador web a "cert.jks" después de crear su par de claves del navegador.

4. Restaurar el nuevo “cert.jks” modificado

Copia “C:\Program Files (x86)\TSplus\Clients\cert.jks” en “C:\Program Files (x86)\TSplus\Clients\webserver” y reinicia los servidores web.

5. Importación y prueba de certificado

El ejemplo de lote proporcionado debería haber generado un archivo de prueba “BrowserUser1.p12”. Cuando abras la dirección HTTPS, recibirás un mensaje de seguridad y no podrás acceder a las páginas del servidor web. Con Chrome o IE, puedes hacer clic en este archivo ‘BrowserUser1.p12’ para importar el certificado en el almacén de claves predeterminado de Windows. Con FireFox, debes ir a Configuración e importar este archivo “BrowserUser1.p12” en tu carpeta de certificados.

Tan pronto como lo hayas importado correctamente, podrás acceder a la dirección HTTPS.

El administrador puede crear un archivo de par de claves separado para cada usuario.

Por ejemplo:

forBrowserUser1.p12 forBrowserUser2.p12 forBrowserUser3.p12

Y puede exportar estos certificados en cert.jks. Si desea deshabilitar el acceso a un usuario, solo tendrá que eliminar a este usuario de "cert.jks". Al hacerlo, el usuario perderá su autorización y no podrá acceder al servidor web.

Esta autenticación mutua solo afecta las conexiones HTTPS y la conexión HTTP estará prohibida con la línea de comandos: settings.bin>disable_http_only=true

Abrir archivos en el lado del cliente

Resumen

Esta función es poderosa. Permite abrir documentos ubicados en el servidor en el lado del cliente según su extensión de archivo.

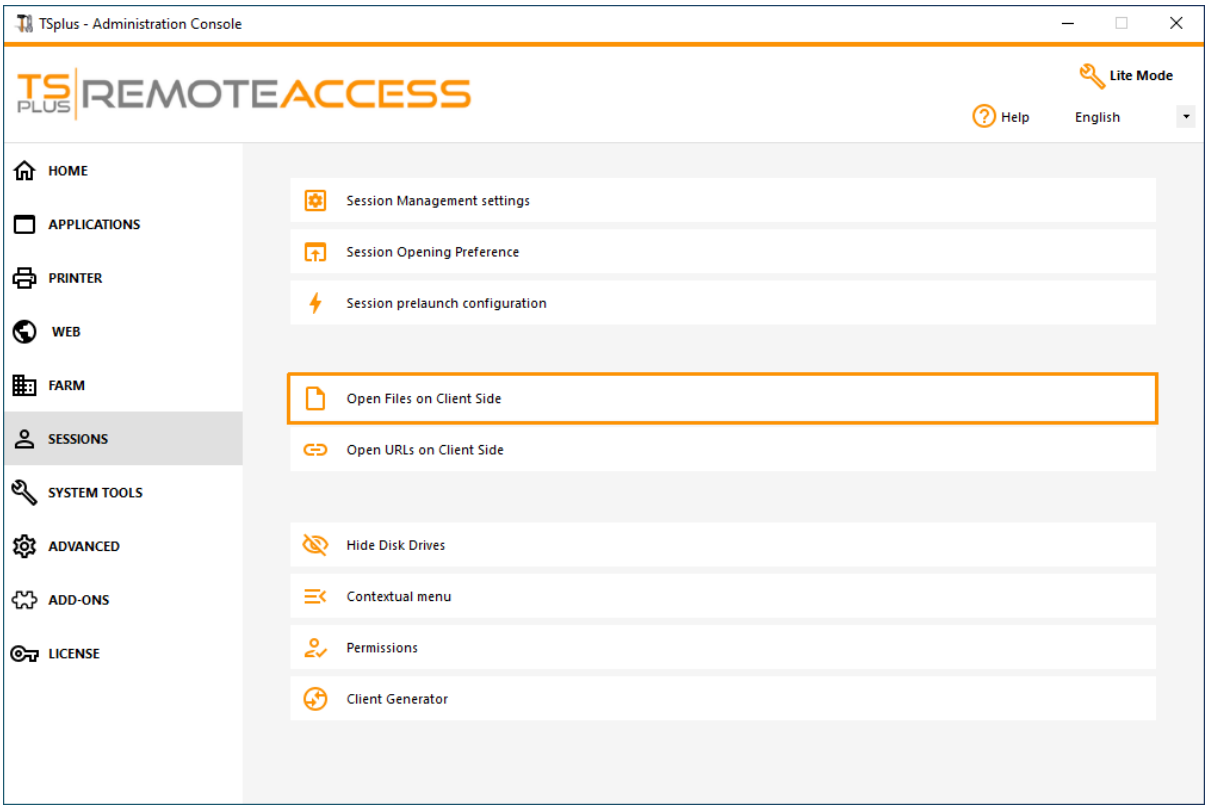
Por ejemplo, puedes abrir un documento de Microsoft Office Word sin tener Office instalado en tu servidor.

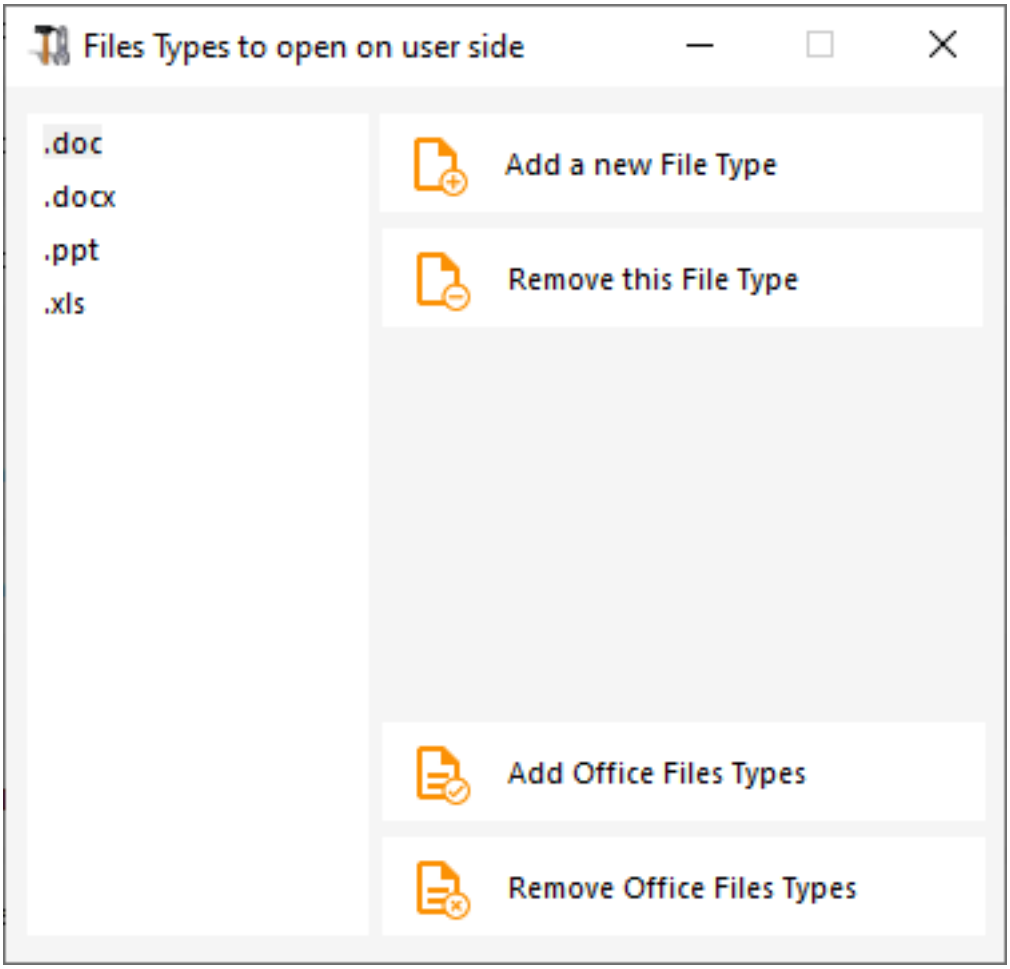
El documento .docx (o .xlsx) se carga automáticamente en el lado del usuario donde se utilizará la Office local para abrirlo.

Si está alojando su aplicación en un servidor en la nube y si su aplicación está generando un documento de Excel, Access o Word, esta función evita preocuparse por las licencias de Office en el servidor.

Configurar un tipo de archivo para abrir en el lado del cliente

El tile "Abrir archivos en el lado del cliente" se encuentra en la pestaña "Sesiones - Configuración" de AdminTool. Haga clic en él para mostrar la ventana de configuración:





El botón “Agregar un nuevo tipo de archivo” te permite añadir una extensión (como “.docx” para

Microsoft Office Word 2007-2010) a la lista.

Todos los archivos que tengan una extensión en esta lista se abrirán en el lado del cliente. , siempre que utilice uno de los clientes de conexión de Terminal Service Plus:

- Cualquier cliente de Terminal Service Plus generado (RemoteApp o RDP)
- Cualquier conexión de Windows desde el Portal Web de Terminal Service Plus
- Cualquier conexión HTML5 desde el Portal Web de Terminal Service Plus

Advertencia: esta función no es compatible con:

- Cualquier cliente RDP (mstsc por ejemplo)

Solución de problemas

Si ha configurado un tipo de archivo para abrir en el lado del cliente y no está funcionando (es decir, el archivo aún se abre en su propia computadora), le aconsejamos que verifique la lista de "Abrir con" en el menú contextual de Windows:

- haga clic derecho en el archivo.
- haga clic en el elemento del menú "Abrir con".
- si hay más de una aplicación en esta lista, haga clic en "Elegir programa predeterminado" y seleccione "OpenOnClient.exe".

Esta herramienta de Terminal Service Plus aplica su configuración a todos los usuarios que utilizan el ordenador, sin embargo, tenga en cuenta las siguientes reglas:

- Windows permite a cada usuario cambiar este programa de apertura predeterminado por otro programa de su elección.
- Usando el cliente de conexión HTML5, el archivo será descargado y gestionado por el navegador local. Algunos navegadores tratan ciertos tipos de archivos de maneras específicas, por lo que también se deben verificar dos veces la configuración del navegador.

Estas reglas explican la mayoría de los problemas al usar la función Open On Client, por eso te aconsejamos comenzar revisando el programa predeterminado:

- para el usuario conectado en el servidor
- para el usuario en el cliente
- para el navegador en el cliente (al usar HTML5)

Abrir URLs en el lado del cliente

Resumen

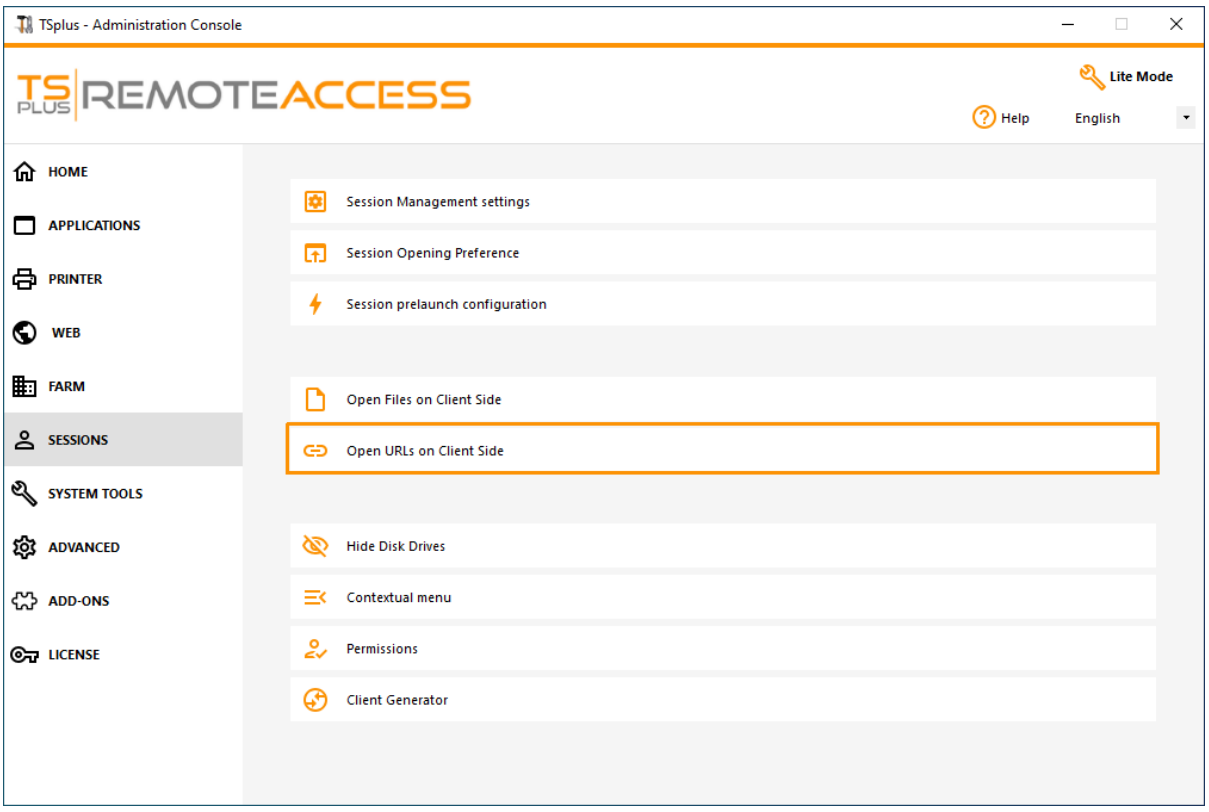
Esta función es poderosa. Permite abrir en el lado del cliente todos los enlaces de sitios web y accesos directos de sitios web ubicados en el servidor.

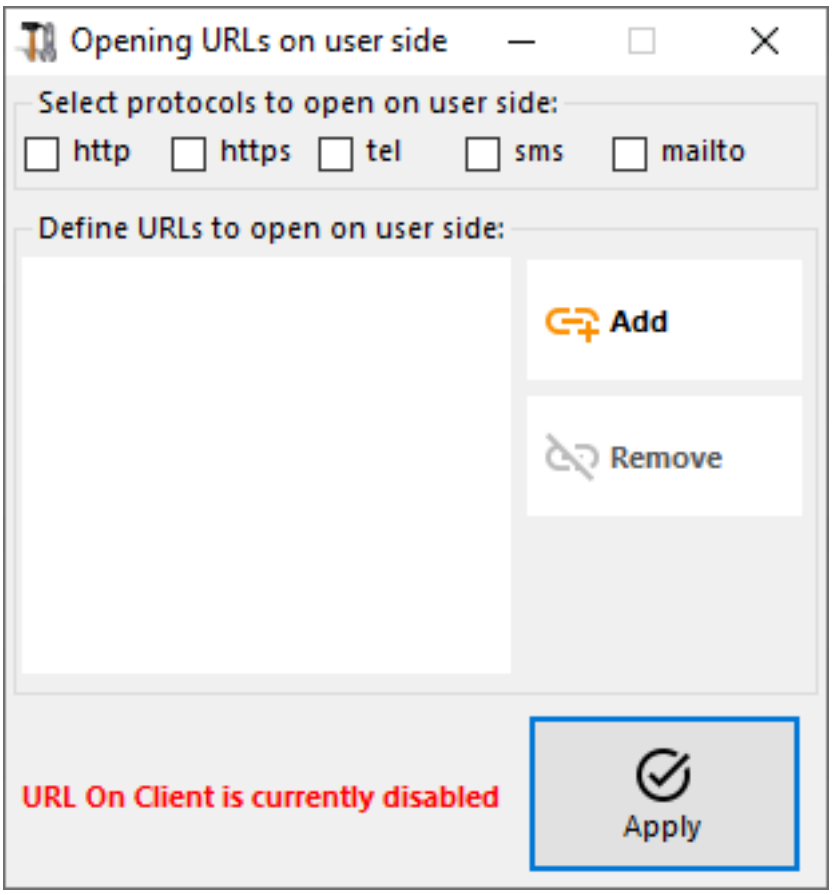
Por ejemplo, puedes abrir videos de YouTube directamente en el cliente, ahorrando así mucho ancho de banda y potencia de CPU en tu servidor.

La dirección web (URL) se transfiere automáticamente al lado del usuario donde se utilizará el navegador predeterminado local para abrirla.

Habilitar esta función en un servidor

El mosaico "Abrir URLs en el lado del cliente" se encuentra en la pestaña "Sesiones - Configuración" de AdminTool. Haga clic en él para mostrar la ventana de configuración:





Las casillas de los protocolos http y https no están marcadas por defecto.
También puede activar los protocolos tel, sms y mailto marcando las casillas correspondientes.

Luego haga clic en el botón "Aplicar", que le permite activar esta función para todos los usuarios en el servidor.

Para habilitar completamente esta función, cada usuario tendrá que reiniciar su sesión (cerrar sesión y luego iniciar sesión) antes de que puedan usar esta función.

Todos los enlaces web y accesos directos se abrirán en el lado del cliente. , siempre que utilice uno de los clientes de conexión de Terminal Service Plus:

- Cualquier cliente de Terminal Service Plus generado (RemoteApp o RDP)
- Cualquier conexión de Windows desde el Portal Web de Terminal Service Plus
- Cualquier conexión HTML5 desde el Portal Web de Terminal Service Plus.

Advertencia: esta función no es compatible con:

- Cualquier cliente RDP (mstsc por ejemplo).

Comportamiento del navegador web (Portal web):

Algunos navegadores web, particularmente en dispositivos iOS, no permiten que los enlaces se abran automáticamente desde nuestra aplicación. En estos casos, se muestra un enlace clicable

para que los usuarios puedan acceder manualmente al destino previsto.



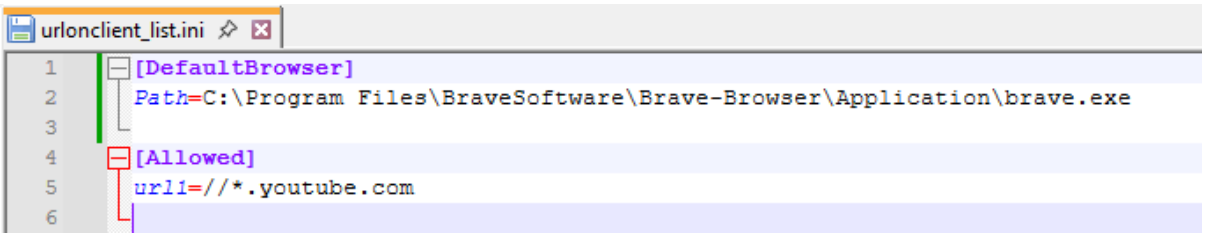
Cambiando el navegador web predeterminado del servidor

Todas las URL que no estén definidas para abrirse en el lado del cliente continuarán abriéndose en el lado del servidor, utilizando Microsoft Edge o Internet Explorer. Si desea cambiar el navegador web predeterminado utilizado en el lado del servidor, debe editar el archivo de configuración. **urlonclient_list.ini** ubicado en la carpeta de instalación de TSPlus.

La ubicación exacta (dependiendo de su ruta de instalación exacta) debería ser: C:\Program Files (x86)\TSplus\UserDesktop\files\urlonclient_list.ini .

Necesitas agregar una nueva sección “DefaultBrowser” en el archivo, y una entrada “Path” con el valor de la ruta del navegador web que deseas. Así:

[DefaultBrowser]
Path=C:\Path\To\Your\Favorite\WebBrowser.exe



Estableciendo el navegador predeterminado a Brave

☐ **Si ha reemplazado firefox.exe por c:\wsession\URLonClient.exe**

y quieres que Firefox sea tu navegador web predeterminado en el lado del servidor :

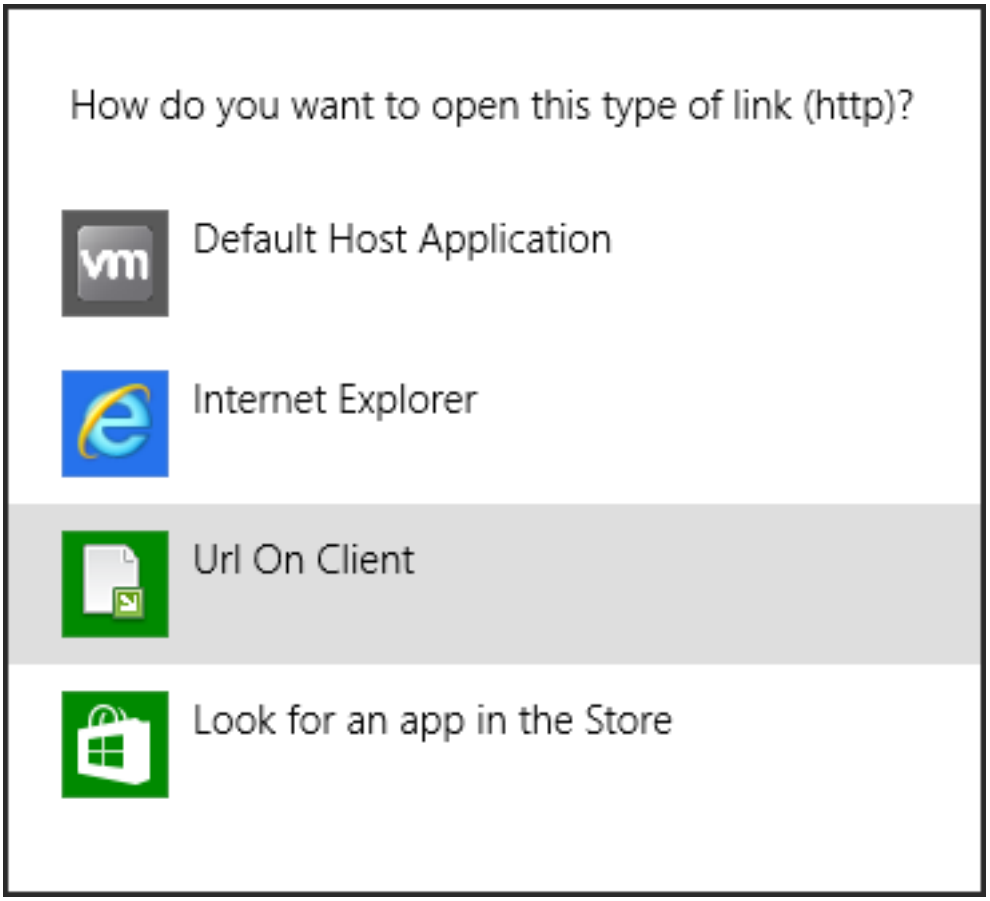
- Renombra el archivo antiguo firefox.exe a firefox-real.exe.
- utilice el nuevo nombre del ejecutable en el **urlonclient_list.ini** archivo :

[DefaultBrowser]
Path=C:\Program Files\Mozilla Firefox\firefox-real.exe

Windows 8 y 8.1

A partir de Windows 8, Microsoft ha prohibido el cambio automático del navegador predeterminado del usuario.

Esta es la razón por la cual, una vez que la función está activada en el servidor, cada usuario tendrá que elegir 'Url en Cliente' cuando se le pregunte por un navegador predeterminado.



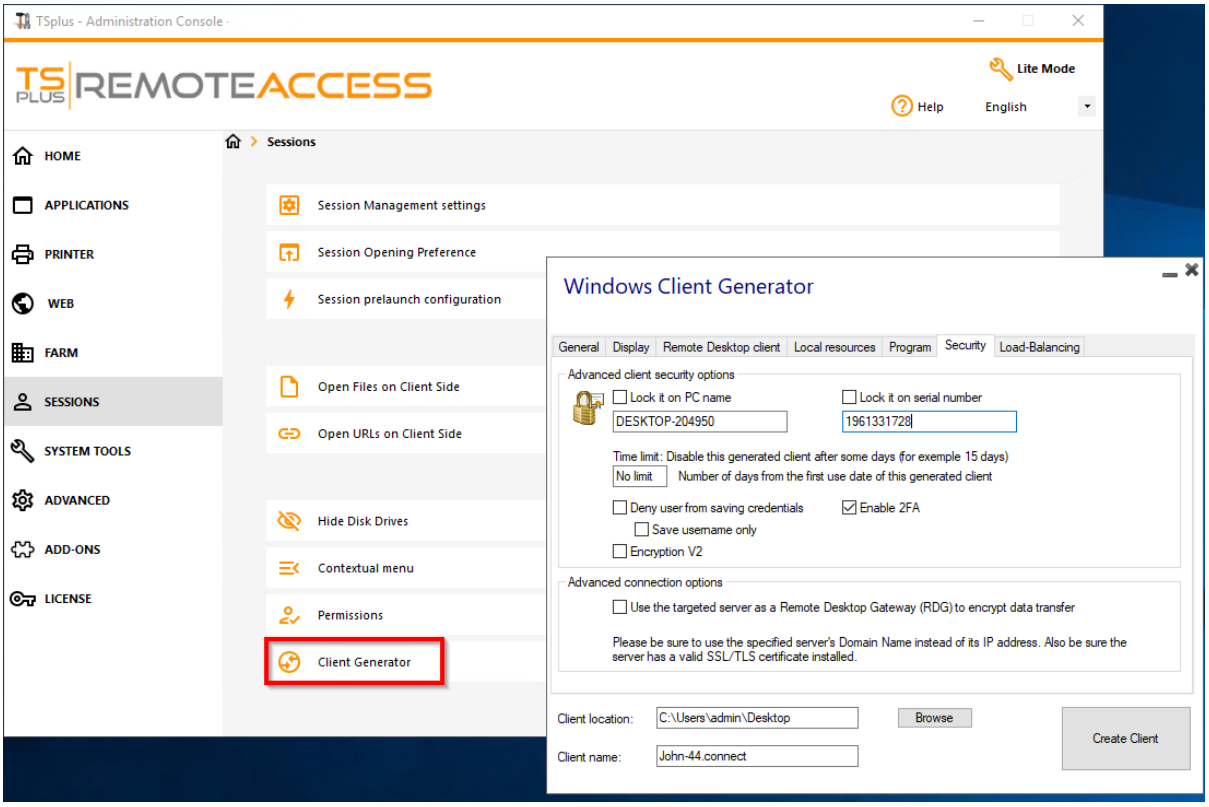
Esta ventana solo se mostrará la primera vez que un usuario abra un enlace web. Desafortunadamente, esta es la política de Microsoft Windows y no estamos al tanto de ninguna solución alternativa.

Generador de Cliente Portátil

TSplus crea por defecto un icono para el Generador de Cliente Portátil:



También se puede acceder en la pestaña de Sesiones del AdminTool:



Permite crear 2 tipos de clientes de conexión que se pueden copiar en el escritorio de los

usuarios o en una memoria USB para uso portátil.

Nota Los clientes de conexión no son compatibles con computadoras Mac.

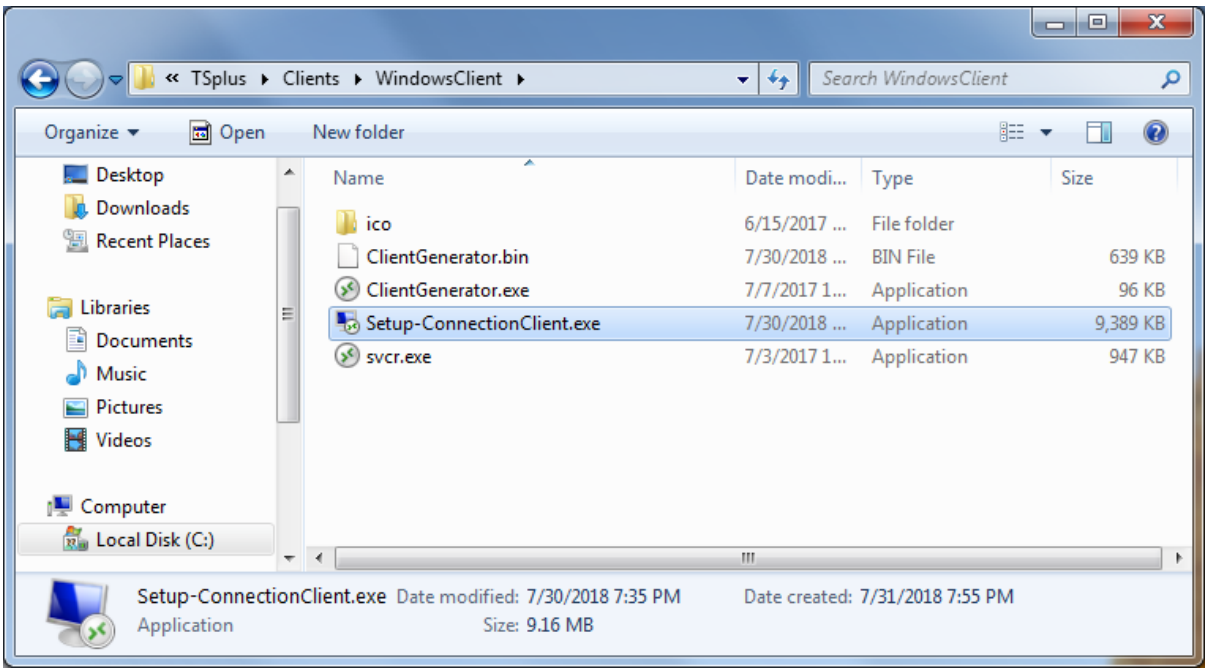
Desde el lanzamiento de TSplus 11.40, el generador de clientes ha sido rediseñado para estar firmado numéricamente y evitar reacciones falsas/positivas de los antivirus.

En lugar de un programa ".exe", el nuevo Generador de Clientes está creando un archivo plano cifrado con la extensión ".connect":

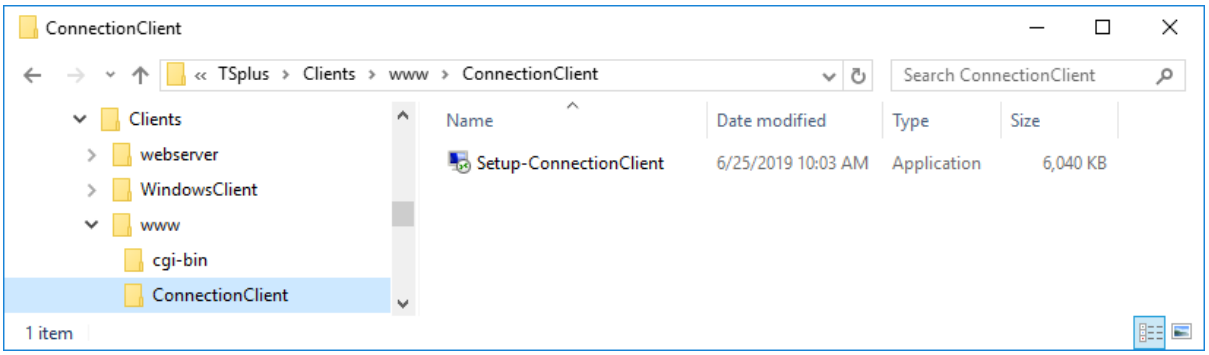


Requisito previo en el lado del cliente

En el lado del cliente, cada usuario deberá ejecutar un programa firmado llamado “Setup-ConnectionClient.exe” como requisito previo. Este programa está disponible en su servidor, en la carpeta del programa TSplus: TSplus\Clients\WindowsClient:



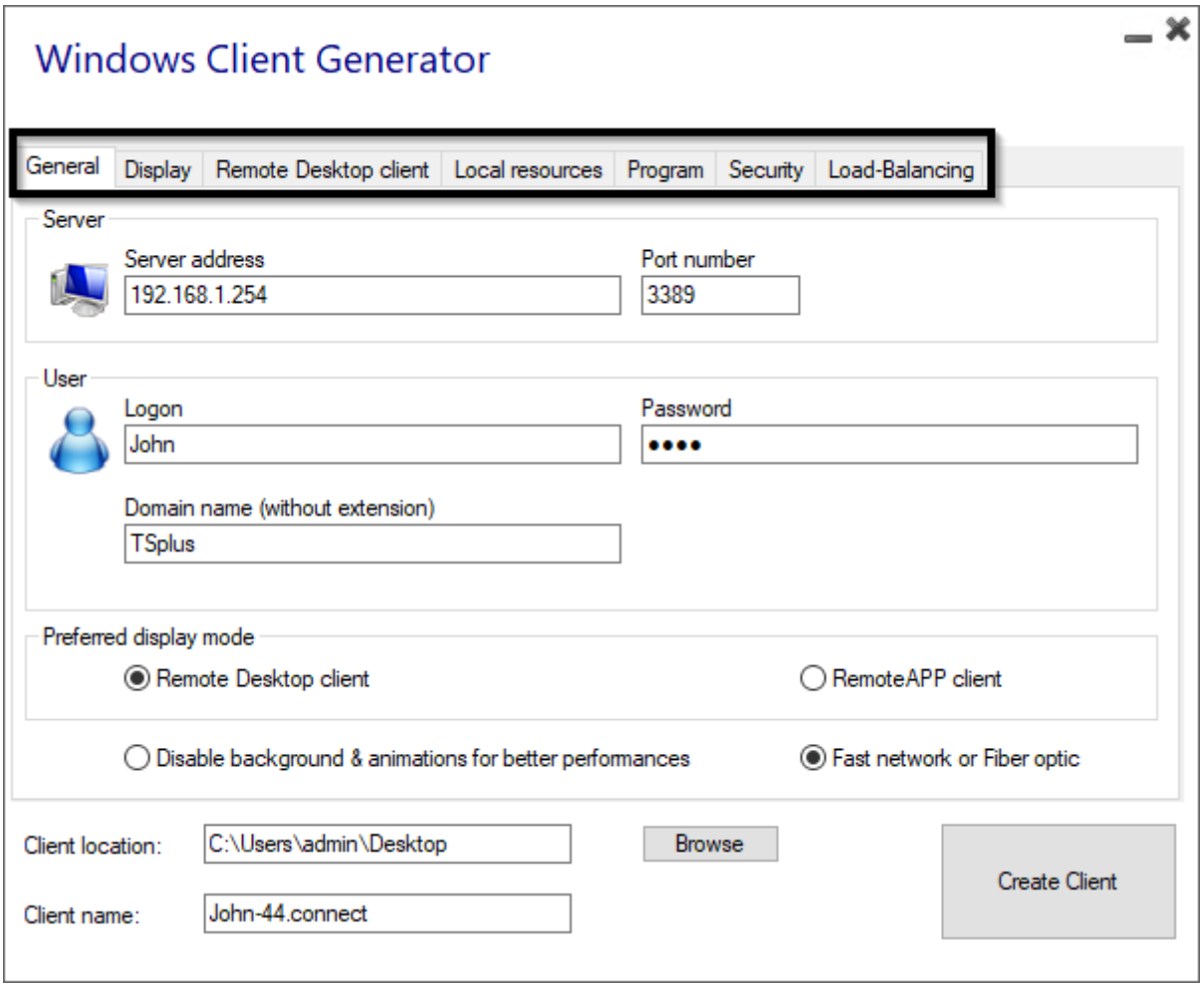
o en la carpeta TSplus\Clients\www:



o por descargándolo .

Descripción Detallada

Haga clic en **un tabulador** ir a la información correspondiente:



Cuando inicias el generador de clientes, la primera pestaña que se muestra es la pestaña general. Aquí encontrarás todos los ajustes de conexión esenciales que necesitas para

comenzar.

- **Dirección del servidor:** Ingrese la dirección IP del servidor al que le gustaría que el cliente se conectara.
- **Número de puerto:** Ingrese el número de puerto del servidor. El predeterminado es 3389.
- **Nombre de usuario y contraseña:** Si ingresas un nombre de usuario y una contraseña, el programa cliente no pedirá al usuario que lo vuelva a escribir en cada sesión.

Para restablecer este guardado de inicio de sesión/contraseña, debe crear y editar un acceso directo del Cliente de Escritorio Remoto y agregar el -reset en cambiar al final del campo de destino.

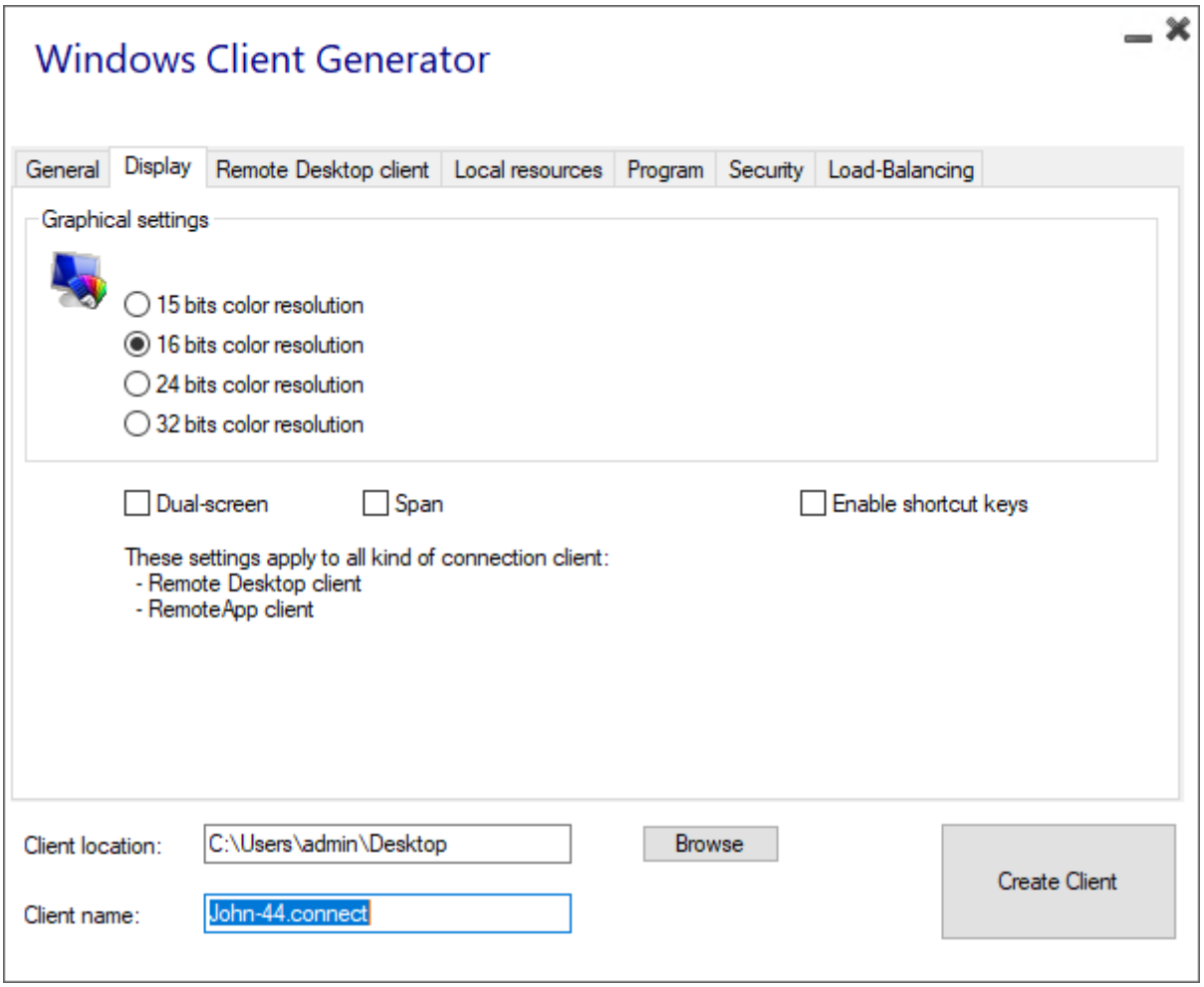
Credenciales

- Si no desea guardar las credenciales, ingrese "nosavecredential" en el campo de inicio de sesión del Generador de Cliente Portátil.
- Si no desea mostrar la ventana de inicio de sesión con el nombre de usuario, la contraseña y el nombre de dominio, simplemente ingrese "nopassword" en el campo de contraseña.
- Si desea habilitar el inicio de sesión automático, ingrese *SSO en el campo de nombre de usuario, el programa cliente solo pedirá el nombre de usuario y la contraseña durante la primera conexión. Guardará esta información en la estación de trabajo del usuario para que el usuario no tenga que identificarse nunca más.
- Si desea que el nombre del usuario local actual se muestre como un inicio de sesión para la sesión, ingrese **, o %USERNAME% en el campo de inicio de sesión.

- **Nombre de dominio:** Ingrese un nombre de dominio si lo tiene.
- **Modo de visualización preferido:** Puedes elegir tu modo de visualización preferido entre las siguientes opciones:
  - El Escritorio Remoto Clásico , mostrando su entorno de sesión remota.

- El Cliente de conexión Microsoft RemoteApp para mostrar sus aplicaciones remotas como si estuvieran instaladas localmente. Tiene un mejor rendimiento gráfico en aplicaciones minimizadas.

- **Velocidad de red** Puedes elegir entre dos opciones dependiendo de la velocidad de tu red:
  - Desactivar la visualización de fondo y las animaciones gráficas para redes de baja velocidad.
  - Habilitar la visualización en segundo plano y las animaciones gráficas para fibra óptica o red rápida.
- **Ubicación del cliente:** Defina la ubicación de su cliente generado.
- **Nombre del cliente:** Puedes nombrar a tu cliente como desees.

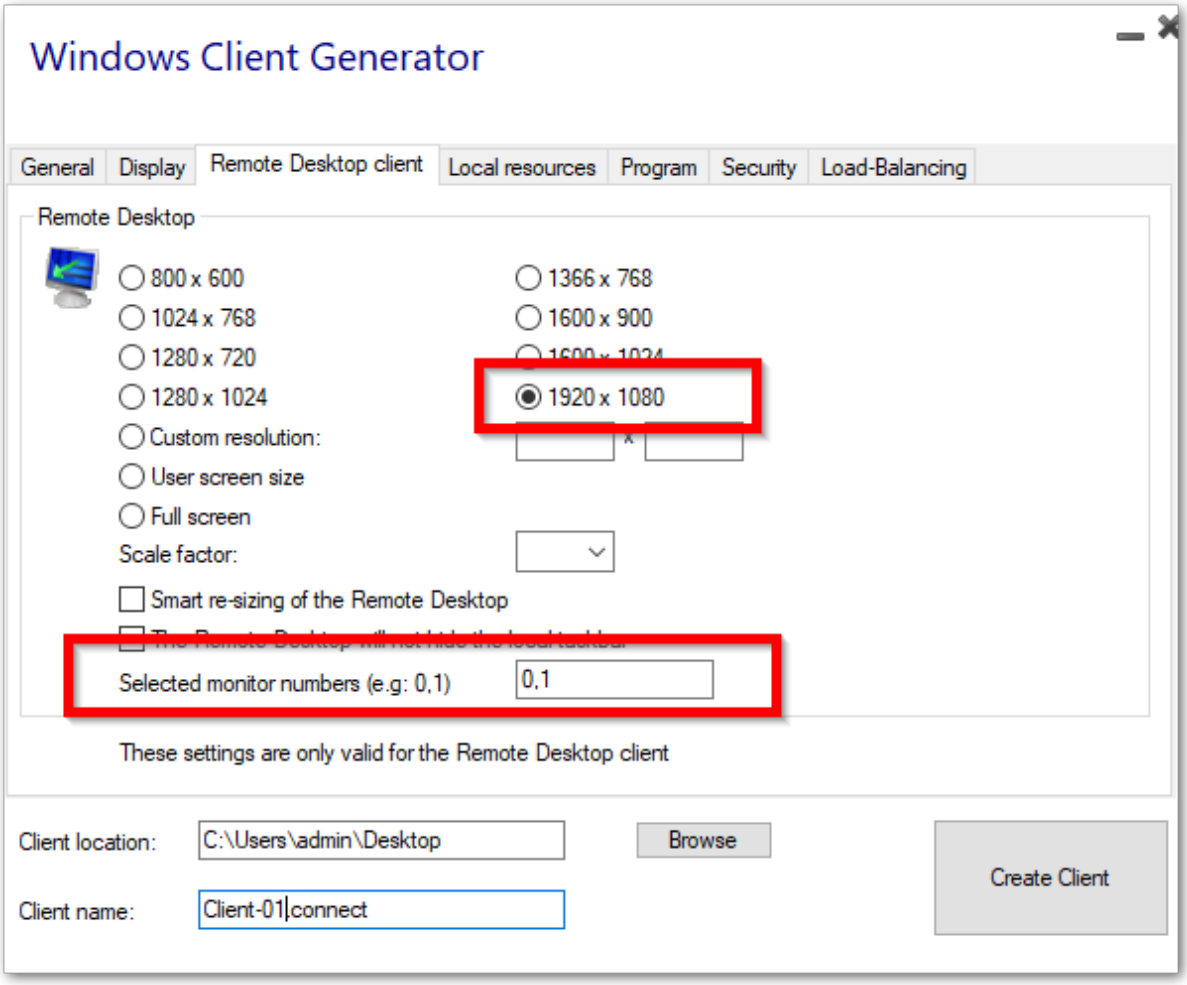


En esta pestaña, puedes cambiar el color y la resolución de pantalla de la sesión.

También puedes adaptar tu sesión para pantallas duales, con o sin extensión. La opción de extensión te permite ampliar tu sesión a través de ambas pantallas.

Puedes permitir el uso de la tecla TAB en la sesión.

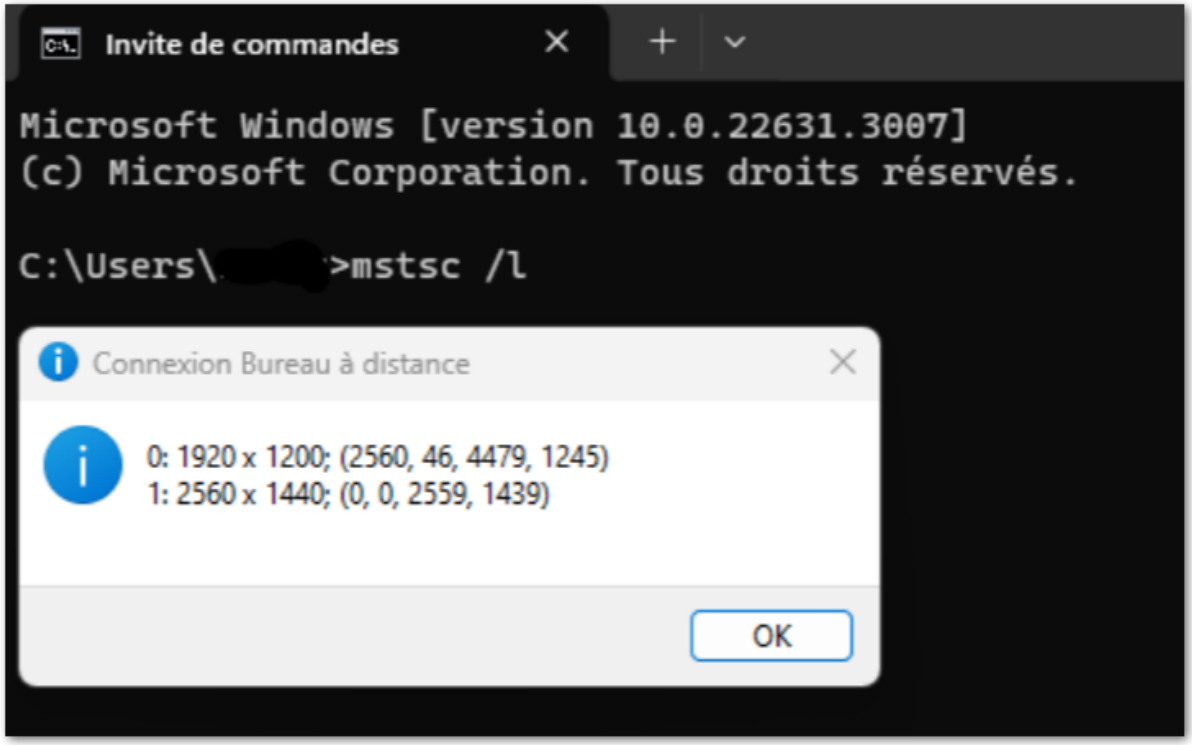
En esta pestaña, puedes elegir qué resolución deseas habilitar para el usuario:



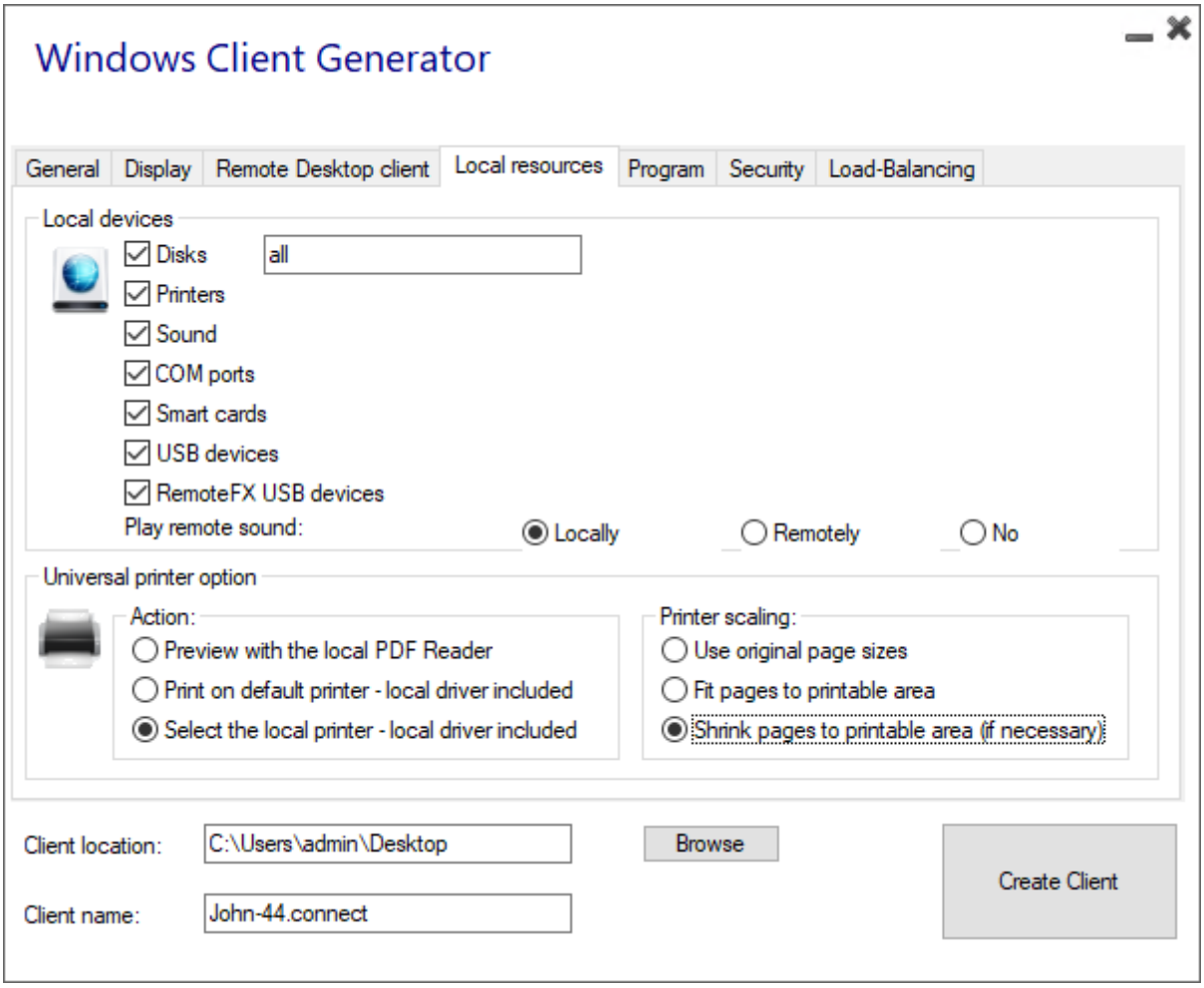
Puedes marcar las casillas para habilitar el ajuste inteligente del Escritorio Remoto, y si deseas que el Escritorio Remoto no oculte ni se superponga a la barra de tareas local.

Opción de selección de pantalla

Esto le permite indicar los monitores que desea utilizar para la sesión RDP. El campo debe llenarse con la lista de números de pantalla a utilizar (separados por una coma, un espacio o un punto y coma).



Para identificar los números de pantalla, simplemente ejecute el comando **mstsc /l**



La pestaña de recursos locales reúne todos los dispositivos que puedes redirigir en tu sesión remota.

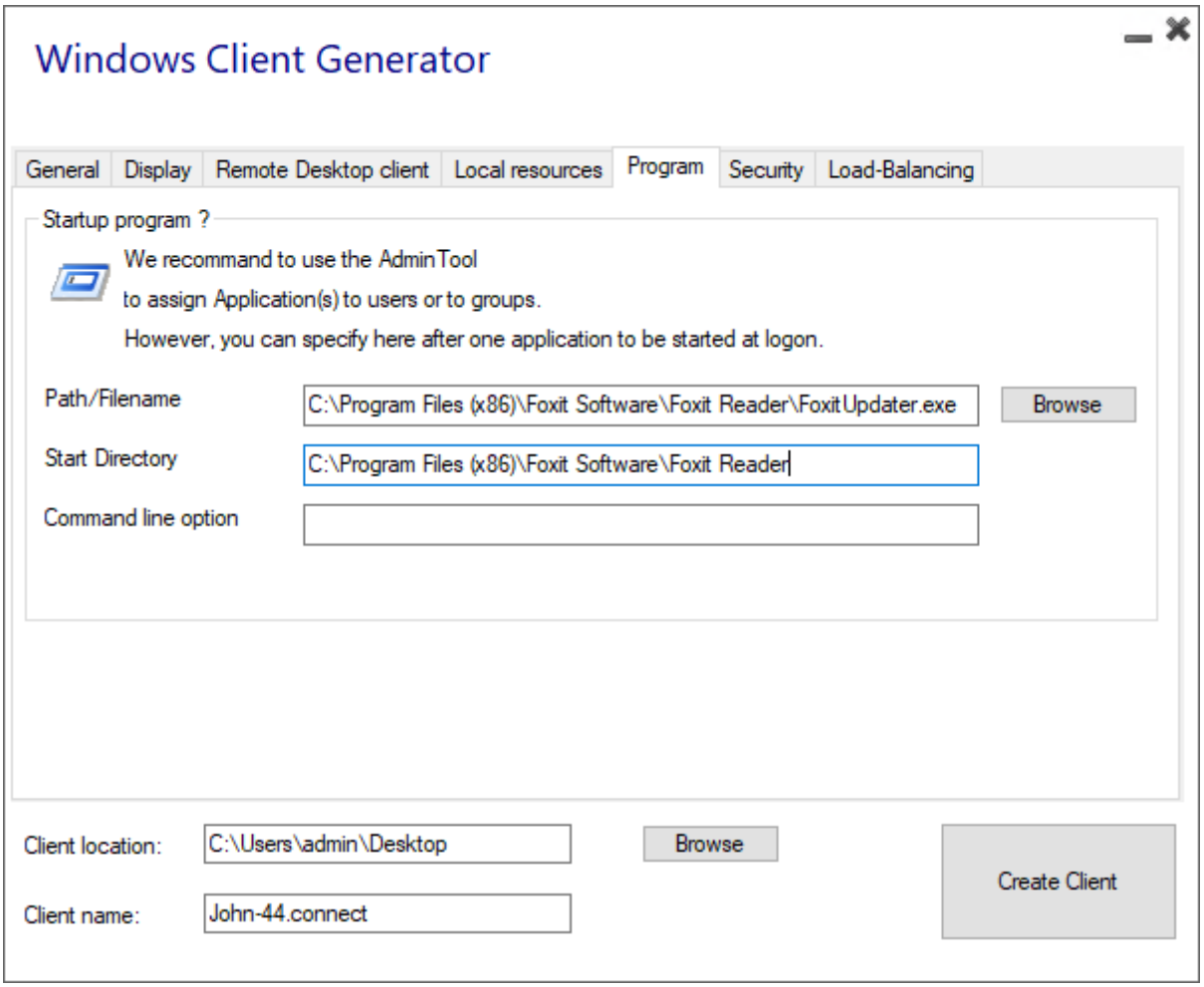
El campo editable junto al **discos** La caja permite especificar qué discos están disponibles en la sesión remota. Solo tienes que separar cada letra de disco (C :, E: …) por una coma. Cuando la caja de discos está marcada y no se especifica ningún disco, todos los discos están incluidos en la sesión remota.

Impresoras corresponden a los puertos LPT, y los puertos COM corresponden a los puertos serie. Desde la versión 11.50 de TSplus, estos dispositivos locales se seleccionan por defecto.

A continuación, puede elegir su opción de impresión, con la impresora universal:

- **Vista previa del lector de PDF local:** El documento se generará como un PDF y el Acrobat Reader local abrirá el archivo. El usuario puede imprimirlo o guardar una copia en su disco duro local.
- **Imprimir en la impresora predeterminada del usuario:** el documento se enviará automáticamente a la impresora predeterminada del usuario (el controlador de impresión local está incluido en el cliente de conexión de TSplus).
- **Seleccionar una impresora local:** El usuario puede seleccionar una de sus impresoras locales (el controlador de impresión local está incluido en el cliente de conexión de TSplus).

Si no tiene un lector de PDF instalado en su máquina, le recomendamos el uso de Foxit Reader.



Puedes establecer una aplicación de inicio a través del Generador de Cliente Portátil y especificar su ruta, directorio y parámetros, desde la versión 11.30.

Sin embargo, le recomendamos que utilice la AdminTool para asignar las aplicaciones deseadas.

TSplus ofrece dos capas adicionales de seguridad física para mantener seguras las conexiones de sus usuarios.

La conexión se puede bloquear al ID de una llave USB, bloqueada a un nombre de computadora, o se pueden usar ambas capas de seguridad simultáneamente.

Opción avanzada de seguridad del cliente

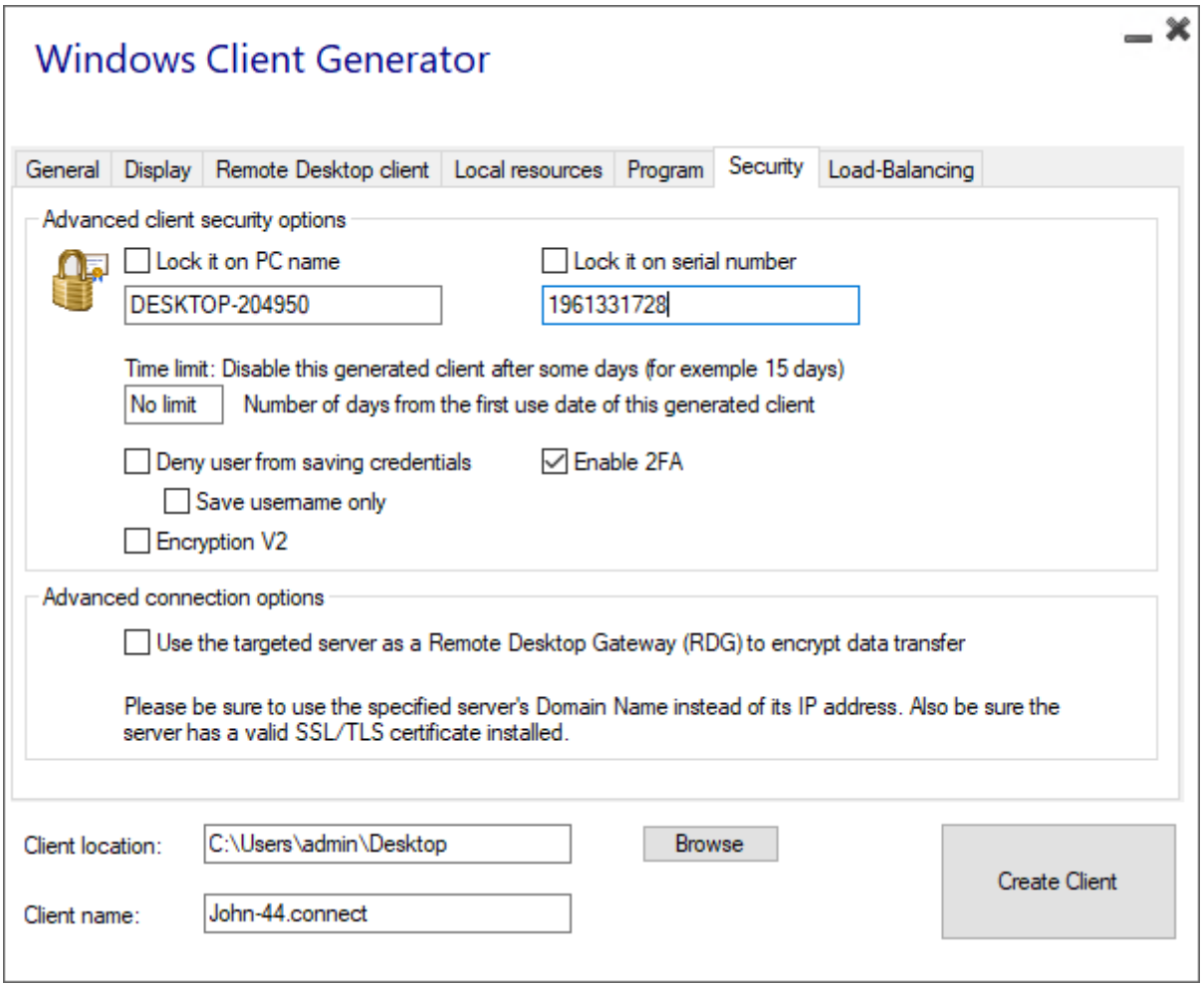
- **Si está bloqueado a una llave USB** el usuario puede iniciar una conexión desde cualquier computadora con Windows que califique insertando la llave USB y utilizando el programa de conexión colocado allí por el administrador.
- **Si está bloqueado a un nombre de computadora** el usuario solo puede conectarse con éxito desde el ordenador cuyo nombre ha sido registrado con el servidor para la conexión del cliente portátil de ese usuario. Si se utilizan ambas opciones de seguridad, el usuario está limitado a conectarse desde su dispositivo específico y solo si la clave USB preconfigurada

correcta está en su lugar.

Para bloquear un cliente de conexión en una llave USB, puede hacerlo copiando el generador de clientes ubicado en: C:\Program Files (x86)\TSplus\Clients\WindowsClient

Ahora haz doble clic en el generador de clientes y verifica el candado en la casilla del número de serie ubicada en la pestaña de seguridad. Una vez hecho esto, puedes eliminar el generador de clientes de la llave USB.

El nuevo cliente de conexión generado se colocará en el escritorio, ¡no olvides copiarlo de nuevo a la llave USB! Puedes eliminar el generador de clientes que copiaste en la llave USB después.



- Puedes definir el **límite de tiempo** desde la fecha de primer uso de un cliente generado al ingresar el valor en el cuadro de límite de tiempo. (que por defecto está configurado en "sin límite").

- Las cajas a continuación le permiten:

- No mostrar la capacidad de guardar credenciales para un cliente generado.
  - Guardar solo el nombre de usuario.
  - Usar cifrado V2.

Soporte para la autenticación de dos factores

El generador de clientes admite **autenticación de dos factores** desde la versión 15.30.3.15. El soporte de autenticación de dos factores también requiere un **Edición Web Móvil o superior** .

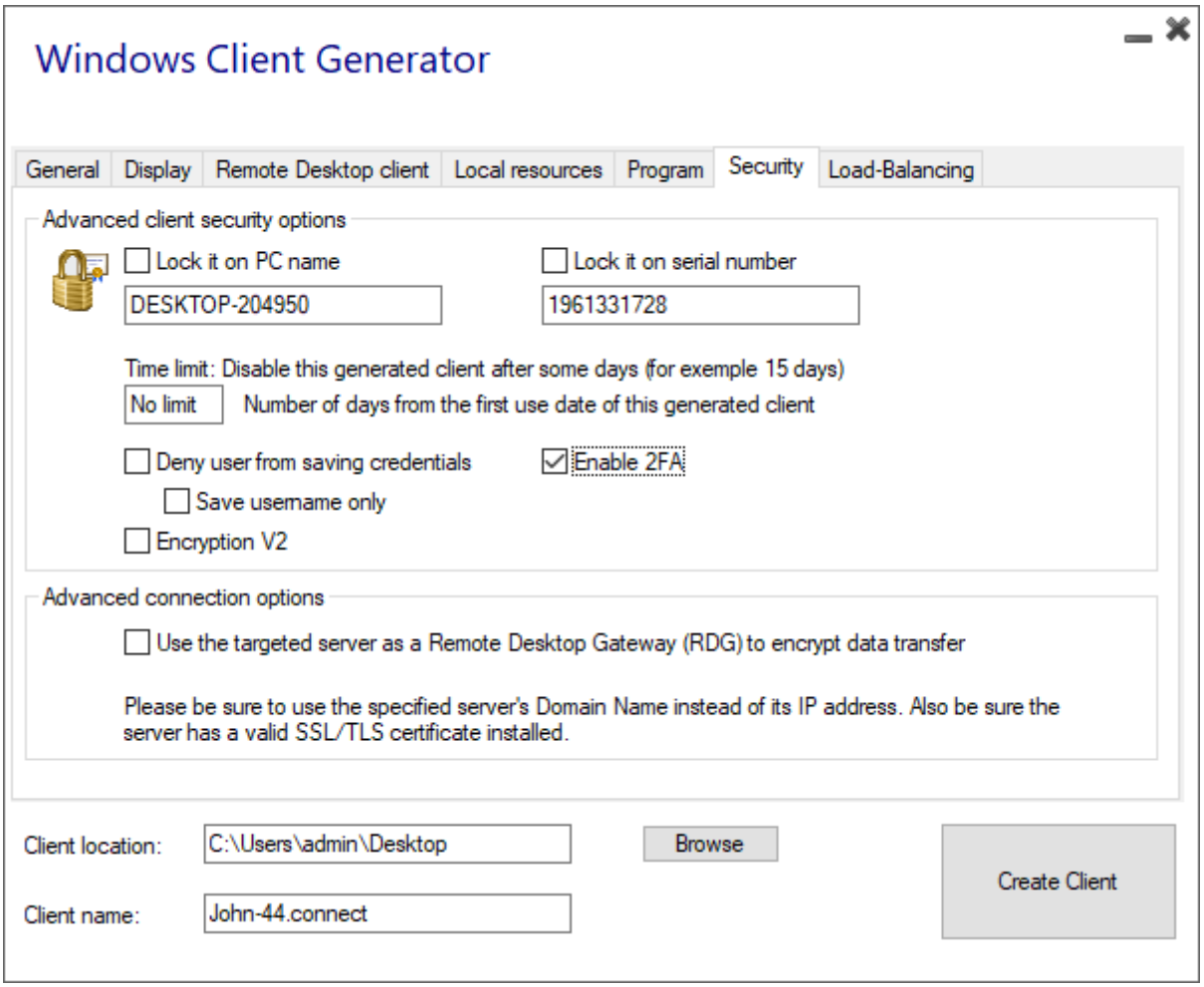
Por favor, consulte a Página de documentación de Autenticación de Dos Factores para obtener más información sobre cómo configurar y habilitar la autenticación de dos factores para usuarios y grupos en su instalación de TSplus Remote Access.

Por favor, tenga en cuenta los siguientes requisitos adicionales para habilitar la autenticación de dos factores para un cliente generado:

- El cliente de conexión valida el código de autenticación contra el portal web utilizando el puerto HTTPS. Por lo tanto, **El portal web debe estar en funcionamiento.** y accesible a través de su puerto HTTPS desde la máquina cliente.
- Si se modifica el puerto HTTPS del portal web, entonces los clientes generados habilitados para la autenticación de dos factores deben generarse nuevamente. Los clientes generados anteriormente no podrán validar ninguna autenticación de dos factores.

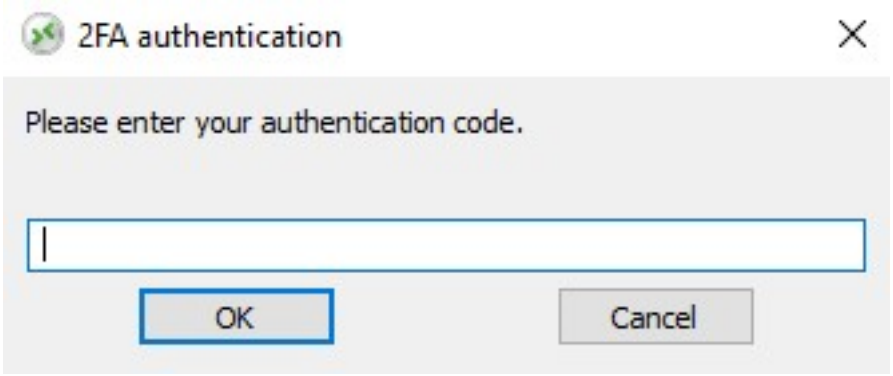
Desde la versión 15.30.3.15, cualquier cliente generado anteriormente y cualquier nuevo cliente generado sin el soporte de 2FA habilitado se comportará de la misma manera que antes. **Si un usuario habilitado para la autenticación de dos factores intenta iniciar sesión utilizando un cliente generado sin soporte explícito para 2FA, se denegará el acceso.** como la autenticación de dos factores no es posible y, por lo tanto, fallará.

Para agregar soporte para la autenticación de dos factores, verifique el **Habilitar 2FA** marque antes de generar su archivo de cliente. Como resultado, se validará la autenticación de dos factores al conectarse al servidor de la aplicación de Remote Access. Si la autenticación de dos factores está habilitada en el servidor de la aplicación y el usuario que se conecta no está configurado, entonces se denegará la conexión.



Ten en cuenta que agregar soporte de 2FA a un cliente generado más tarde no es compatible. Por ejemplo, agregar soporte de 2FA a través de la línea de comandos contra el archivo .connect generado no es compatible.

Una vez que un usuario ha configurado su cuenta en una aplicación de autenticación, podrá conectarse utilizando su contraseña y el código proporcionado por su aplicación de autenticación o por SMS.



Opción de conexión avanzada

Si el servidor objetivo posee un nombre de dominio específico y accesible, así como un certificado SSL/TLS válido instalado, puede habilitar la “Usar el servidor objetivo como un Gateway de Escritorio Remoto (RDG) para cifrar la transferencia de datos”.

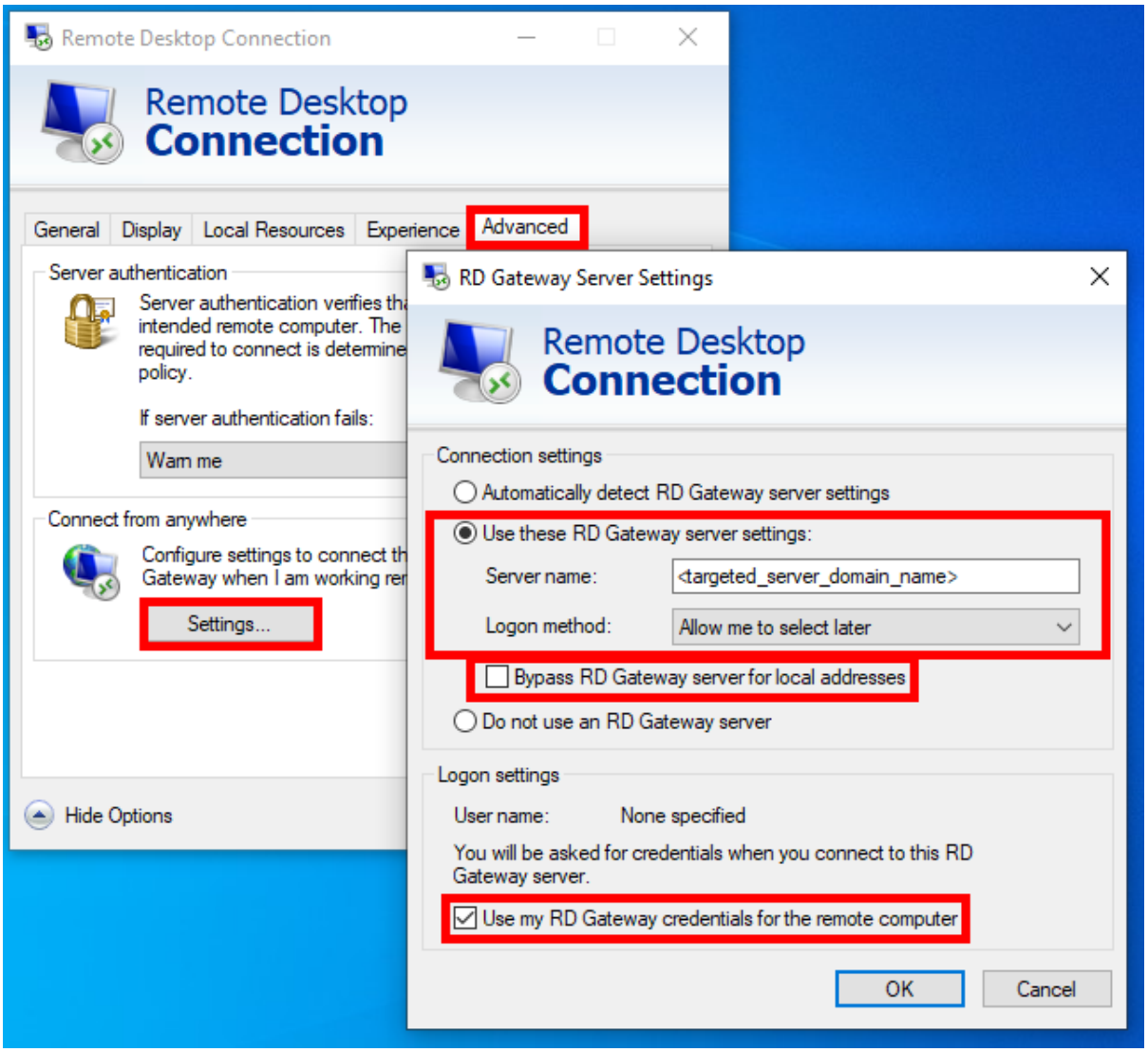
Esta opción hace que la transferencia de datos RDP durante la conexión esté encriptada utilizando encapsulación TLS, lo que la convierte en una alternativa adecuada a cualquier VPN en términos de encriptación de datos.

Utilice mstsc en su lugar para conectarse al RD Gateway

También puede utilizar esta función a través de la configuración de mstsc sin usar un cliente generado si se cumplen los requisitos mencionados anteriormente.

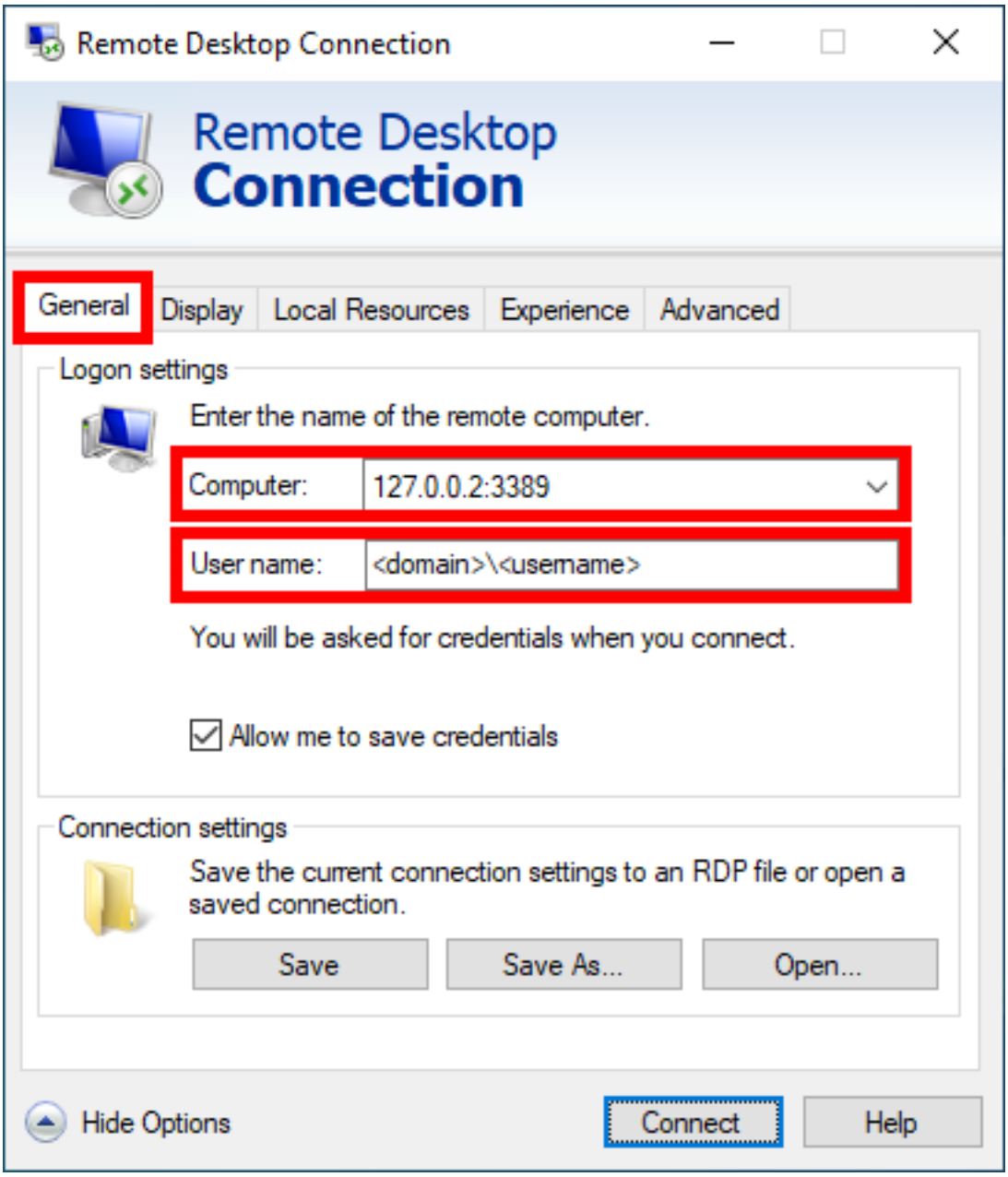
Para hacerlo, ve primero a la pestaña avanzada, luego en la sección "Conectar desde cualquier lugar" haz clic en "Configuración" y configura el Gateway de Escritorio Remoto en:

- Marcar la opción "Usar estas configuraciones del servidor RD Gateway"
- Reemplazando el nombre del servidor con el nombre de dominio del servidor objetivo (sin https://)
- Seleccionando el método de inicio de sesión “Permitir que seleccione más tarde”
- Desmarcando la opción "Omitir el servidor RD Gateway para direcciones locales"
- Marcar la opción "Usar mis credenciales de RD Gateway para el equipo remoto"
- Haciendo clic en "Aceptar" para guardar estos ajustes



Luego, ve a la pestaña "General" y:

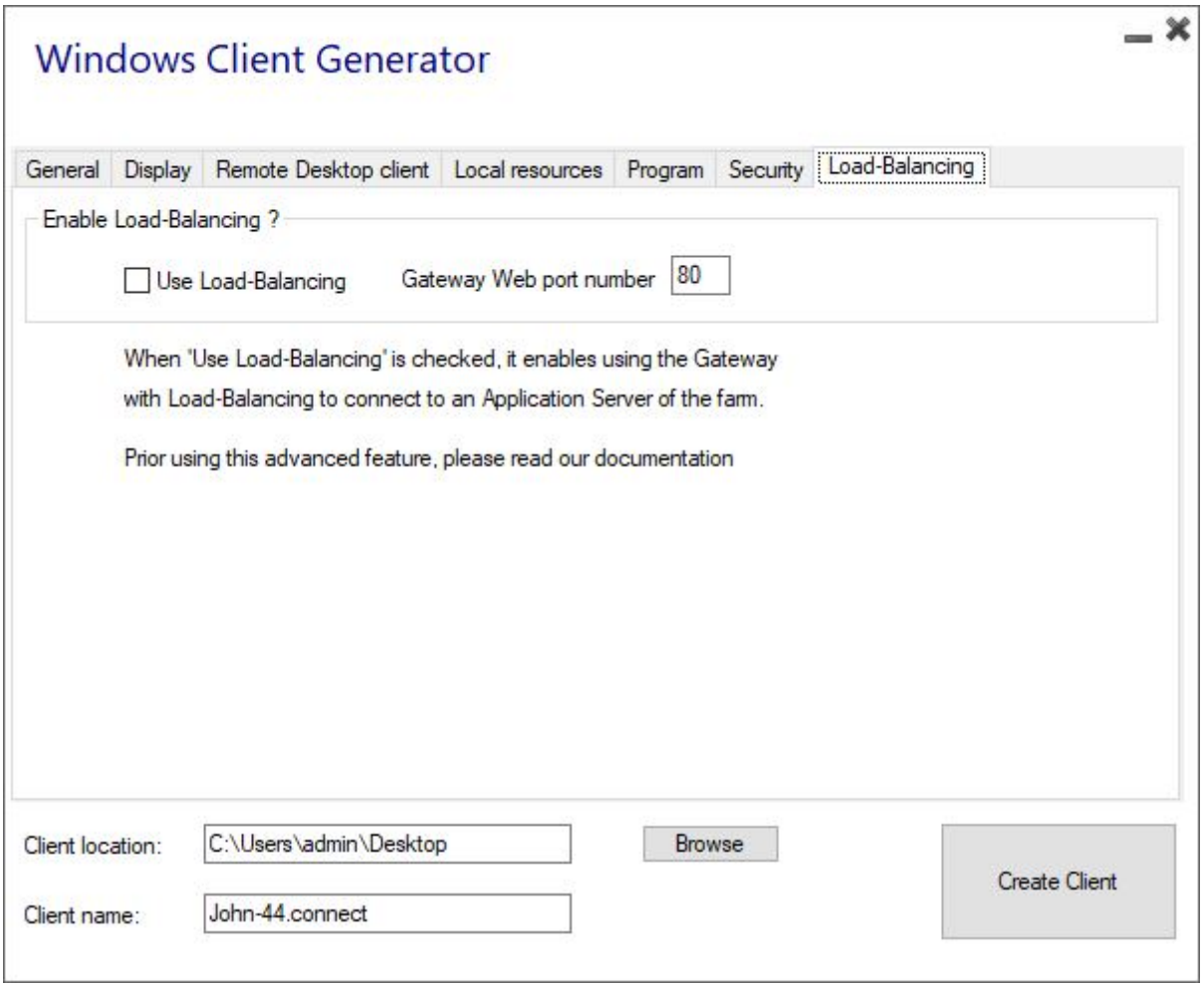
- Reemplace el nombre de la computadora con “127.0.0.2:3389” y cambie el puerto “3389” si está utilizando uno diferente.
- Reemplace el nombre de usuario con el nombre de usuario con el que desea conectarse (**importante: especificar el dominio es obligatorio**)
- Haga clic en "Conectar"

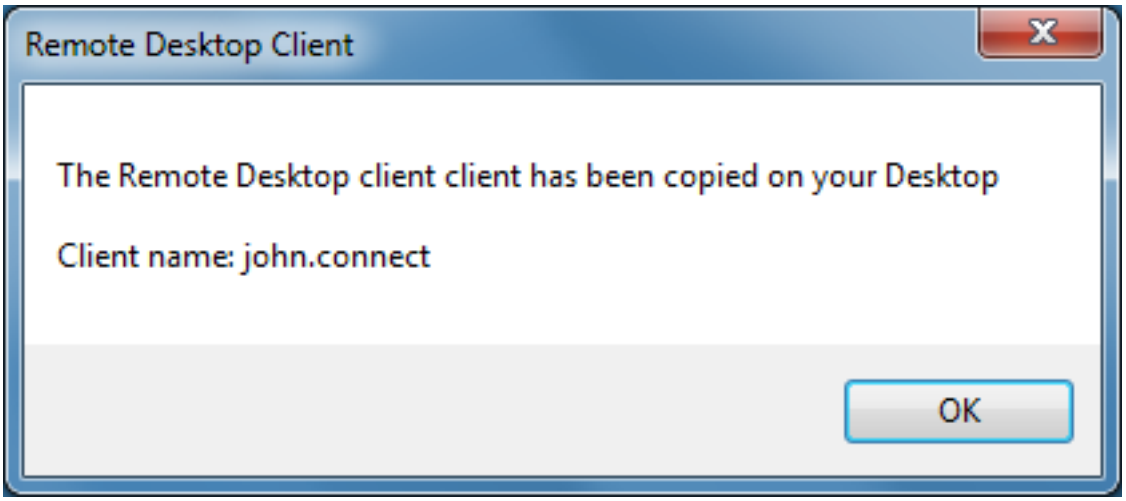


También puede habilitar el balanceo de carga para conectarse a un servidor de su granja.

No marque la casilla "Usar balanceo de carga" si no activó la función de balanceo de carga en su servidor.

Deberá ingresar el puerto web del Gateway, que debe ser el mismo que el puerto web predeterminado utilizado en todos los servidores de su granja.





La personalización del cliente es posible. Consulte la documentación correspondiente en cómo modificar el icono del cliente y editar o eliminar sus parámetros .

Puede habilitar los registros para el Cliente de Conexión en el lado del cliente agregando la siguiente clave del registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\ConnectionClient “Debug”=“true”

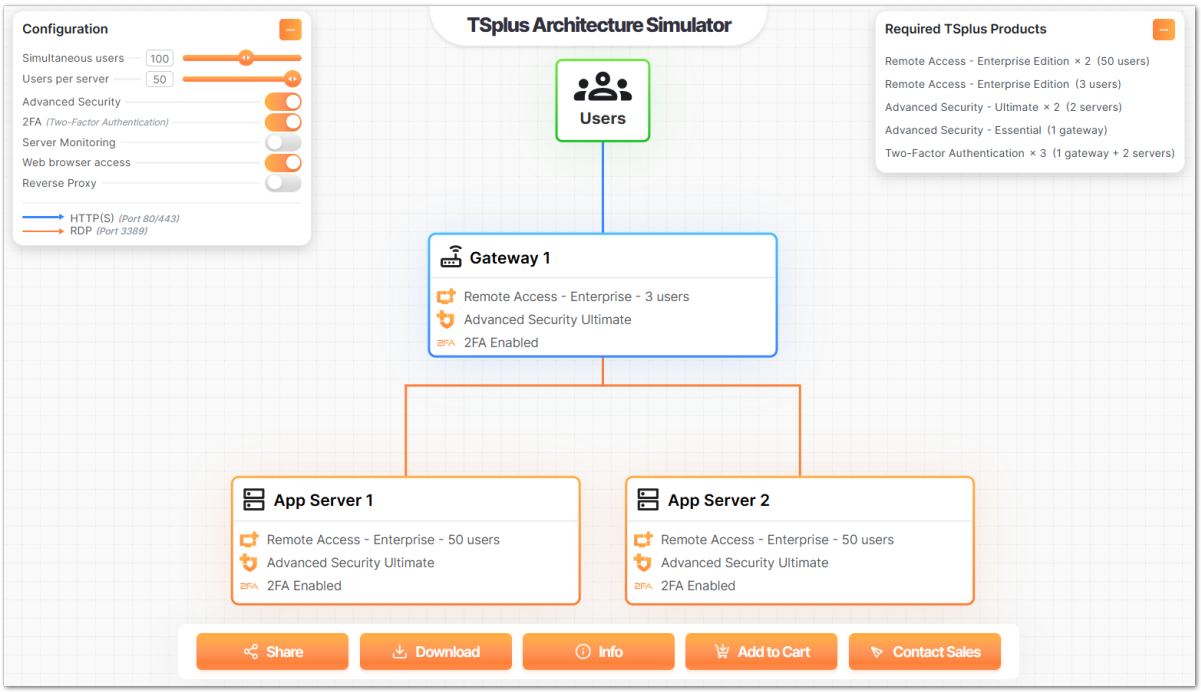
Los registros se encuentran en C:\Users RDP6\logs directory si la instalación es por usuario o en C:\Program Files (x86)\Connection Client\RDP6\logs directory si la instalación es para todos los usuarios.

Requisitos de TSplus Remote Access

Simulador de Arquitectura

Configura tu arquitectura en línea para ayudarte a elegir nuestro software y complementos.

TSplus Architecture Simulator



1. Hardware

Requisitos mínimos del servidor de TSplus Remote Access:

Número de usuarios	Windows 2008 a 2025 o 7 a 11 Pro
3 - 5	I5 o superior Un CPU 2 GHZ Mínimo: 4 GB de RAM Recomendado: 8 GB de RAM

10	I5 o superior Un CPU 2 GHZ Mínimo: 8 GB de RAM Recomendado: 16 GB de RAM
25	Un CPU I7 o Xeon Mínimo: 16 GB de RAM Recomendado: 32 GB de RAM
50 y más	32 GB Dual CPU - Disco SSD dedicado al sistema Mínimo: 32 GB de RAM Recomendado: 64 GB de RAM

Recomendamos utilizar una CPU que tenga menos de diez años.

En cuanto al uso de RAM, dependerá del sistema operativo instalado, el número de usuarios concurrentes y las aplicaciones que se les asignen.

Cada servidor (físico o virtual) puede manejar potencialmente hasta 50 usuarios concurrentes. Para más de 50 sesiones concurrentes, recomendamos utilizar un conjunto de servidores con la función de Balanceo de Carga disponible en TSplus Remote Access Enterprise Edition.

Nota: Las especificaciones exactas de su hardware dependerán de qué tipo de recursos (CPU/RAM/Disco) consumen sus aplicaciones.

Solo **x86 y x64** se admiten arquitecturas.
ARM32 y ARM64 las arquitecturas no son compatibles.

2. Sistema operativo

Su hardware debe utilizar uno de los sistemas operativos a continuación:

- Windows **7 Pro**
- Windows **8/8.1 Pro**
- Windows **10 Pro**
- Windows **11 Pro**
- Windows **Server 2008 SP2/Small Business Server SP2 o 2008 R2 SP1**
- Windows **Server 2012 o 2012 R2**
- Windows **Server 2016**
- Windows **Servidor 2019**
- Windows **Server 2022**
- Windows **Servidor 2025**

Ambas arquitecturas de 32 y 64 bits son compatibles.

El marco requerido es **.NET versión 4.7.2** para todas las versiones de Windows compatibles.

versión de acceso remoto	Versión mínima de Windows
19, LTS 18, LTS 17, LTS 16, LTS 15	Windows 7 Service Pack 1 Windows Server 2008 R2 Service Pack 1
LTS 14	Windows Vista Windows Server 2008

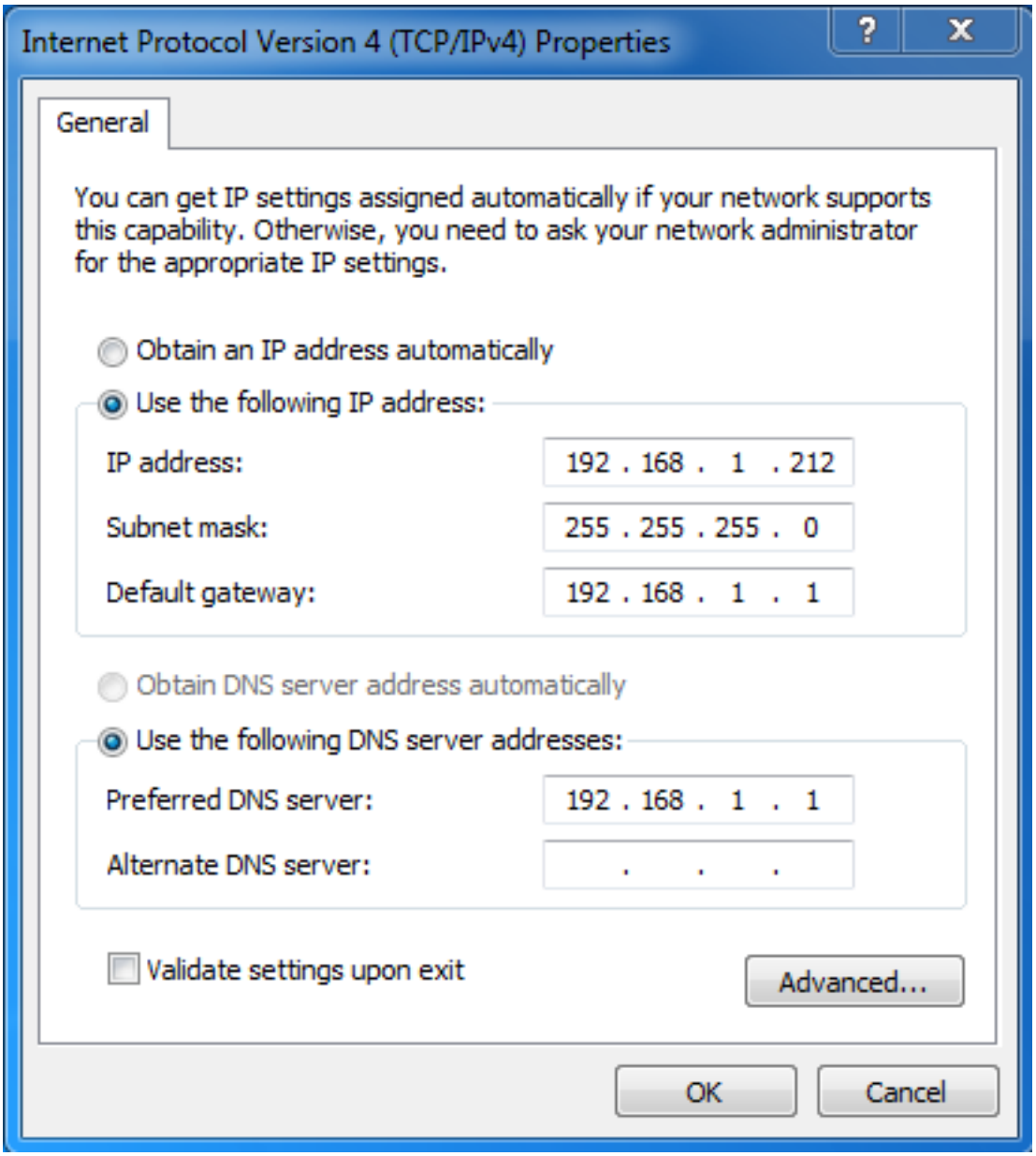
- Si instala Remote Access en un sistema operativo Windows Server, asegúrese de que los roles de RDS/Terminal Services y RDS/Terminal Services Licensing no estén instalados antes de instalar TSplus Remote Access.

Si estos roles están actualmente instalados, elimínalos y reinicia.

- Las ediciones de Windows Home no son compatibles.
- En Windows Server 2016, se permiten un máximo de 15 sesiones para acceso a Escritorio Remoto.
- Windows Server 2016, 2019, 2022 Essentials Edition no es compatible ni recomendado para usar TSplus Remote Access.
- TSplus Remote Access servidor web integrado requiere **Java OpenJDK 17 o superior.** .

3. Parámetros de red

El servidor de acceso remoto debe tener una dirección IP privada estática:



Acceso remoto (desde una red de área amplia - WAN)

- Se recomienda una conexión a internet de banda ancha, así como una dirección IP pública estática. Si no tiene una dirección IP estática, considere utilizar un servicio de DNS dinámico como
- El puerto TCP RDP (por defecto 3389) debe estar abierto en ambas direcciones en su firewall.

3. Seguridad

Desde principios de 2024,
TSplus ha actualizado su mecanismo de generación automática de certificados SSL/TLS para alinearse con el cambio en la cadena de confianza de Let's Encrypt: el **DST Root CA X3** root ha sido reemplazado por **ISRG Root X1** .

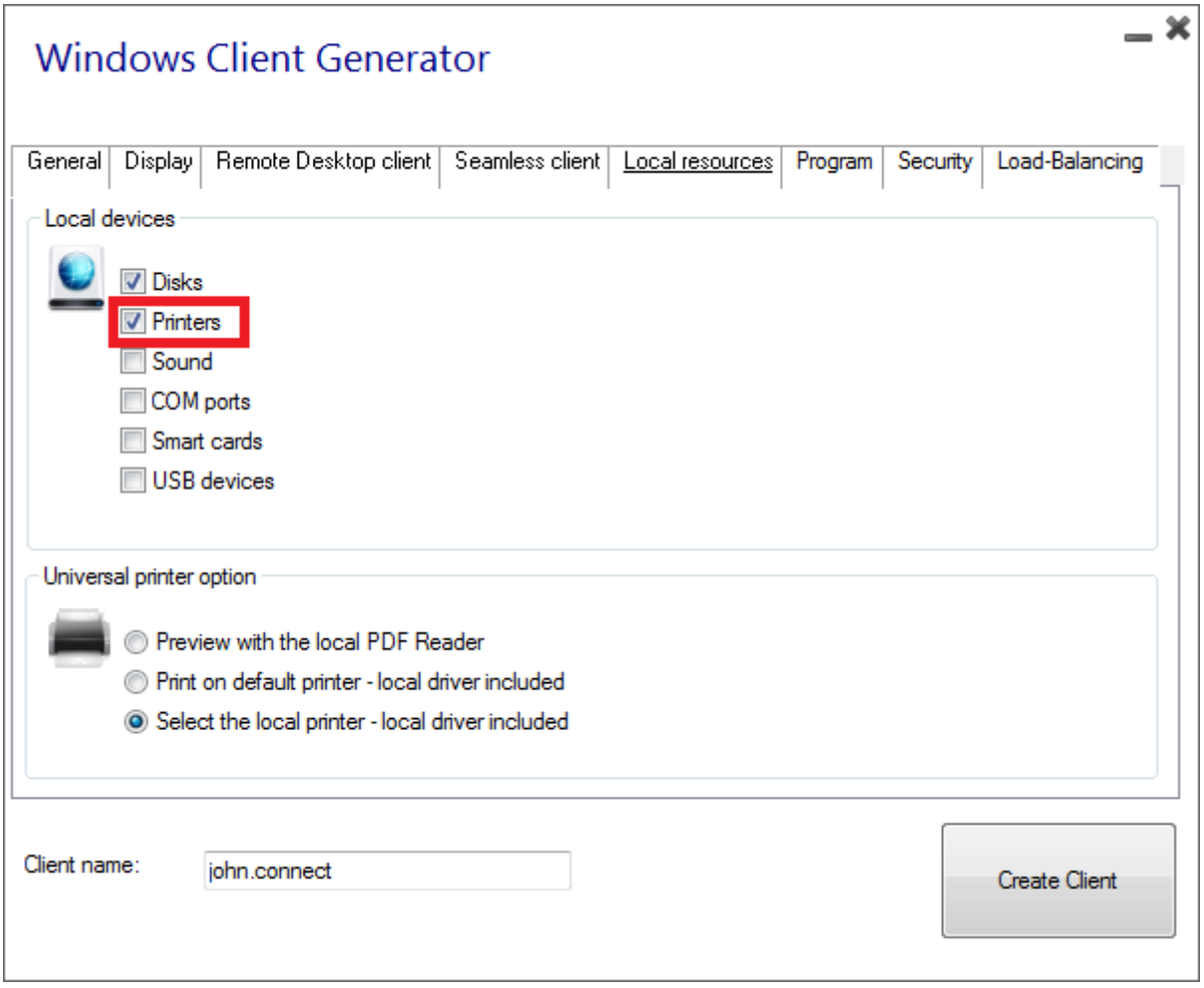
Si un cliente o estación de trabajo no reconoce el nuevo certificado, puede ser necesario agregar **ISRG Root X1** al almacén de certificados de confianza de Windows.

TSplus funciona con certificados comodín y admite el protocolo TLS para conexiones remotas seguras.

Impresión con la función de mapeo de impresora RDP estándar

Esto es comúnmente utilizado por usuarios de Remote Desktop y es equivalente a lo que tendrías con Microsoft Terminal Services.

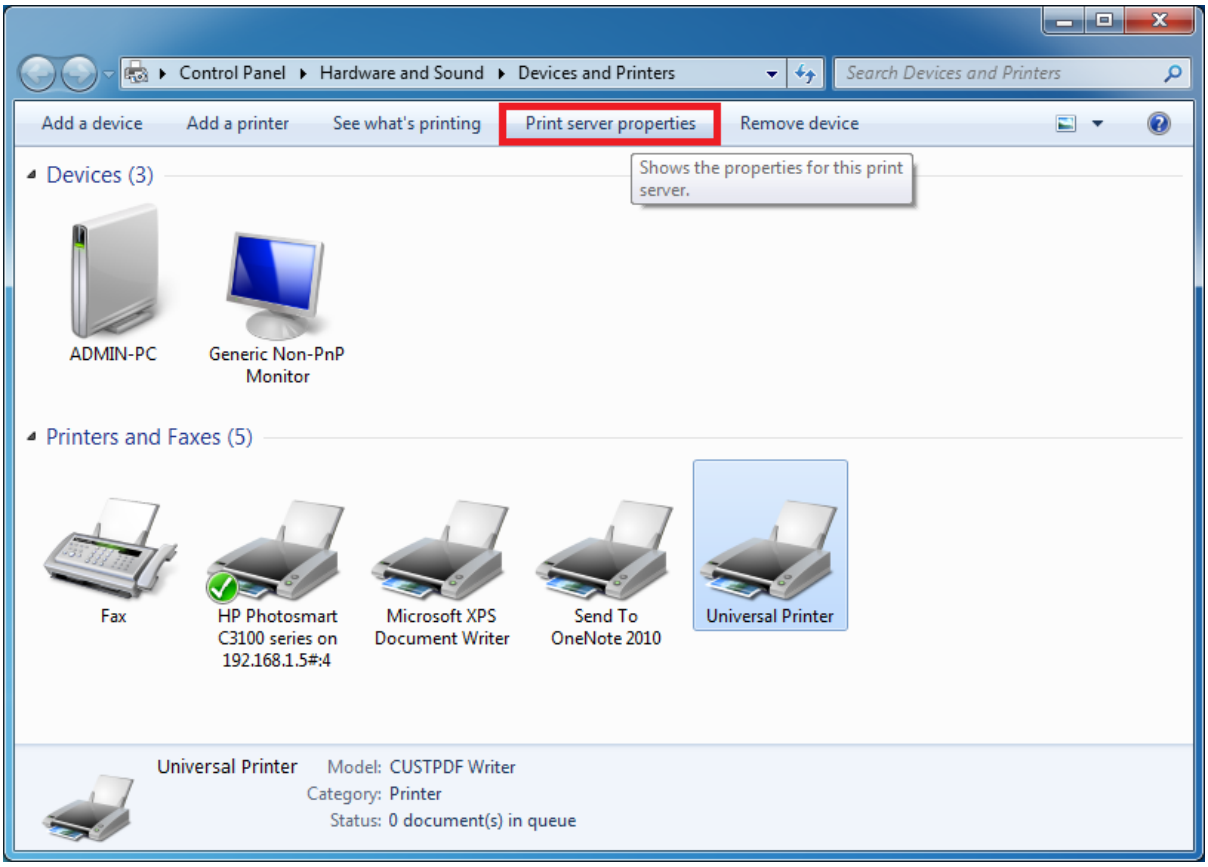
Si planeas usar impresoras exóticas, asegúrate de marcar la casilla de impresoras en la pestaña de recursos locales del generador de clientes.



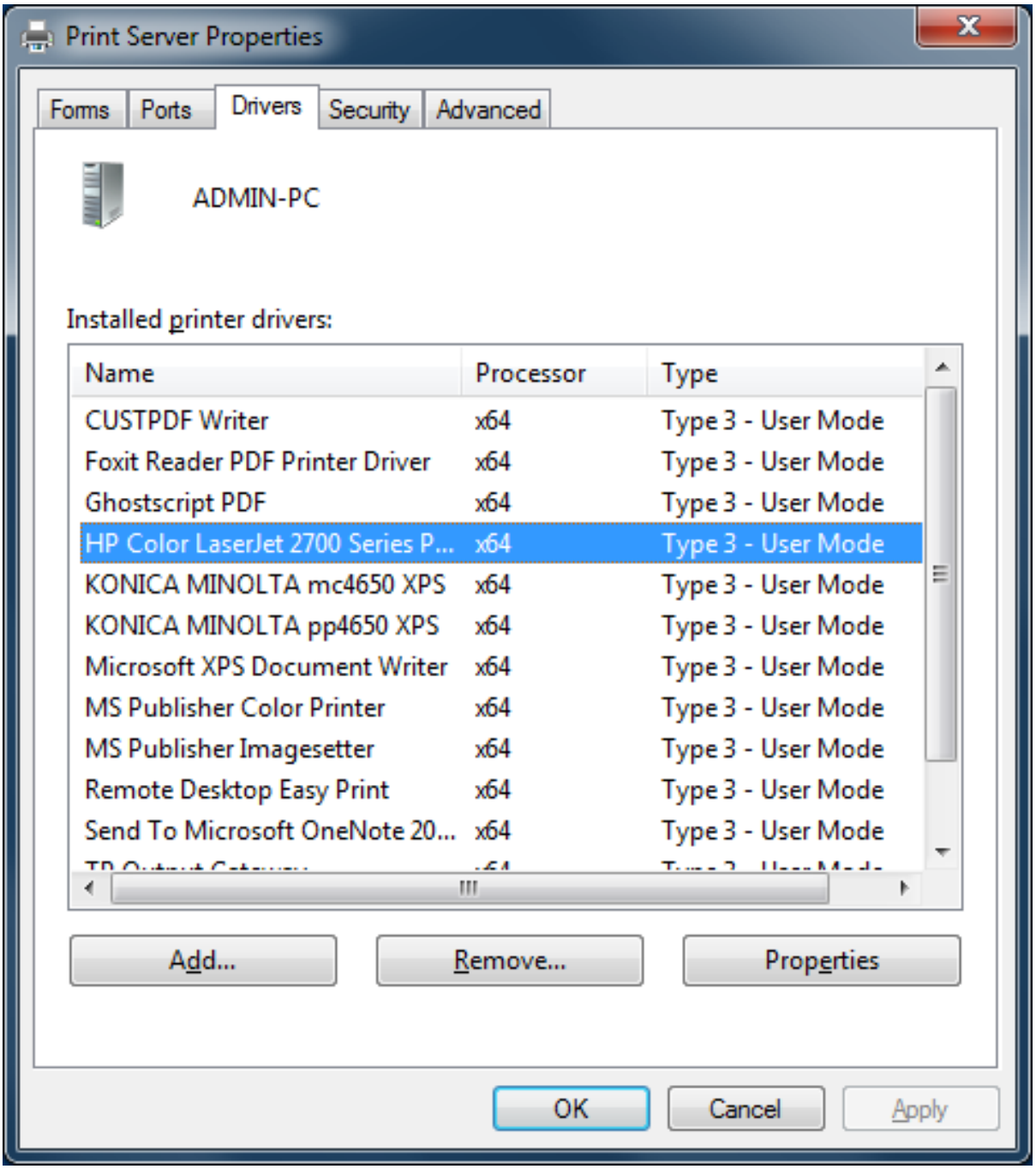
La mayoría de las veces, será necesario que instales la misma versión de los controladores de la impresora tanto en el cliente como en el servidor para que funcione correctamente.

Esto significa que si su servidor es Windows 2008 de 64 bits y sus computadoras cliente están ejecutando Windows XP de 32 bits, necesitará instalar los controladores de impresora de XP de 32 bits en el servidor.

Haga clic en el menú de inicio, luego en Dispositivos e impresoras. Haga clic en cualquier impresora para mostrar el botón de propiedades del servidor de impresión en la parte superior de la ventana.



Una vez en las Propiedades del Servidor de Impresión, haga clic en la pestaña Controlador para agregar manualmente su controlador de cliente. (En este caso, estamos instalando el controlador de 32 bits de Windows XP)



También puede instalar directamente los controladores de su impresora utilizando la información y los controladores del sitio web del fabricante de la impresora.

- Se recomienda consultar el manual de hardware para un procedimiento de instalación en un entorno de servidor terminal.
- Si está utilizando impresoras USB, asegúrese de haber actualizado el protocolo RDP de su computadora cliente a la versión 6 de RDP o superior para garantizar la máxima compatibilidad con las impresoras redirigidas.

Para obtener los mejores resultados, se recomienda no utilizar impresoras USB. La compatibilidad y la fiabilidad mejoran al usar impresoras COM o LPT.

Algunas impresoras exóticas, como las impresoras de etiquetas o de recibos, pueden no ser

adecuadas para ser redirigidas en una sesión de TSplus, siempre debes consultar con el fabricante de tu hardware sobre la compatibilidad y los procedimientos de instalación en un entorno de RDS o servidor terminal, que en este caso es muy similar a TSplus.

TSplus Remote Access v19: Guía de inicio rápido

Requisitos :

En el servidor :

- **OS:** Microsoft Windows versiones 7 a 11 o Windows Server 2008R2 a 2025 con al menos 2GB de RAM.
- TSplus no admite la instalación de Remote Access en las Ediciones Home de Windows.
- El sistema operativo **debe** estar en la unidad C:
- Java Runtime Environment. Si Java no está instalado, Remote Access instalará OpenJDK durante la configuración.
- Si está instalando Remote Access en un sistema operativo Windows Server, asegúrese de que los roles de RDS/Servicios de Terminal y de licencias de RDS/Servicios de Terminal estén **no instalado** antes de instalar TSplus Remote Access.
- Su servidor de Remote Access debe tener una dirección IP privada estática.
- Para el acceso externo, su servidor debe tener una dirección IP pública estática o un proveedor de DNS dinámico.
- TSplus Remote Access servidor web integrado requiere **Java OpenJDK 17 o superior.** .

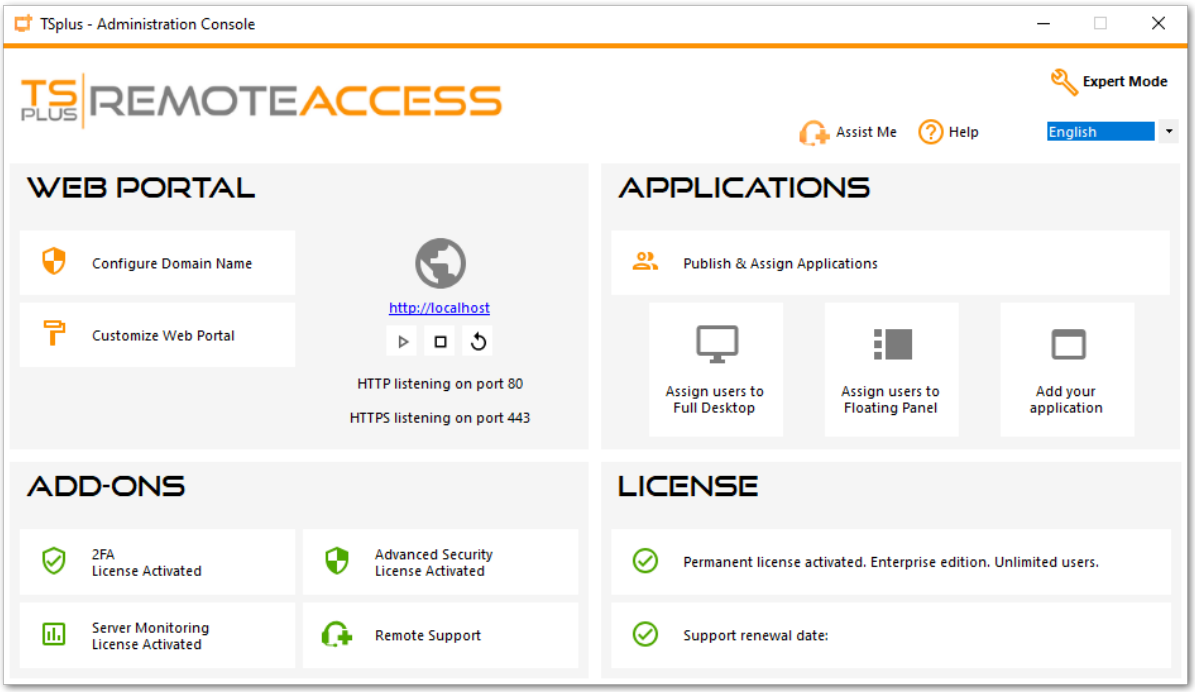
En el Cliente :

- **OS:** Las versiones de Microsoft Windows 7 a 11 son totalmente compatibles.
- Para MacOS, puedes usar cualquier cliente RDP para Mac o el cliente HTML5 de TSplus.
- Para Linux, puedes usar Rdesktop o el cliente HTML5 de TSplus.
- Entorno de Ejecución de Java.
- Un lector de PDF (ejemplo: Foxit Reader o Acrobat DC)

Para obtener más detalles sobre los requisitos previos, consulte la documentación

Nota:

A partir de la versión 15 de Remote Access, la consola de administración ha cambiado su apariencia. **Modo Lite** y un **Modo Experto** se han introducido. Los administradores pueden alternar entre los dos estilos de interfaz haciendo clic en el botón en la esquina superior derecha de la Consola de Administración.



Paso 1: Instalación.

Nota:

La versión de prueba de Remote Access es la edición Enterprise completamente funcional. Está licenciada para hasta 5 usuarios concurrentes por un período de 15 días.

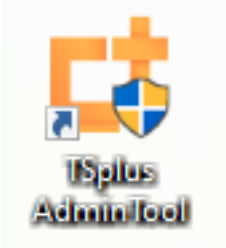
Instalar TSplus Remote Access es un proceso fácil. Simplemente descárgalo desde nuestro sitio web, ejecuta el programa Setup-TSplus.exe.

Los archivos se descomprimen y se copian en:

- C:\Program Files\TSplus (sistemas de 32 bits)
- C:\Program Files(x86)\TSplus (sistemas de 64 bits).

Una vez que la instalación esté completa, el instalador le pedirá que reinicie.

Después del reinicio, verás 2 nuevos íconos en tu Escritorio:



El AdminTool es lo que necesitas para usar Remote Access.

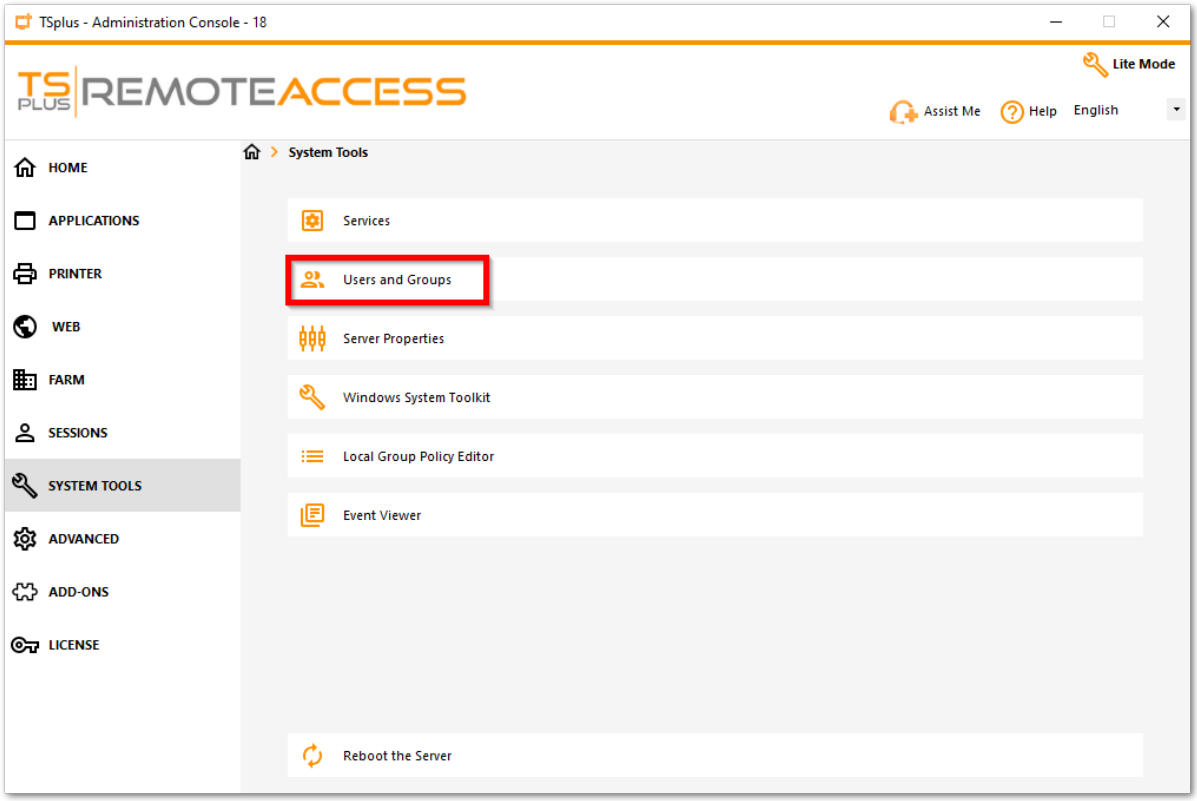


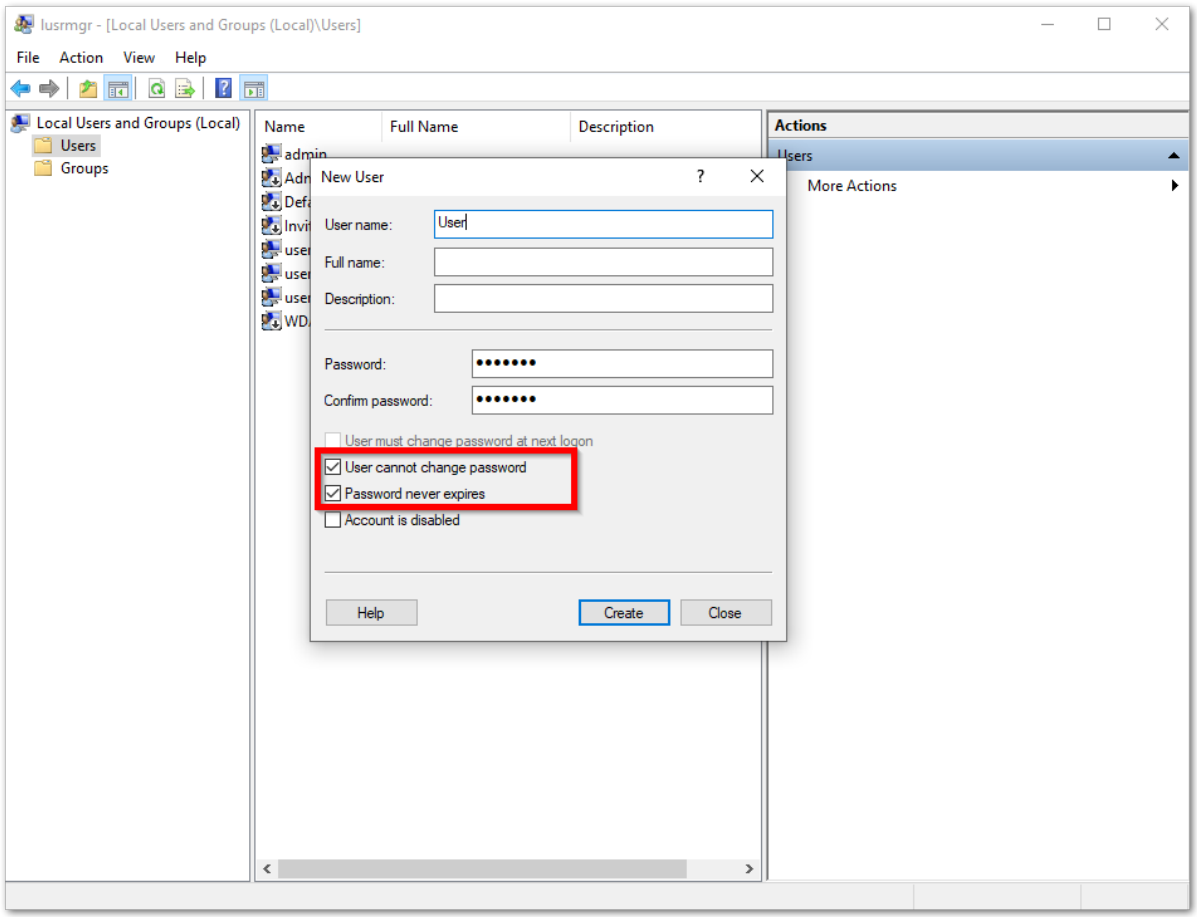
El Generador de Clientes Portátiles se utiliza para crear clientes de conexión de Remote Access para sus usuarios.

Ver la documentación para obtener instrucciones completas de instalación.

Paso 2: Creando usuarios.

Después del reinicio, el servidor de Remote Access está casi listo para funcionar. Ahora crearemos usuarios. Abre el AdminTool para comenzar. Luego ve a la pestaña de Herramientas del sistema y haz clic en "Usuarios y grupos". Esto te llevará a la ventana de Usuarios y grupos locales.





Cada usuario debe tener un nombre de usuario Y una contraseña. Al crear usuarios, tenga en cuenta la casilla etiquetada como "El usuario debe cambiar la contraseña en el próximo inicio de

sesión". Si no desea que sus usuarios cambien su contraseña durante el primer inicio de sesión, desmarque esta casilla y marque "La contraseña nunca expira" o "El usuario no puede cambiar la contraseña".

Paso 3: Seleccione el cliente más adecuado para sus necesidades.

Remote Access es compatible con el Protocolo de Escritorio Remoto de Windows. Cualquier usuario puede conectarse localmente o de forma remota con un cliente estándar de Conexión de Escritorio Remoto (mstsc.exe) o cualquier cliente compatible con RDP. Para beneficiarse completamente de las funciones avanzadas en Remote Access (RemoteApp, Impresora Universal…) puede utilizar un cliente generado o el Portal Web de Remote Access.

Remote Access es una solución muy flexible y ofrece múltiples formas de abrir una sesión:

- **Conexión clásica de escritorio remoto** MSTSC.EXE.
- **Cliente RDP portátil de TSplus** que mostrará un entorno en ventana para su conexión remota que puede minimizar en la barra de tareas de Windows.
- **cliente MS RemoteAPP** que mostrará la aplicación utilizando el MS RemoteApp nativo.
- **cliente de Windows** sobre el Portal Web de TSplus.
- **cliente HTML5** sobre el Portal Web de TSplus.

Estos clientes brindan al usuario la siguiente experiencia:

Con Conexión de Escritorio Remoto (mstsc.exe)

- **Conexión** La conexión es muy estándar. La Impresora Universal no es compatible con este tipo de conexión.

- **Mostrar** Los usuarios verán su sesión dentro de una ventana de Remote Desktop. Este escritorio muestra el contenido de la carpeta de escritorio del usuario.

  Si el administrador ha asignado aplicaciones específicas con el AdminTool, solo se mostrarán estas aplicaciones (sin barra de tareas, sin escritorio).

TSplus cliente generado por RDP .

Esta es una solución única de TSplus, permite a los usuarios locales y remotos conectarse utilizando un solo programa dedicado.

Incluye el programa de conexión, la función avanzada de impresión universal, portabilidad con un alto nivel de seguridad mientras se mantiene muy simple para los usuarios.

Para obtener más información sobre el uso del Generador de Clientes de TSplus, consulte esta documentación

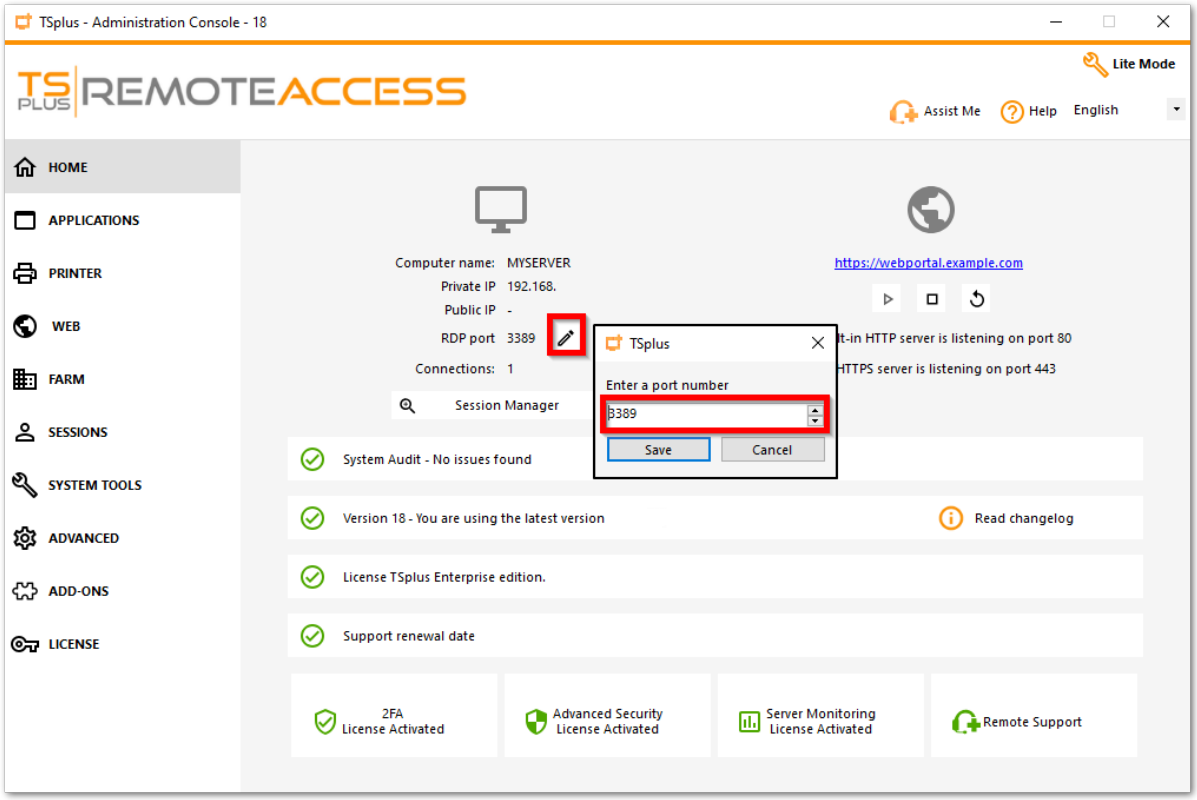
El Cliente generado por TSplus RemoteApp .

Las aplicaciones remotas se verán y comportarán como una aplicación local. En lugar de una ventana clásica de Escritorio Remoto, podrás alternar entre tus aplicaciones locales y remotas sin tener que minimizar una ventana de Escritorio Remoto.

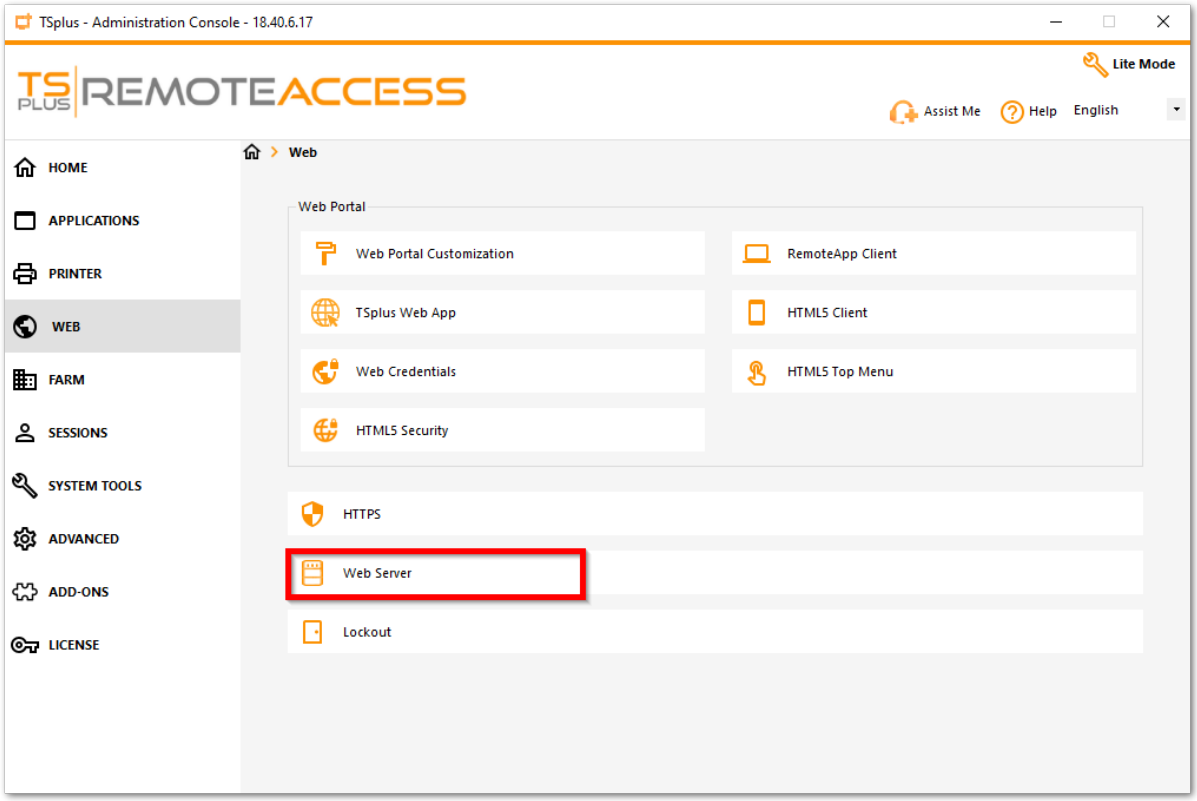
Para más información sobre estos clientes, consulte esta documentación .

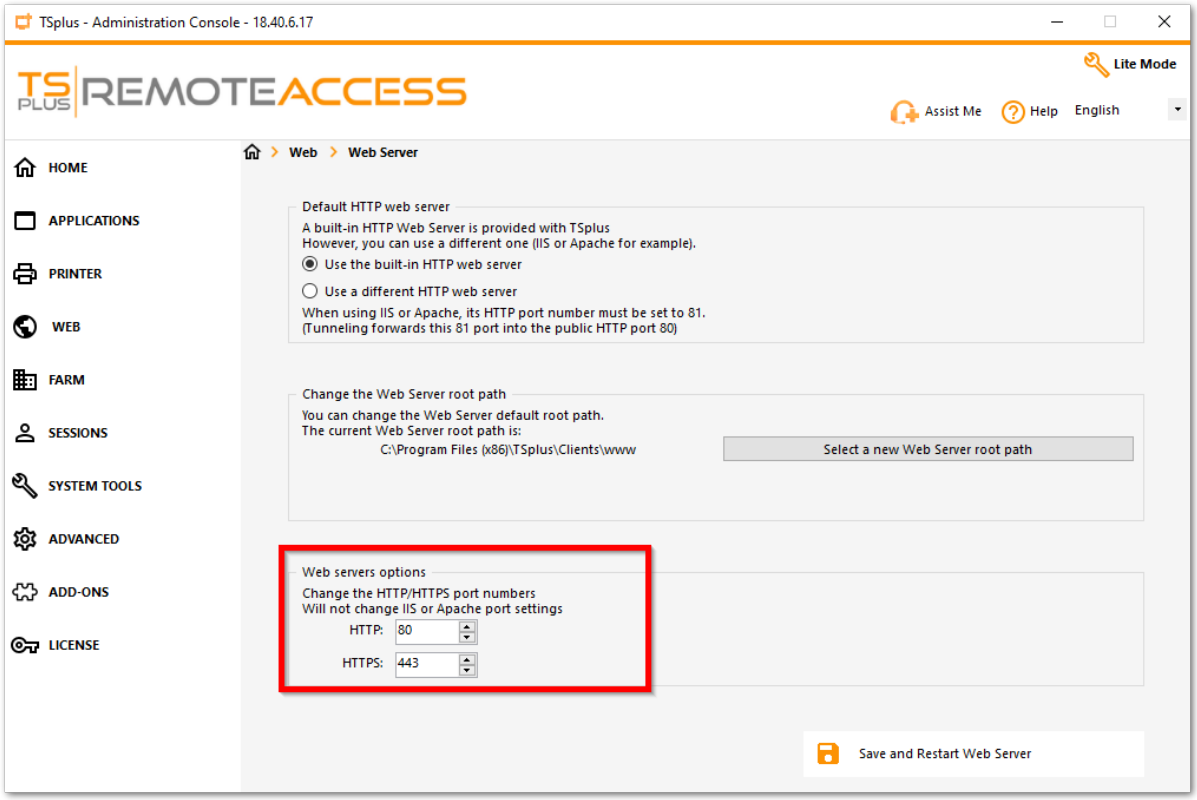
Accediendo a su servidor TSplus Remote Access desde una ubicación remota

Para acceder a su servidor Remote Access desde fuera de su red local, deberá crear una regla de reenvío de puertos o redirección de puertos de los puertos 3389/80/443, dependiendo de su método de conexión preferido. Puede cambiar el puerto RDP en la pestaña Inicio:



Los puertos 80/443 se pueden cambiar en la pestaña del Servidor Web:



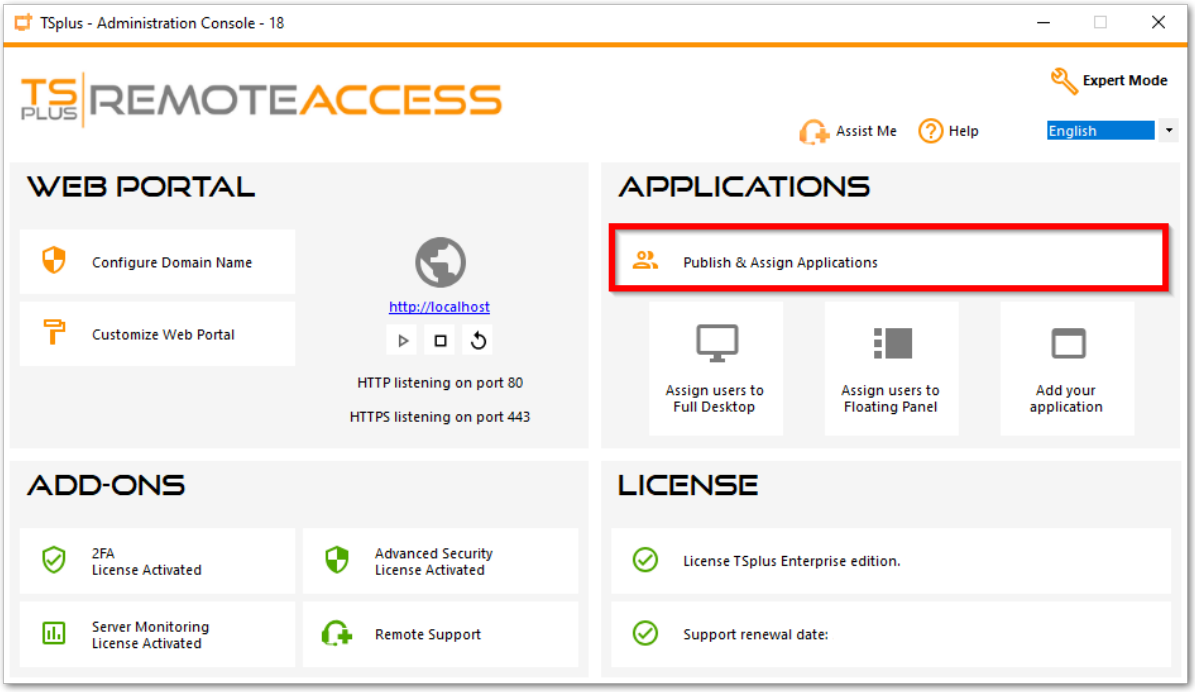


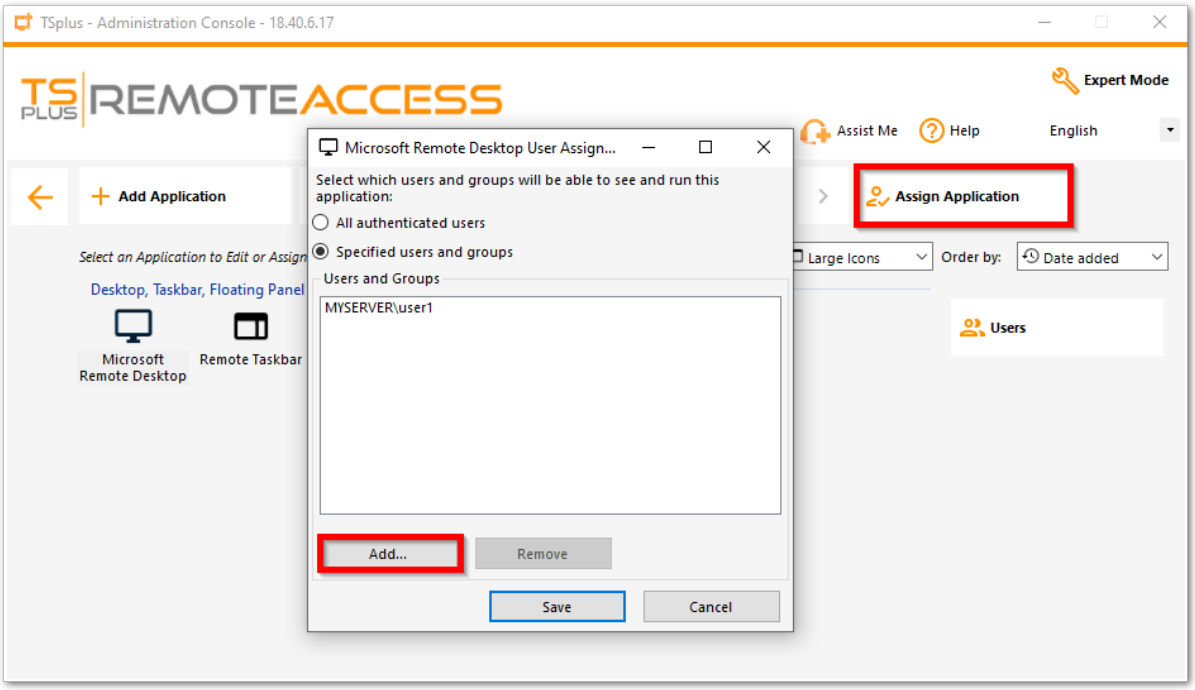
Paso 4: Publicación de Aplicaciones y Control de Aplicaciones.

En el AdminTool de Remote Access puedes asignar aplicaciones a usuarios o grupos.

- Si asignas una aplicación a un usuario, solo verá esta aplicación.
- También puedes asignarles la barra de tareas de TSplus, el panel flotante o el panel de aplicaciones para mostrar múltiples aplicaciones.
- También puedes publicar un escritorio remoto completo.

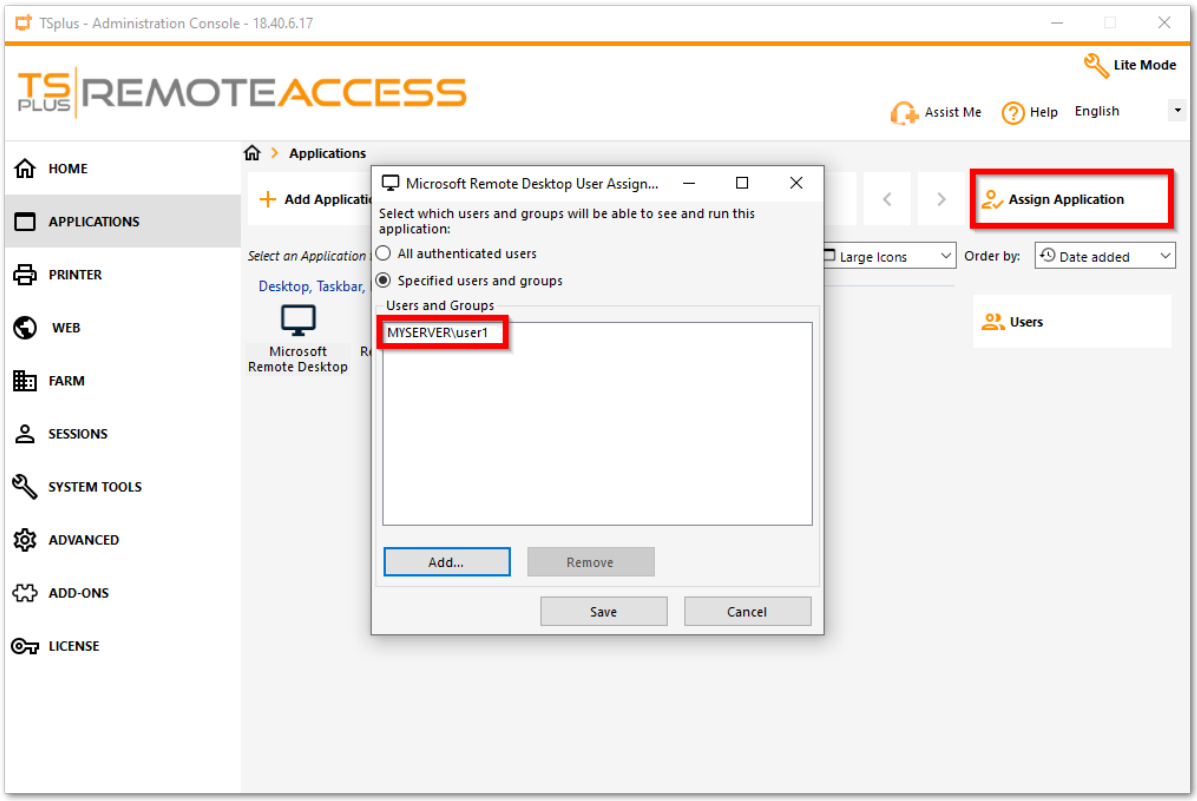
Ahora disponible en
Modo Lite
desde la pestaña de inicio.





O ir a **Modo Experto** > Pestaña de aplicaciones para agregar, editar, eliminar y asignar

aplicaciones.



En este ejemplo, el administrador ha decidido que el usuario 'John' obtendrá la barra de tareas de TSplus. Ver esta documentación para más información.

¡Gracias por usar TSplus Remote Access!

Rehosting su licencia de TSplus

Rehosting en línea

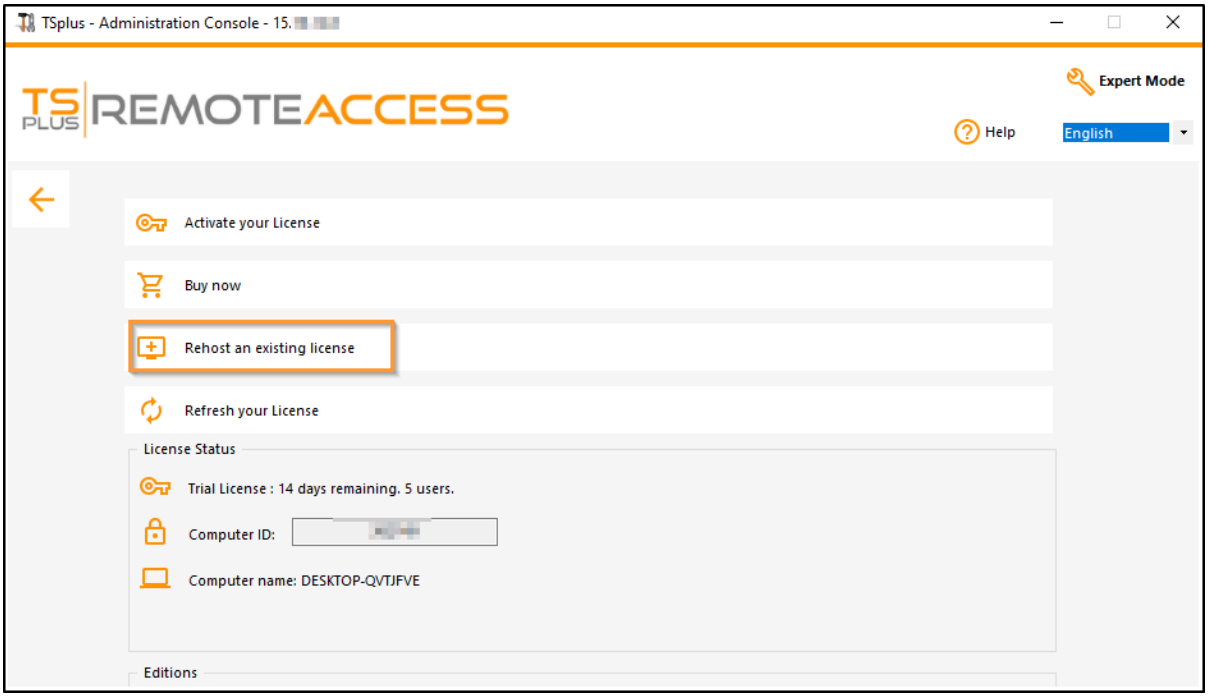
La activación en línea está autorizada una vez al mes.

Prerequisites: Es necesario tener una suscripción de soporte activa para reubicar su licencia.

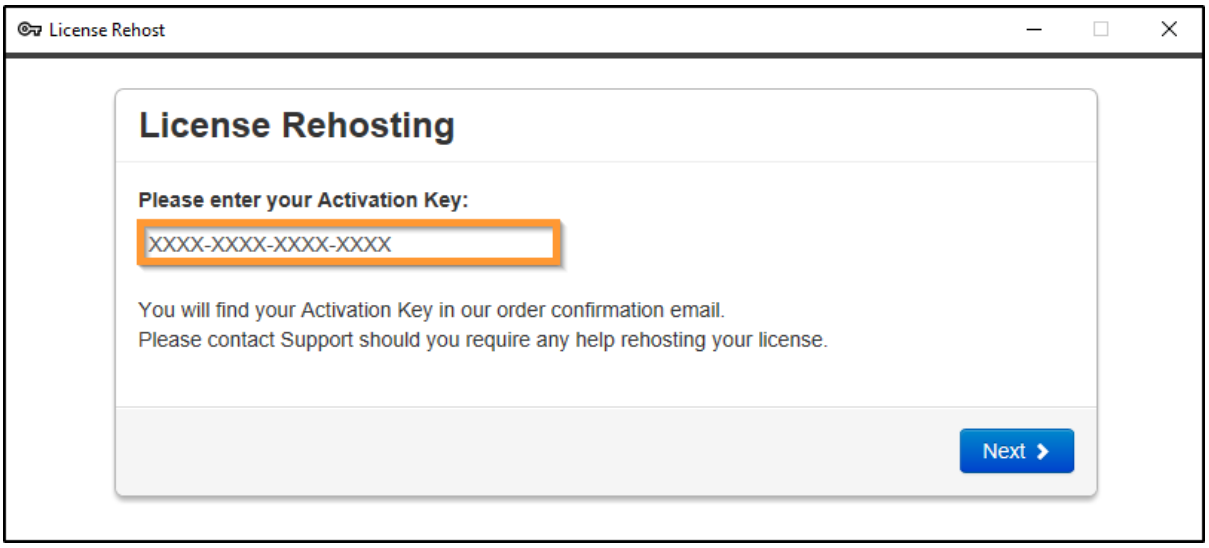
Es necesario instalar una nueva versión de Remote Access no clonada para generar un nuevo ID de computadora.

Si ha duplicado su servidor y clonado el Remote Access, por favor vaya a la siguiente página: Clona tu servidor

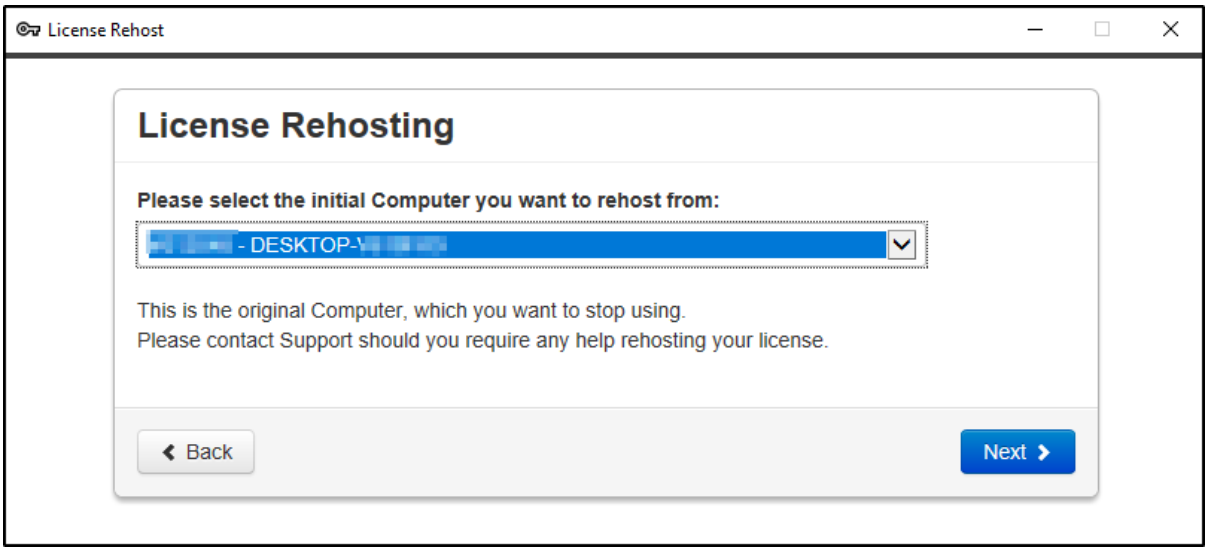
En el nuevo servidor Ve a la pestaña "Licencia" Haz clic en "Reasignar una licencia existente"



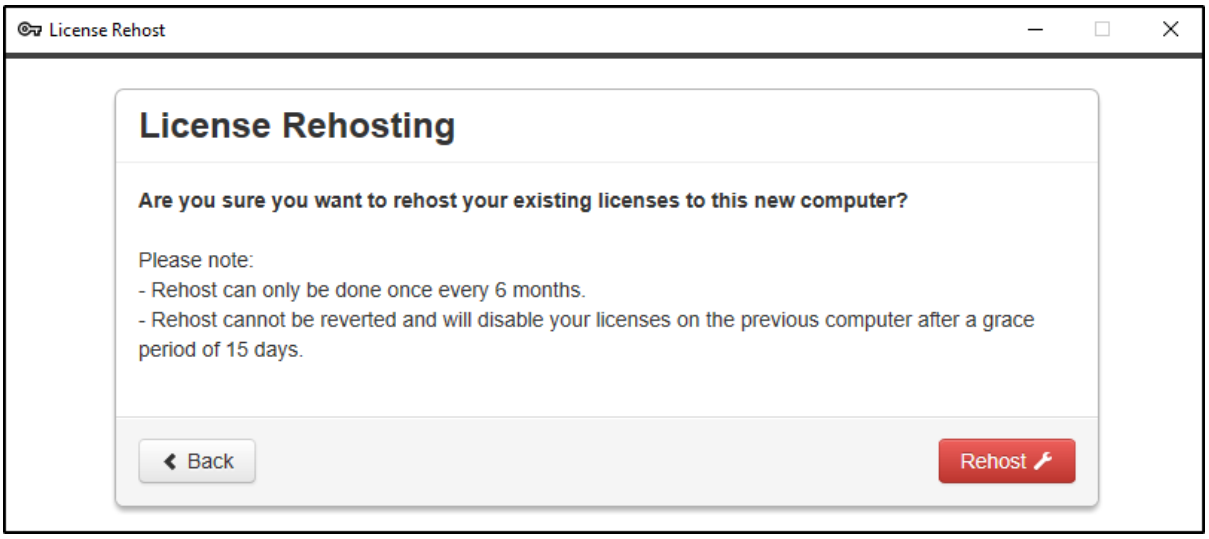
Ingrese su clave de activación:



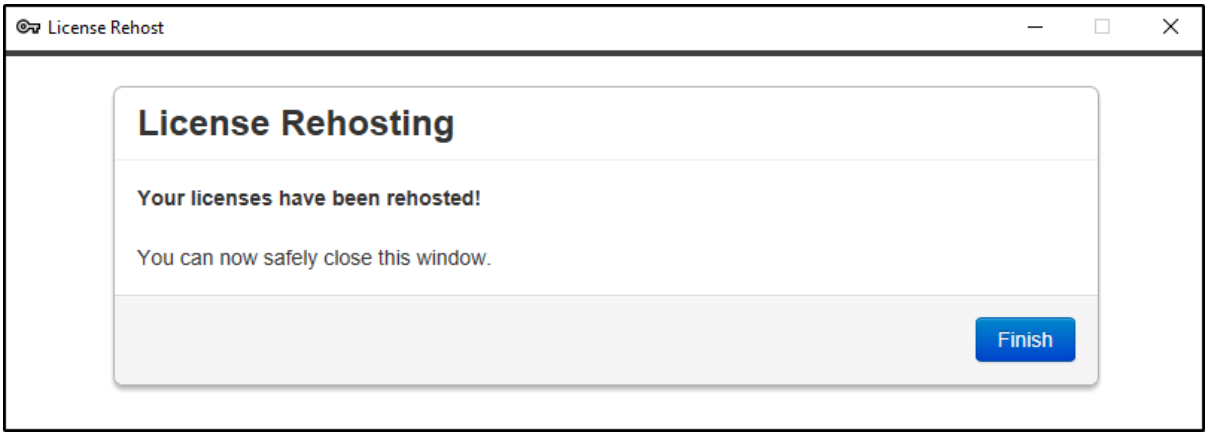
Seleccione la computadora inicial que desea reubicar.



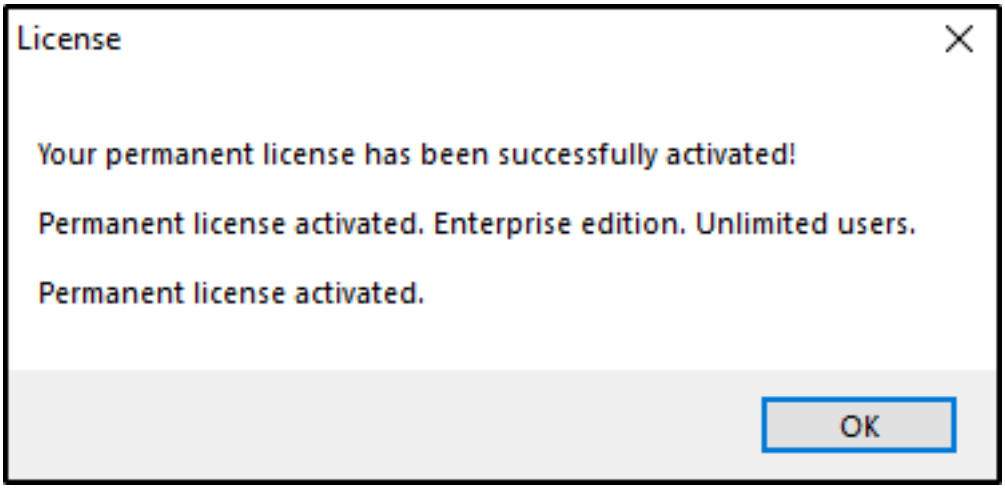
Confirmar rehosting



Su rehosting de licencia ha finalizado.

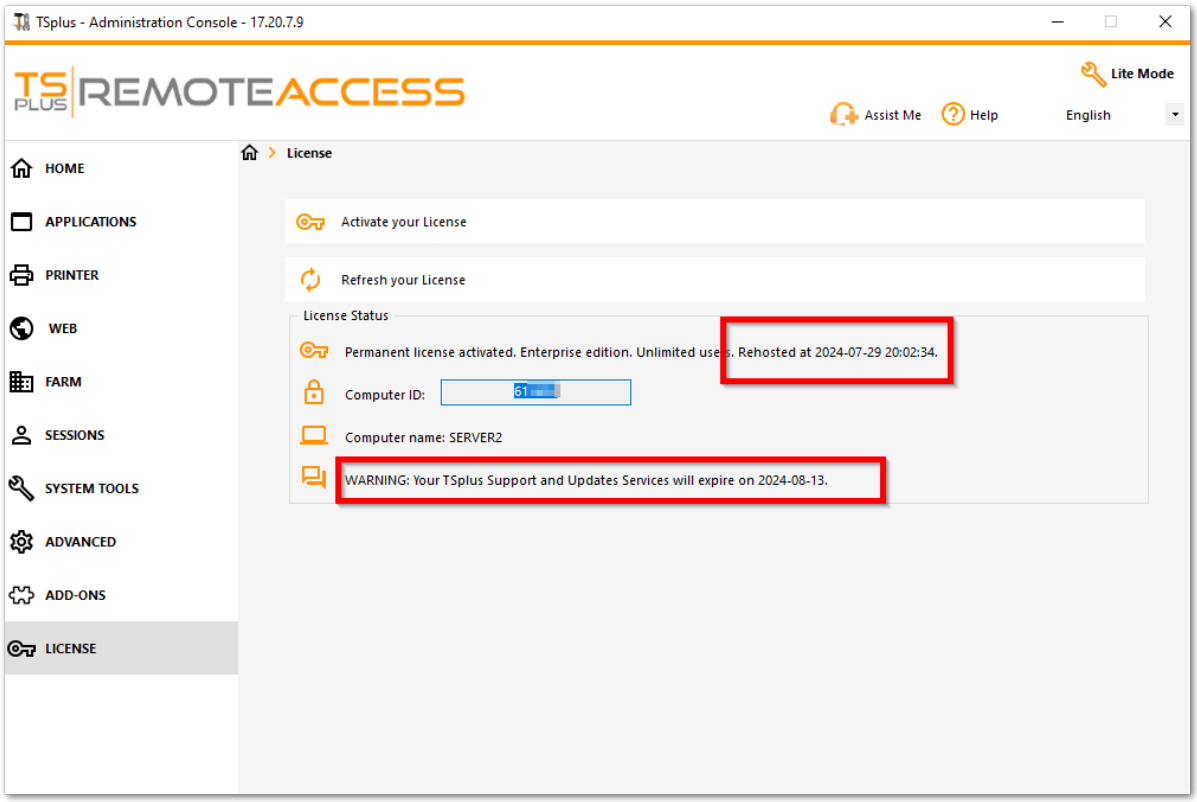


Espere unos momentos para que su AdminTool se sincronice hasta que aparezca la ventana.



¡Felicitaciones, su licencia ha sido activada con éxito!

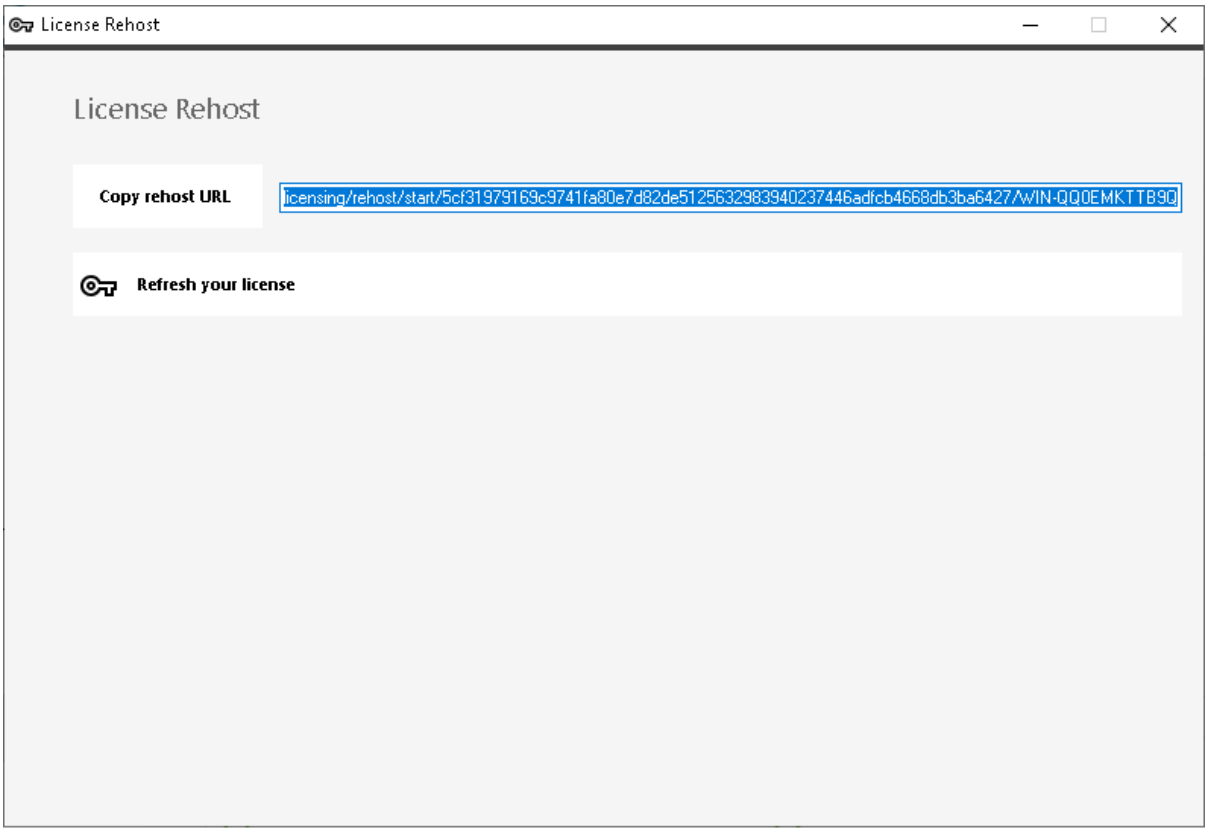
Nota: Aparecerá un mensaje en el servidor antiguo con la fecha de rehosting así como la fecha de finalización de uso.
Después de un rehosting, el antiguo servidor seguirá funcionando para **15 días** para ayudarte a hacer la transición.



Rehosting sin conexión

La activación sin conexión también se puede realizar para licencias de rehosting.

Cuando el servidor no tiene acceso a Internet, el botón 'rehospedar una licencia existente' mostrará la página de rehospedaje sin conexión:



El proceso es el mismo que la Activación Offline.

Conexión remota desde un dispositivo iPhone / iPad / Android

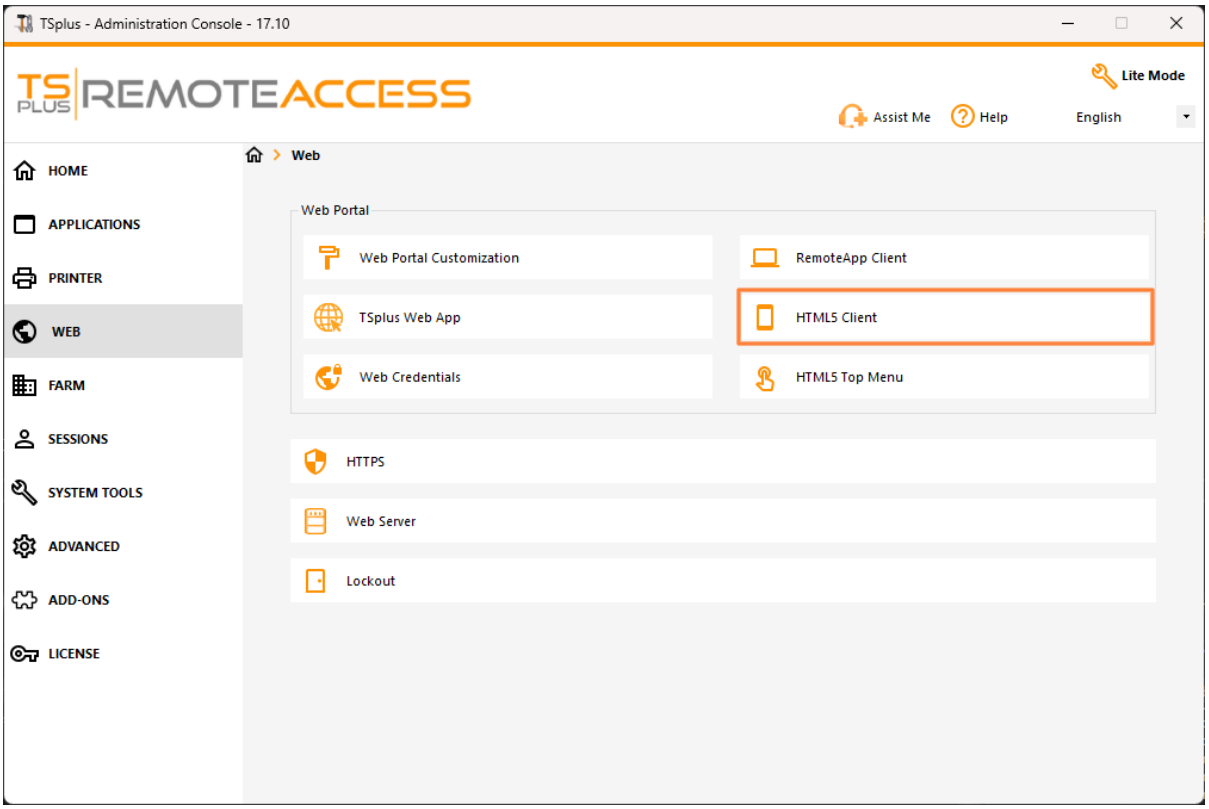
Puedes conectarte a tu servidor de Terminal Service Plus en cualquier navegador desde cualquier dispositivo móvil que soporte la tecnología HTML5, como:

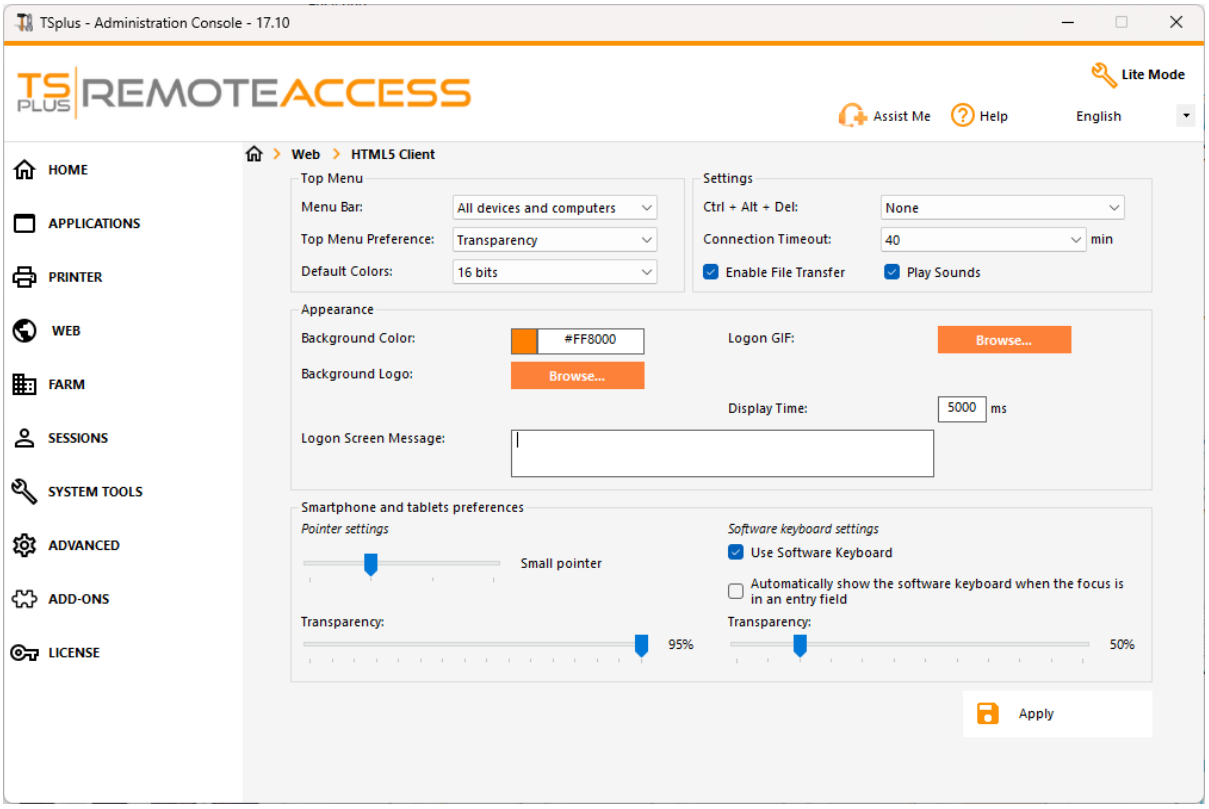
- un iPhone
- un iPad
- un smartphone Android
- una tableta Android

Editar las preferencias para dispositivos móviles

Desde la versión 11.20, el cliente HTML5 de TSplus ha sido mejorado significativamente para ofrecer la mejor experiencia de usuario posible incluso desde teléfonos inteligentes o tabletas. El teclado ha sido rediseñado para aparecer automáticamente cuando el enfoque está sobre un campo de entrada. El puntero del mouse ha sido rediseñado para facilitar la selección de botones y campos, incluso si se encuentran en los bordes izquierdo o inferior de un teléfono inteligente.

Puedes configurar varios ajustes diferentes de HTML5 para dispositivos móviles o computadoras en el mosaico del cliente HTML5 de la pestaña Web:





- Muestre la barra de menú para todos los dispositivos y computadoras o solo para dispositivos móviles.
- Habilitar o Deshabilitar la Transferencia de Archivos.
- Permitir el atajo Ctrl + Alt + Supr en un tipo específico de dispositivo.
- Elige tu opción favorita de visualización del menú superior entre transparencia y sólido.

- El número de bits de color gráfico.
- El tiempo de espera de conexión, la duración máxima (en segundos) que una sesión permanece activa mientras espera que un cliente se reconecte. 0 para deshabilitar el tiempo de espera.
- Mostrar u Ocultar Mensajes de Advertencia.
- Habilitar o deshabilitar sonidos.
- Elige tu color de fondo favorito.
- Agrega un logo al fondo.
- Cambia el mensaje de la pantalla de inicio de sesión y el gif animado, así como su tiempo de visualización en milisegundos.

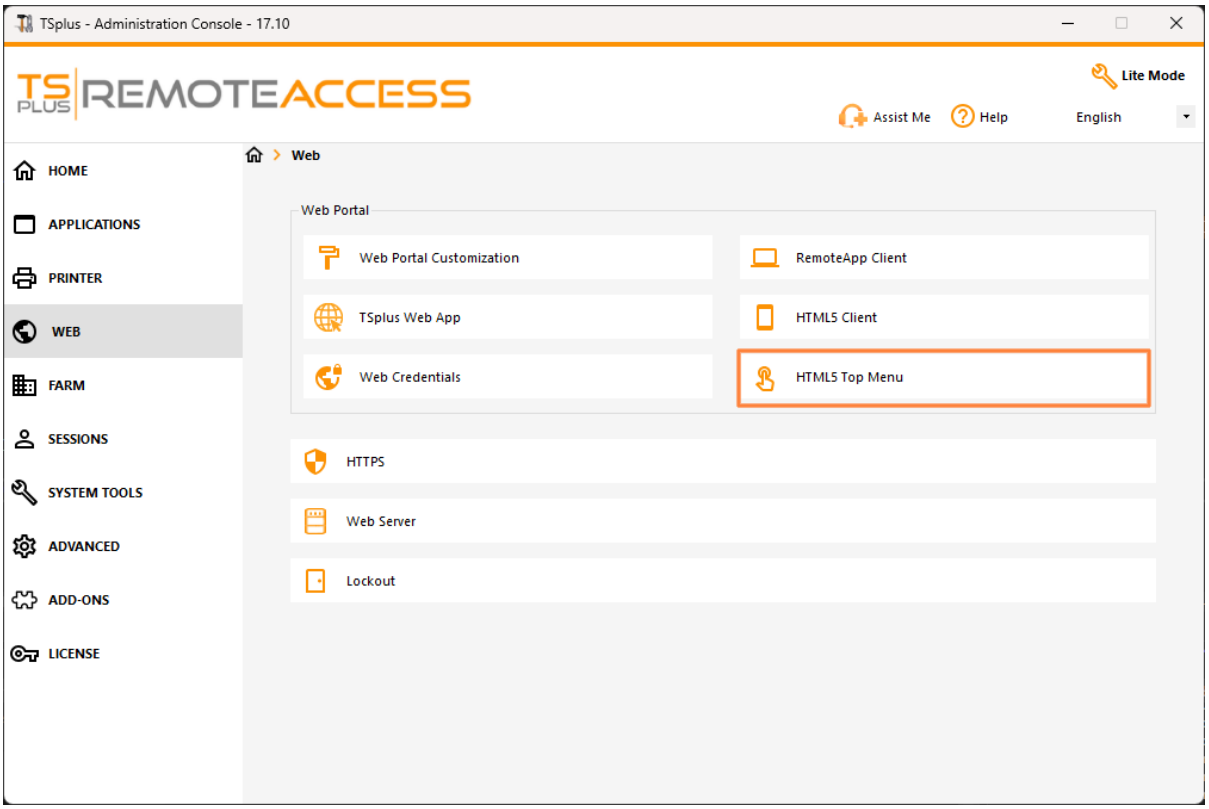
Preferencias de smartphones y tabletas :

- Si el administrador utiliza el teclado del software, cuando oculta un campo de entrada, la aplicación se mueve hacia arriba y el usuario aún puede ver lo que está escribiendo.

- El administrador puede seleccionar un tamaño pequeño, mediano o grande para el puntero del mouse o no tener puntero del mouse en absoluto. Facilita la navegación del usuario dentro de su aplicación.

- Él también puede seleccionar el nivel de transparencia para el mouse y el teclado.

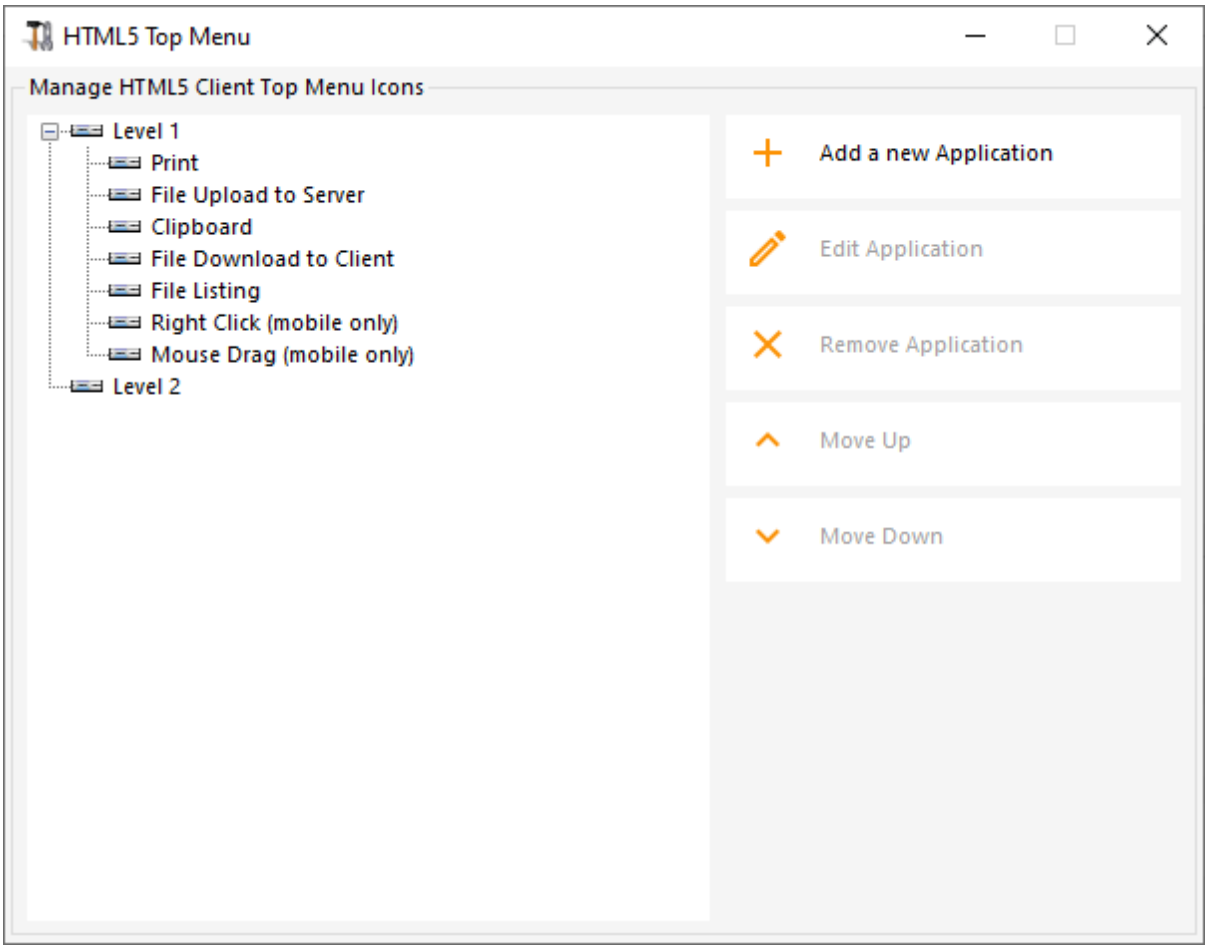
En la pestaña del Menú Superior HTML5, puedes agregar aplicaciones que se mostrarán en el primer o segundo nivel del Menú Superior en HTML5:



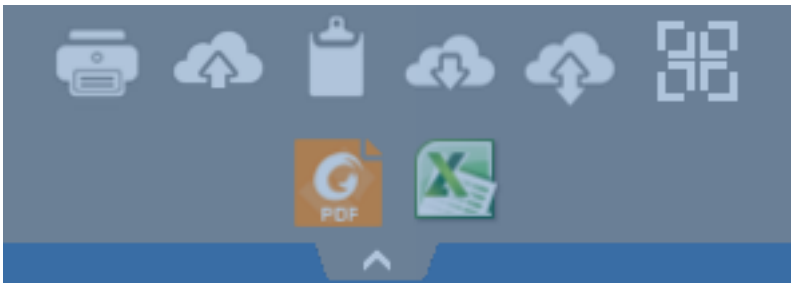
En el nivel uno, puedes encontrar las características integradas de HTML5: impresión, transferencia de archivos y un portapapeles. (Para más información sobre estas características, visita estas páginas:

Impresora Universal para HTML5 , Usando la transferencia de archivos y Usando el portapapeles .)

En este ejemplo, Foxit y Excel se publican en el nivel 2:

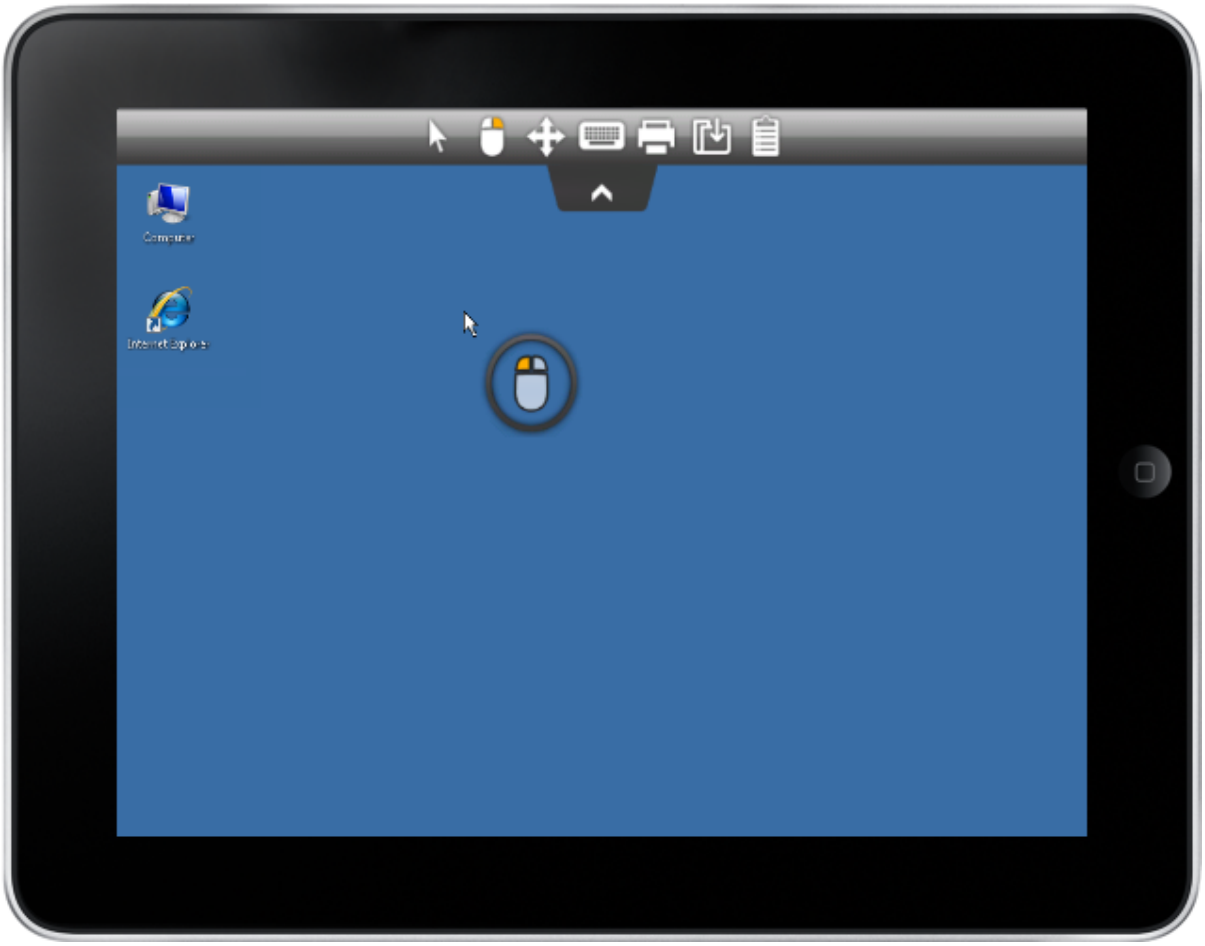


Y se puede encontrar en las funciones integradas en el menú superior de la sesión HTML5:



Además, el ícono en la parte superior derecha te permite cambiar tu sesión a pantalla completa.

Cliente HTML5 integrado de Terminal Service Plus proporciona al usuario un menú completamente nuevo en tabletas y dispositivos móviles. Con este nuevo menú, el usuario tiene un acceso fácil al teclado móvil y al clic derecho, pero también al intercambio de archivos y a nuestra única función de Impresión Universal.



Por favor, consulte a esta documentación para cómo usar el mini ratón y el teclado.

Selección de idioma

Ahora puedes cambiar el idioma con el botón de idioma a la derecha del menú superior:



Puedes elegir el idioma para el país específico que desees en este menú:

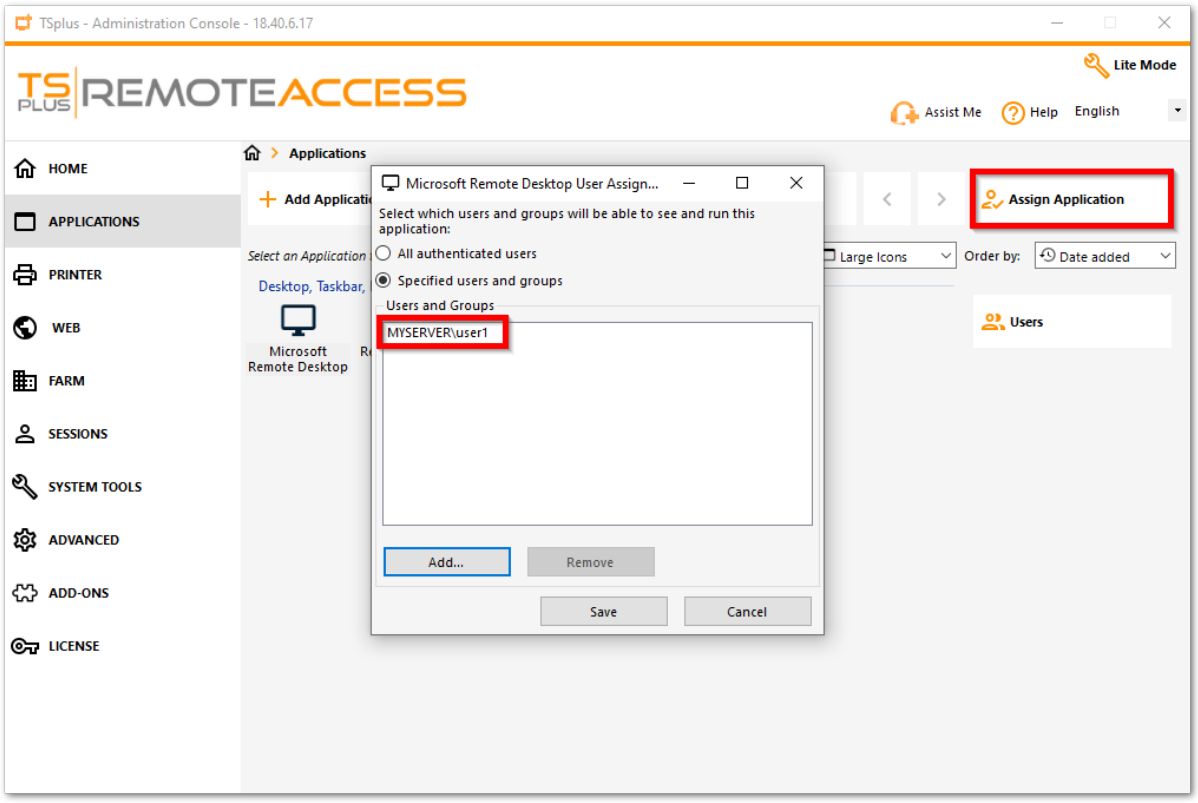
	Language	Locale	Value
◯	Portal	as_portal	
◯	Browser	as_browser	
◯	Gateway	as_gateway	
◯	Arabic	ar_ar	1025
◯	Belarusian	be_be	1059
◯	Bulgarian	bg_bg	1026
◯	Bengali	bn_bn	1093
◯	Bosnian (Cyrillic)	bs_cyrl_ba	8218
◯	Bosnian (Latin)	bs_latn_ba	5146
◯	Catalan	ca_ca	1027
◯	Czech	cs_cs	1029
◯		cs_cz	1029
◯	Welsh	cy_gb	1106
◯	Danish	da_da	1030
◯		da_dk	1030
◯	German (Swiss)	de_ch	2055
◯	German	de_de	1031
◯	Divehi	dv_dv	1125
◯	Greek	el_el	1032
◯		el_gr	1032
◯	English (Canada)	en_ca	4105

Temas de barra de tareas y escritorios remotos

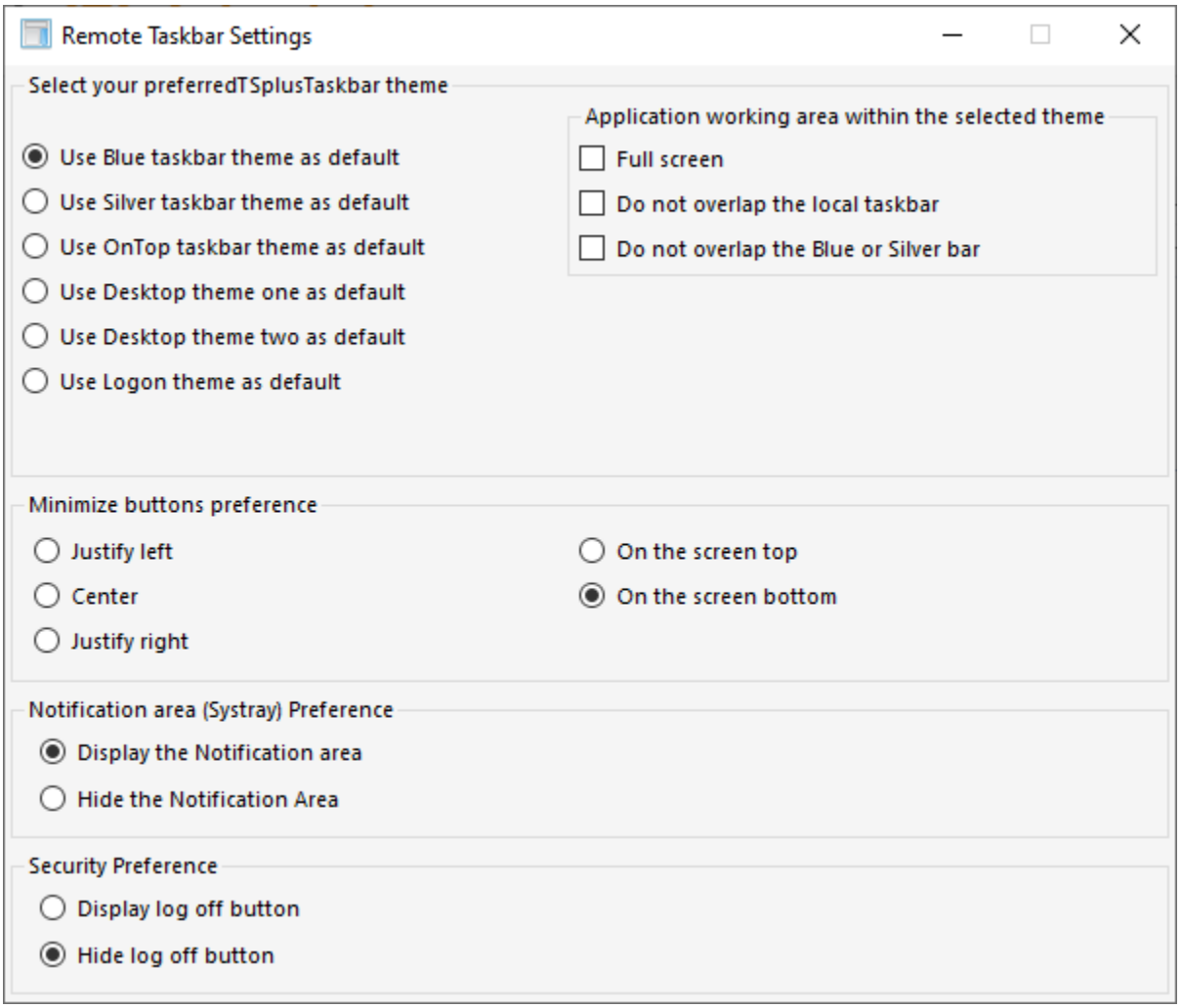
Herramientas de administrador en el servidor

Con el AdminTool, el Administrador puede elegir entre 4 modos de visualización al asignar aplicaciones: El Escritorio Remoto de Microsoft , La barra de tareas remota , El Panel Flotante o El Panel de Aplicaciones La barra de tareas remota, los paneles flotantes y de aplicaciones están disponibles para cualquier método de conexión.

Cuando asignas aplicaciones a un usuario, puedes habilitar la barra de tareas remota de TSplus. El usuario puede iniciar aplicaciones remotas con un solo clic en la barra de tareas de TSplus y aún tener disponible el escritorio local completo. Puedes asignar la barra de tareas remota a tus usuarios o grupos haciendo doble clic en ella o seleccionándola y luego haciendo clic en el mosaico "Asignar aplicación".



El Administrador puede decidir fácilmente cuál será el tema predeterminado de Escritorio Remoto que el usuario verá al abrir una sesión. Seleccione la Barra de Tareas Remota de TSplus, luego haga clic en "Editar Aplicación":



- Solo el Administrador puede elegir los temas para sus usuarios.
- Él puede elegir mostrar las aplicaciones maximizadas en modo de pantalla completa o no superponer la barra de tareas de TSplus, así como las barras de tareas Silver o Blue.
- La posición de los botones minimizados en la barra de tareas se puede cambiar (en la parte superior de la pantalla, en la parte inferior, a la derecha, al lado izquierdo o en el centro).

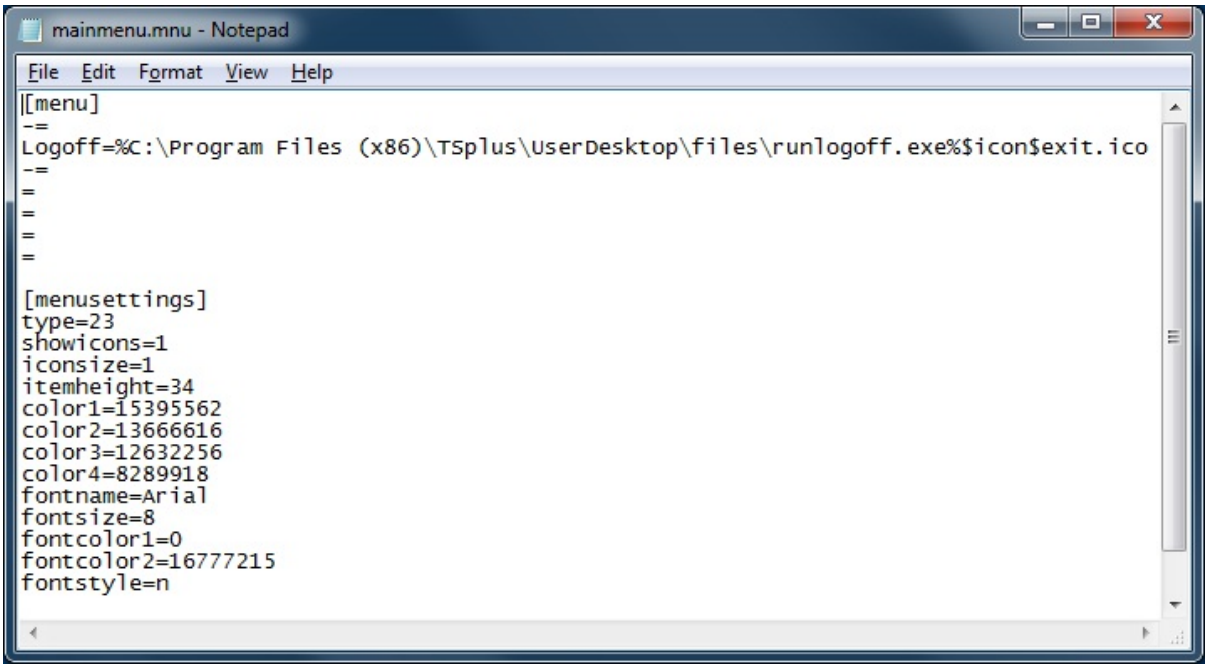
  El administrador incluso puede decidir mostrarlo en la parte superior de la pantalla del usuario en lugar de la parte inferior predeterminada.
-

Los iconos de la bandeja del sistema se pueden ocultar marcando el círculo "Ocultar el área de notificación".

- Desde la versión 12.60 de TSplus, el botón de Cerrar sesión ahora se puede ocultar.

Al editar el menú de usuarios, el Administrador puede agregar/suprimir aplicaciones y funcionalidades. La personalización del menú de usuarios es fácil.

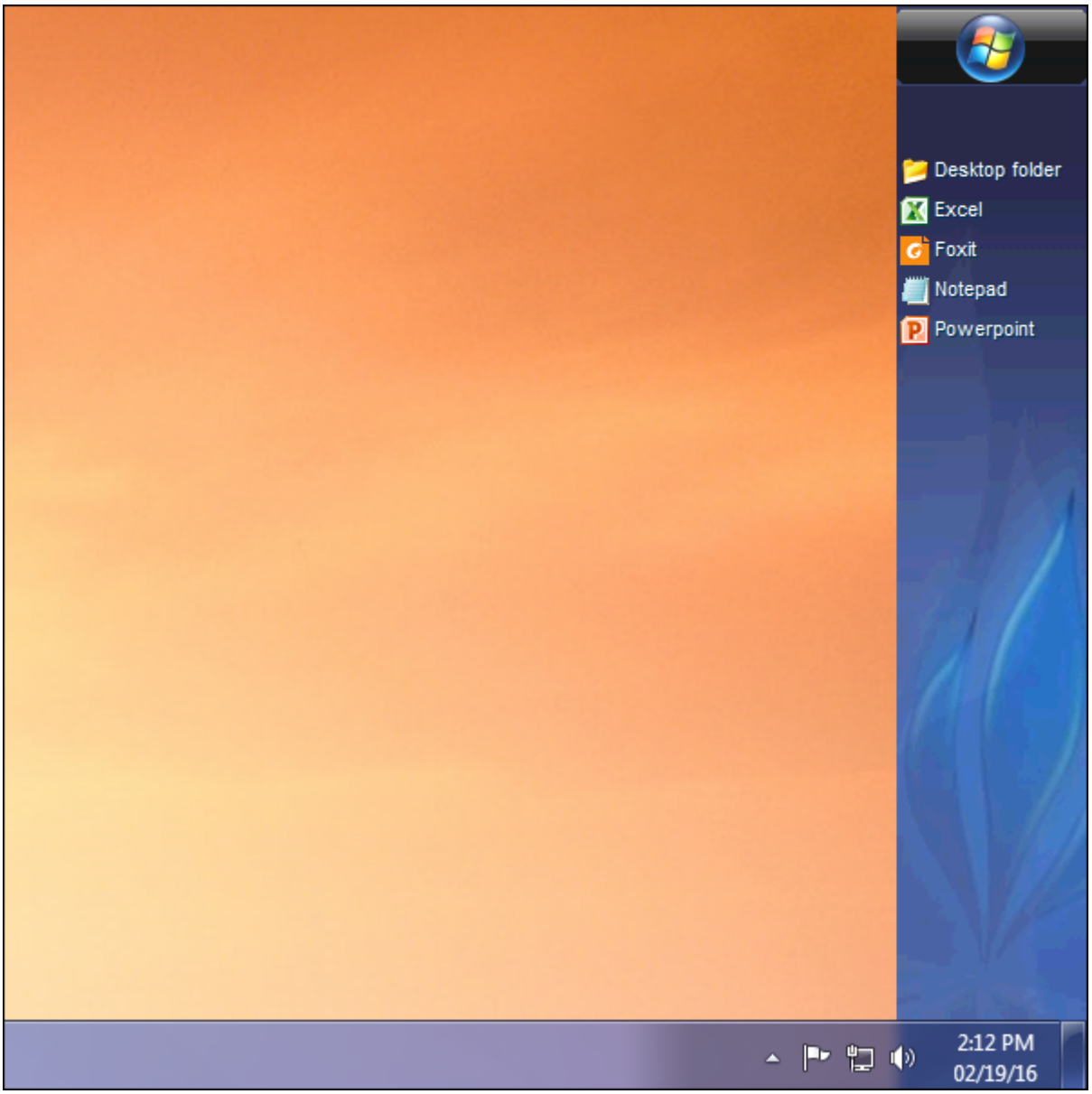
El contenido del menú de usuarios (ubicado en Archivos de Programa/TSplus/UserDesktop/mainmenu.mnu) es modificable por el administrador utilizando el Bloc de notas:



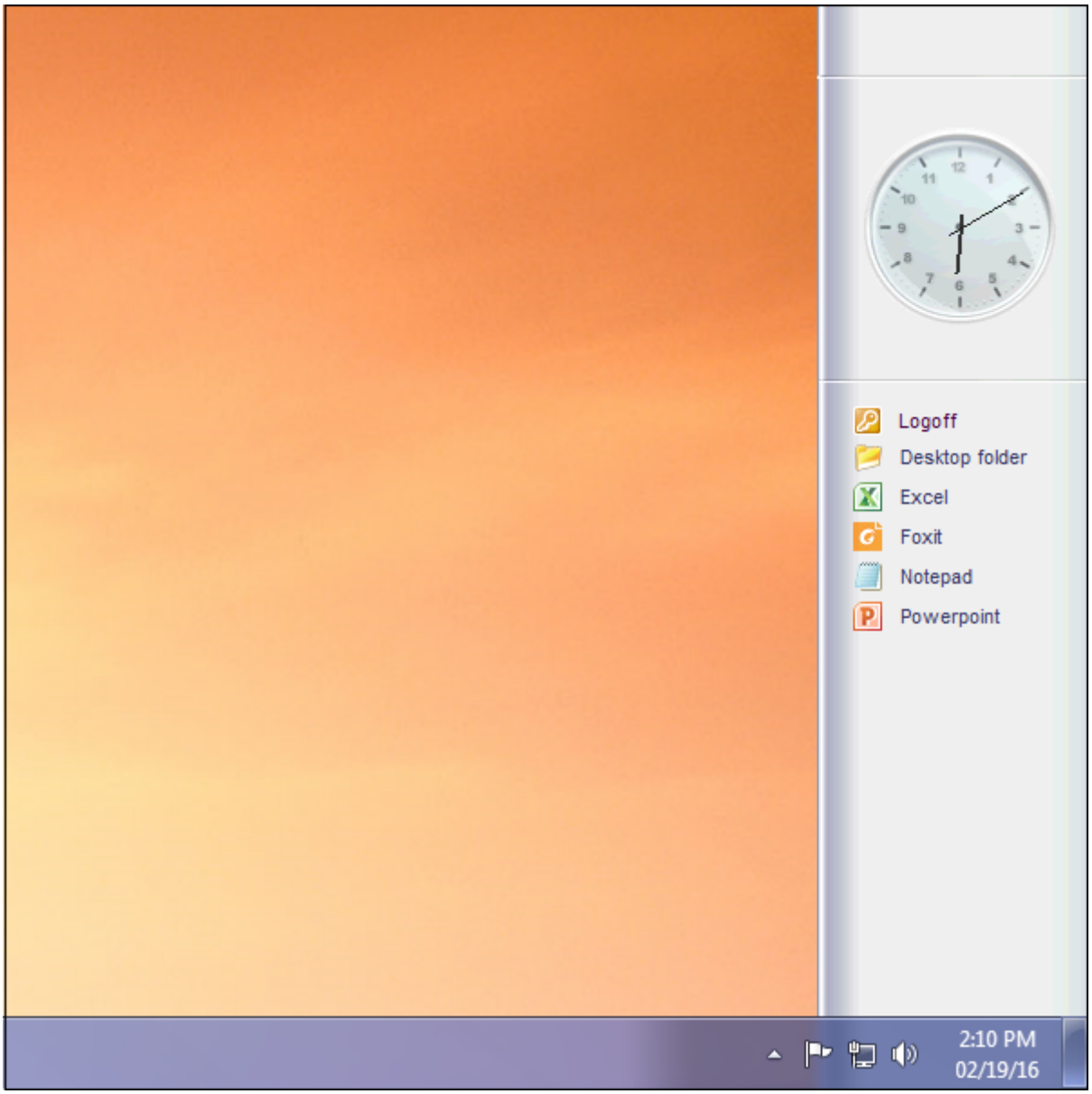
En el mosaico de aplicaciones de AdminTool, el administrador puede seleccionar 3 estilos diferentes de la barra de tareas de Remote Desktop TSplus.

El usuario puede lanzar aplicaciones remotas con un clic en la barra de tareas de TSplus y aún tener el escritorio local completo disponible.

Barra de tareas de tema azul del lado derecho



Barra de tareas del tema plateado del lado derecho



En la barra de tareas superior



Volver Arriba

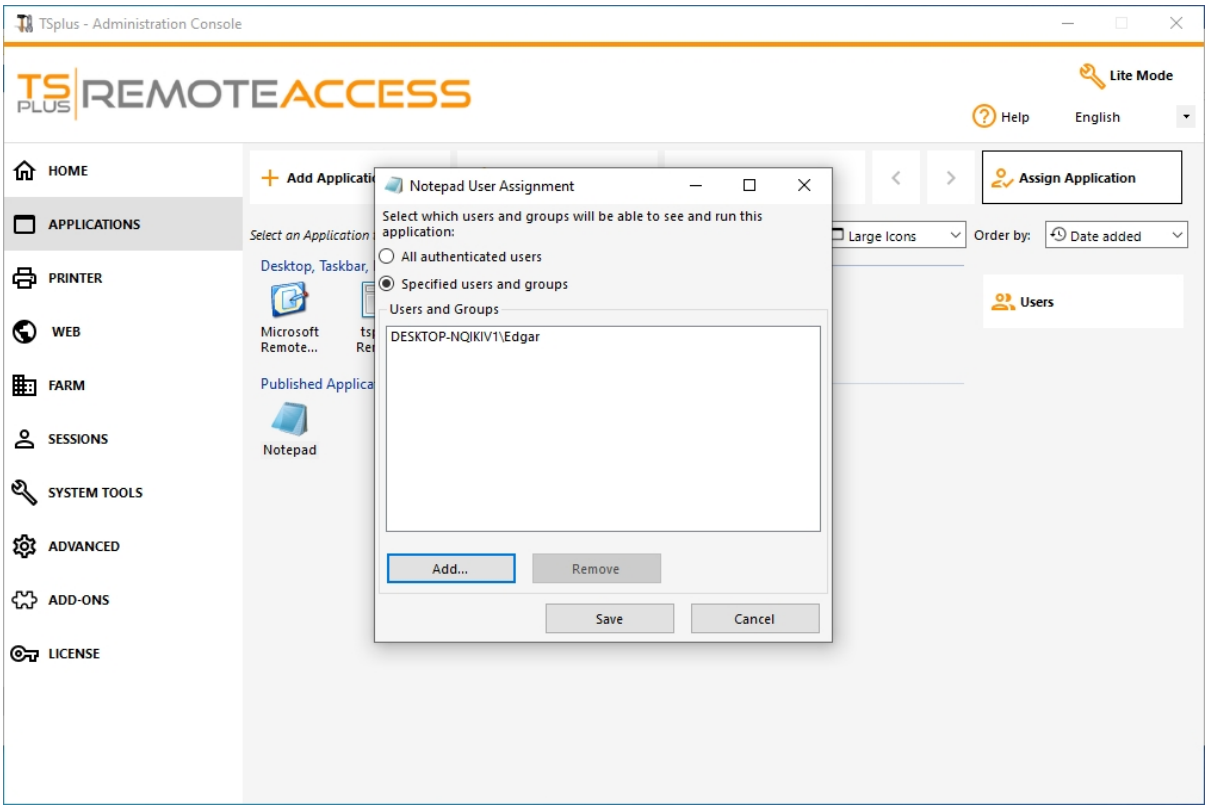
Con el AdminTool, el Administrador puede decidir fácilmente cuál será el tema predeterminado

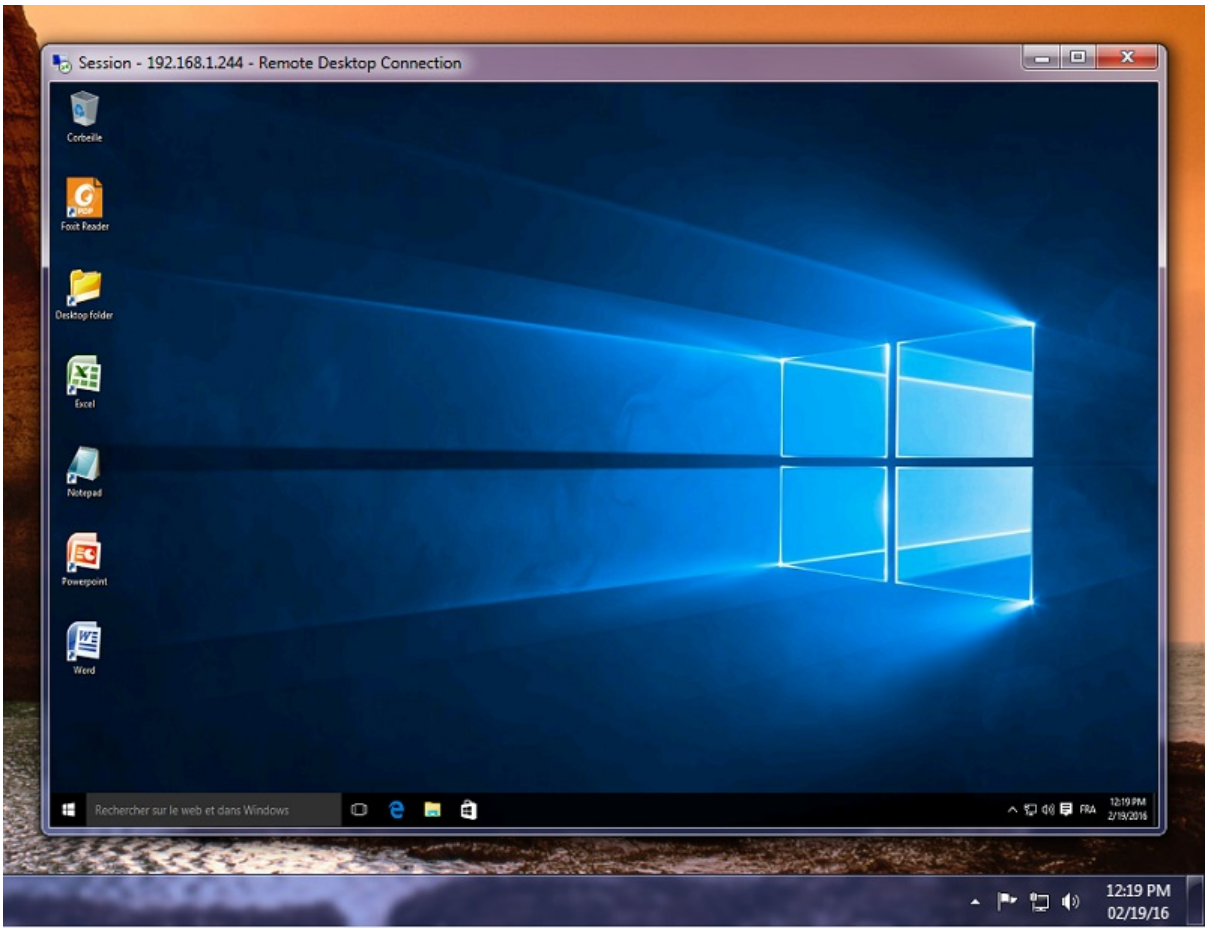
de Remote Desktop que el usuario verá al abrir una sesión. Tiene la opción entre 4 estilos diferentes de Remote Desktop en pantalla completa. También se puede utilizar el Remote Desktop estándar de Microsoft si se prefiere.

Porque estos escritorios de TSplus son escritorios de pantalla completa, la pantalla del usuario se llena por completo cuando se abre una sesión desde clientes delgados dedicados, cualquier cliente basado en RDP, o se accede desde una página web o clientes de Escritorio Remoto de TSplus.

Hay beneficios sobre un Escritorio Remoto estándar. Mejora la seguridad del servidor (sin botón de INICIO ni control total del Escritorio).

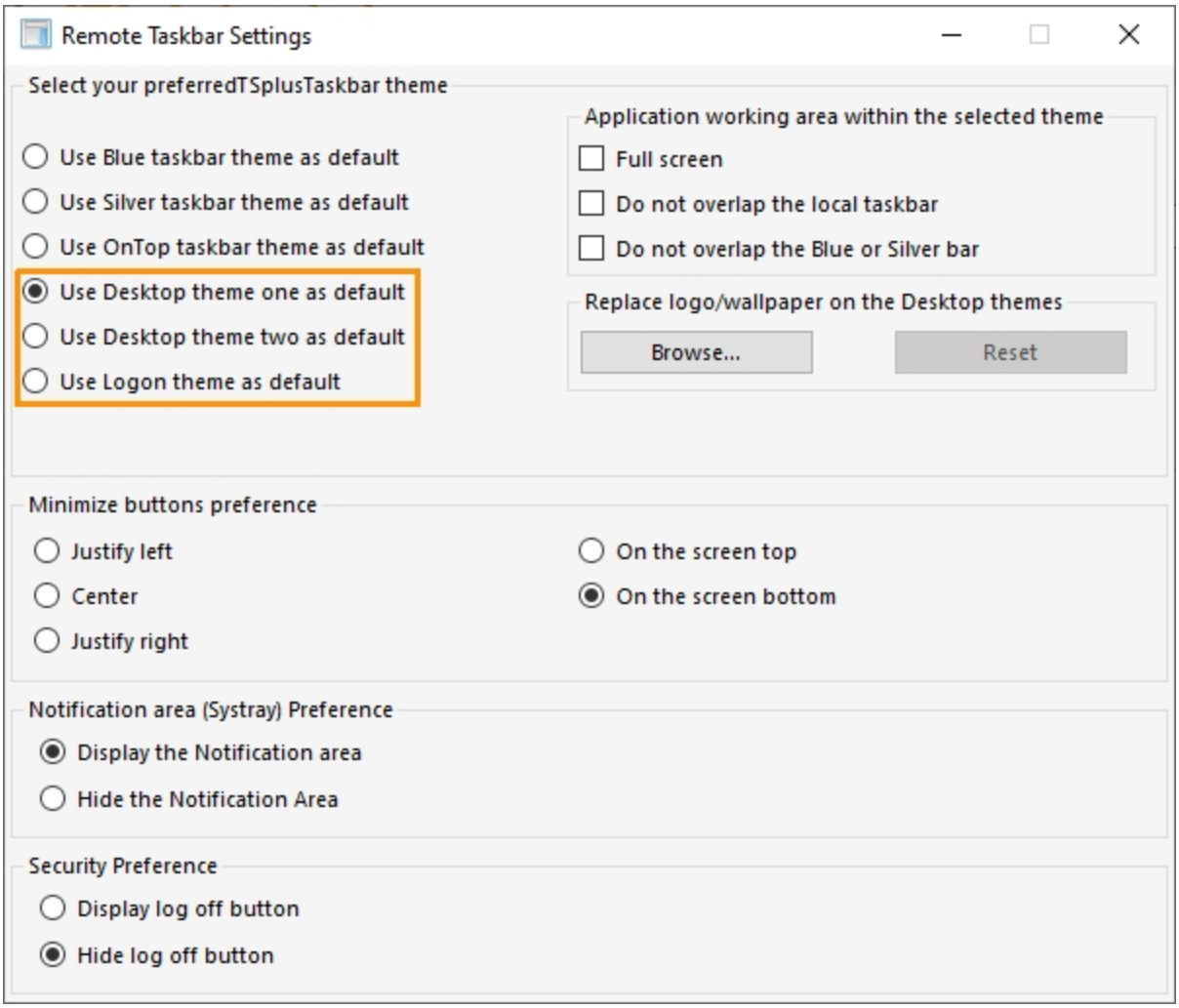
Escritorio Remoto de Microsoft Estándar





- El usuario tiene un escritorio completo que incluye el botón de inicio y control total del escritorio.
- Para asignar a un escritorio completo, simplemente asigna la aplicación de Microsoft Remote Desktop.

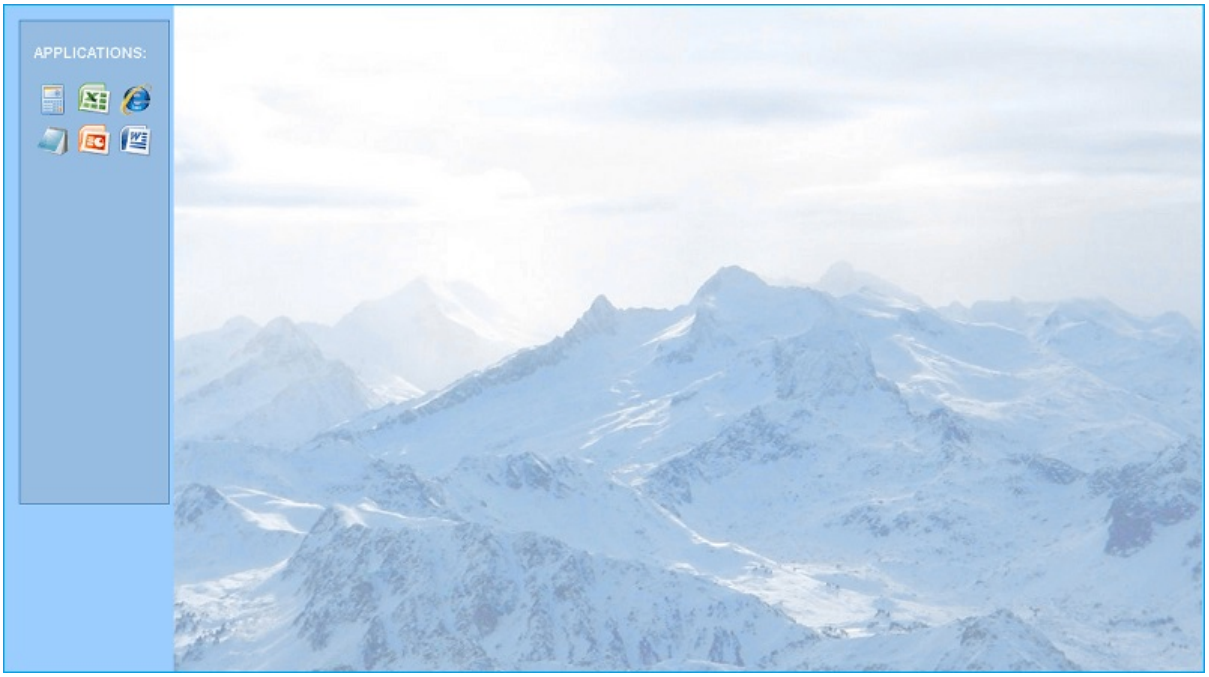
Para cambiar los temas de escritorio, tendrás que asignar la barra de tareas remota de TSplus y elegir entre los 3 temas sugeridos:



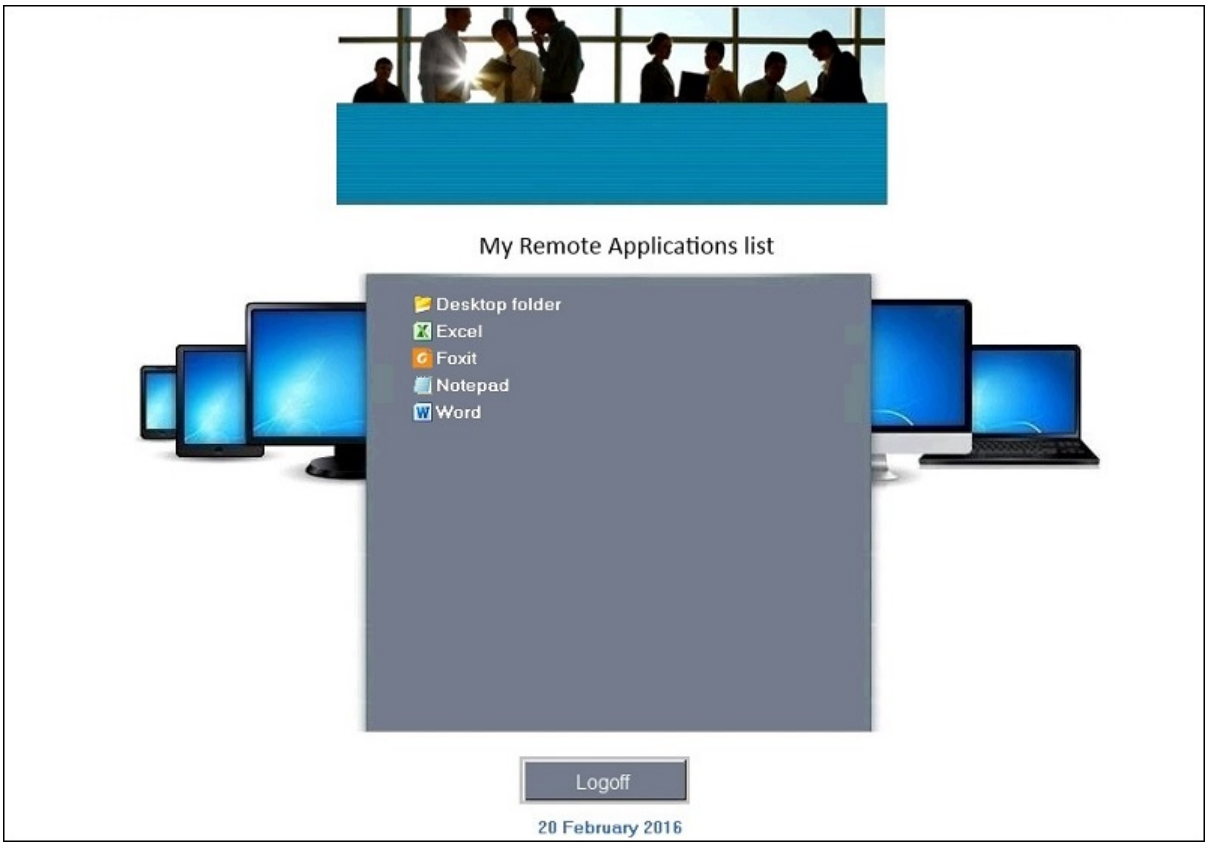
TSplus tema de escritorio uno



TSplus tema de escritorio dos



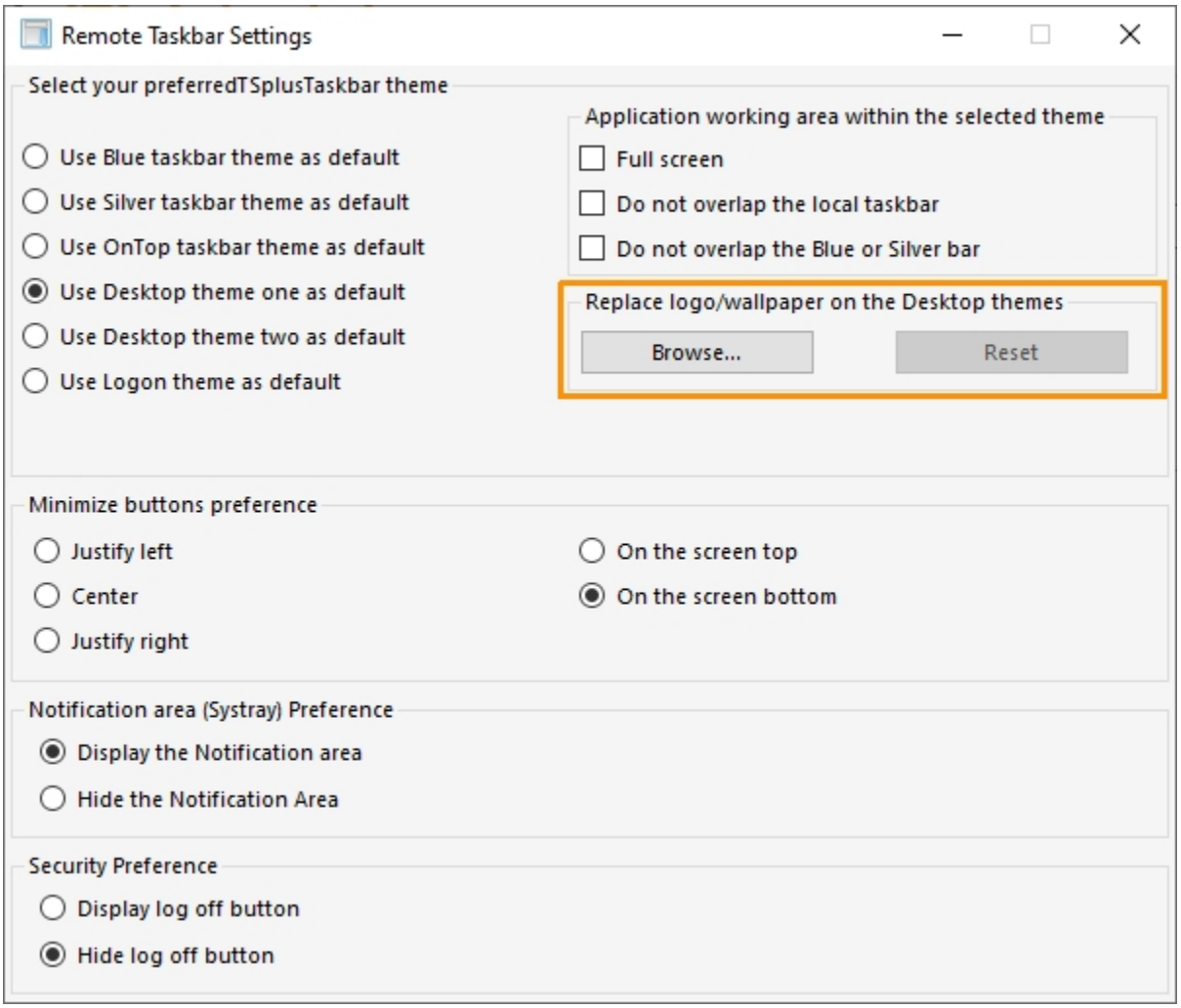
TSplus tema de inicio de sesión



Tema personalizado

Para cada tema, el Administrador puede personalizarlo y, por ejemplo, mostrar el logo

corporativo. También puede agregar su propio fondo de escritorio seleccionando uno de los temas de escritorio y haciendo clic en el botón Reemplazar logo/fondo de pantalla para seleccionar su archivo .jpg, por ejemplo:



- Puedes agregar tu propio fondo de escritorio seleccionando uno de los temas de escritorio y haciendo clic en el botón Reemplazar logo/fondo de pantalla para seleccionar tu archivo .jpg, por ejemplo:


APPLICATIONS:
15 June 17

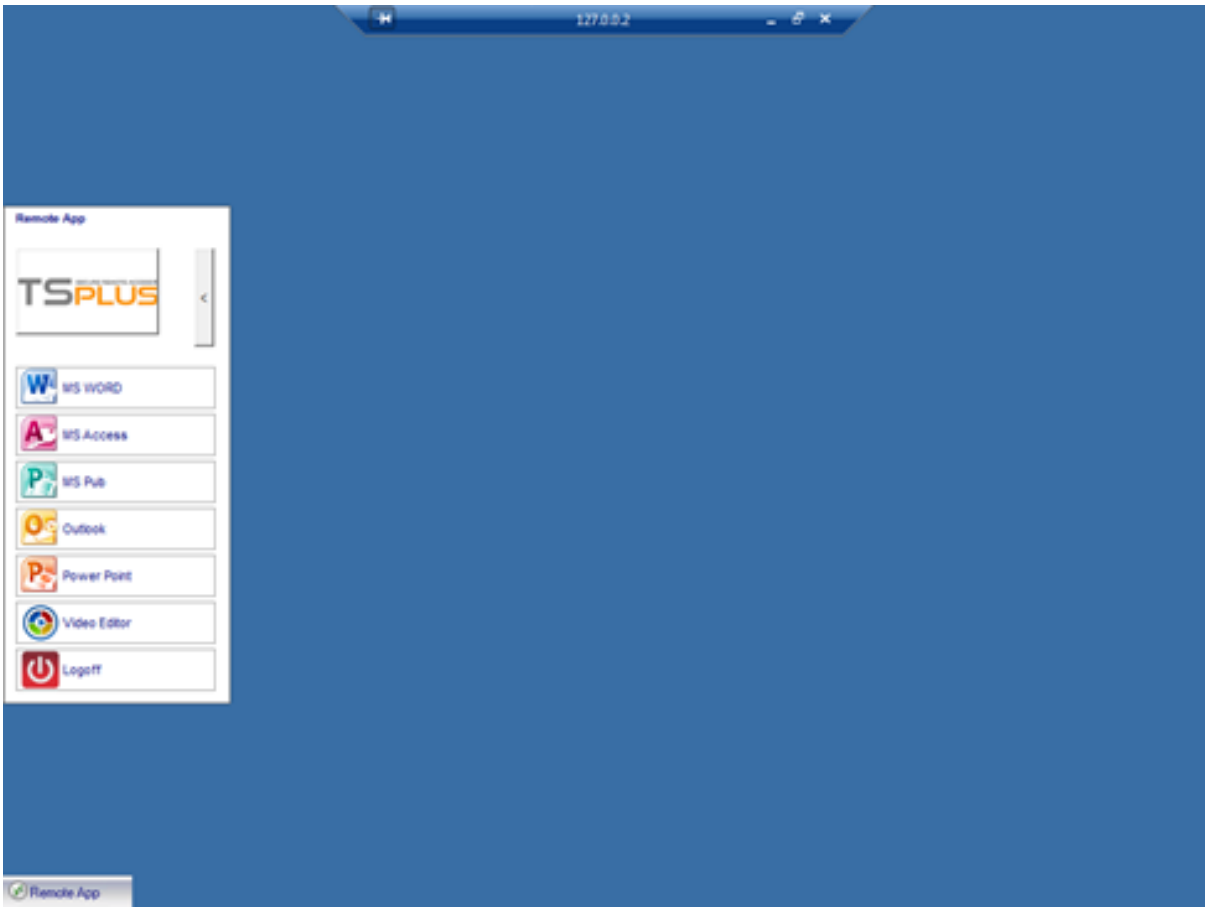
Función RemoteApp en el cliente

En el pasado, el cliente portátil de TSplus generado era el método habitual para que un usuario iniciara aplicaciones. La versión 10.50 introduce **un ícono en el área de notificación** que le da a cada usuario la lista de todas sus Aplicaciones Remotas. Dentro de esta lista de aplicaciones, el usuario puede seleccionar la que desea iniciar.

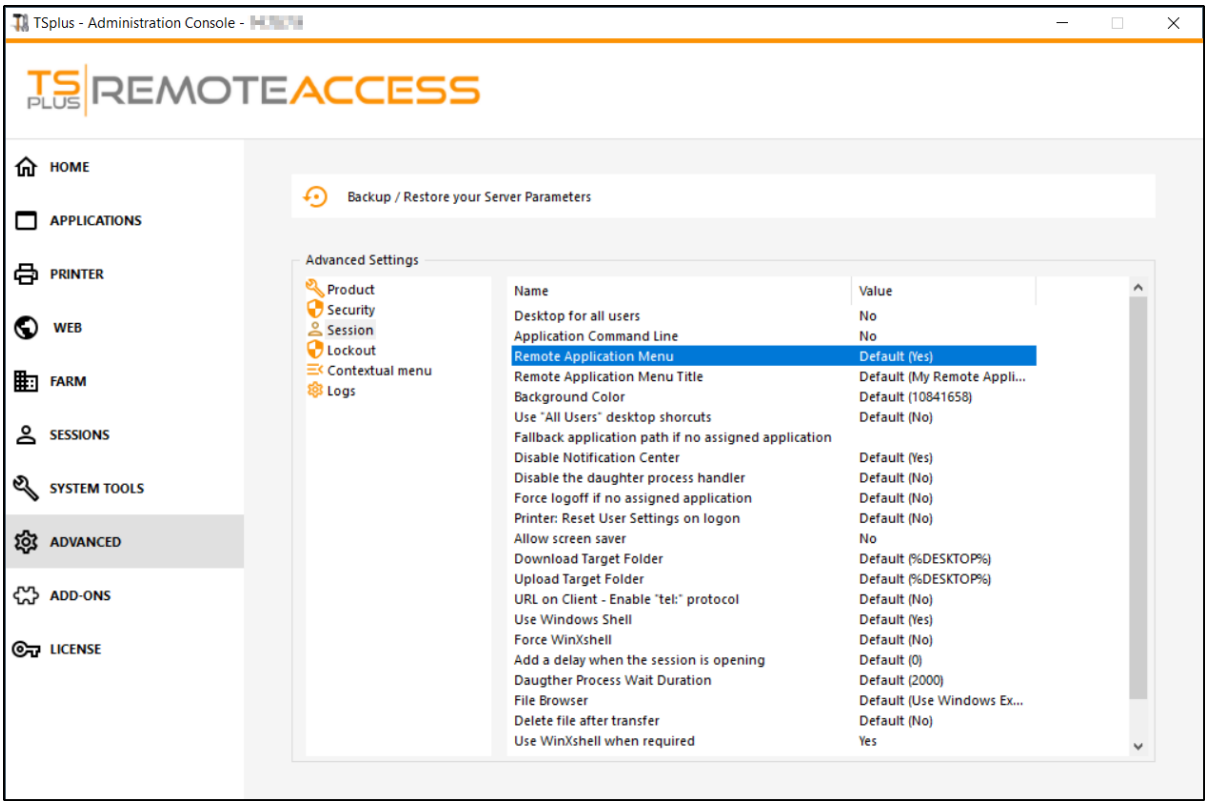
Esta es una nueva forma para que los administradores entreguen aplicaciones remotas (denominadas “RemoteApps”) a sus usuarios. Específicamente, RemoteApp On Client permite un proceso de publicación sencillo que permite que las aplicaciones instaladas directamente en el servidor se proporcionen a los usuarios, permite que los programas RemoteApp se ejecuten junto a programas locales y ofrece integración con una aplicación “lanzador” personalizada para facilitar a los usuarios encontrar y lanzar programas RemoteApp.

La lista de aplicaciones del usuario también aparecerá en el **Menú de inicio** debajo **Todos los programas** en una carpeta llamada **Mis Aplicaciones Remotas** Para implementar esta nueva y asombrosa capacidad de TSplus es simple: El Administrador ha generado nuevos clientes de conexión y los ha permitido con el AdminTool. Esta guía explicará paso a paso lo que sucederá cuando el administrador habilite esta nueva función y entregará a sus usuarios un nuevo cliente de conexión generado.

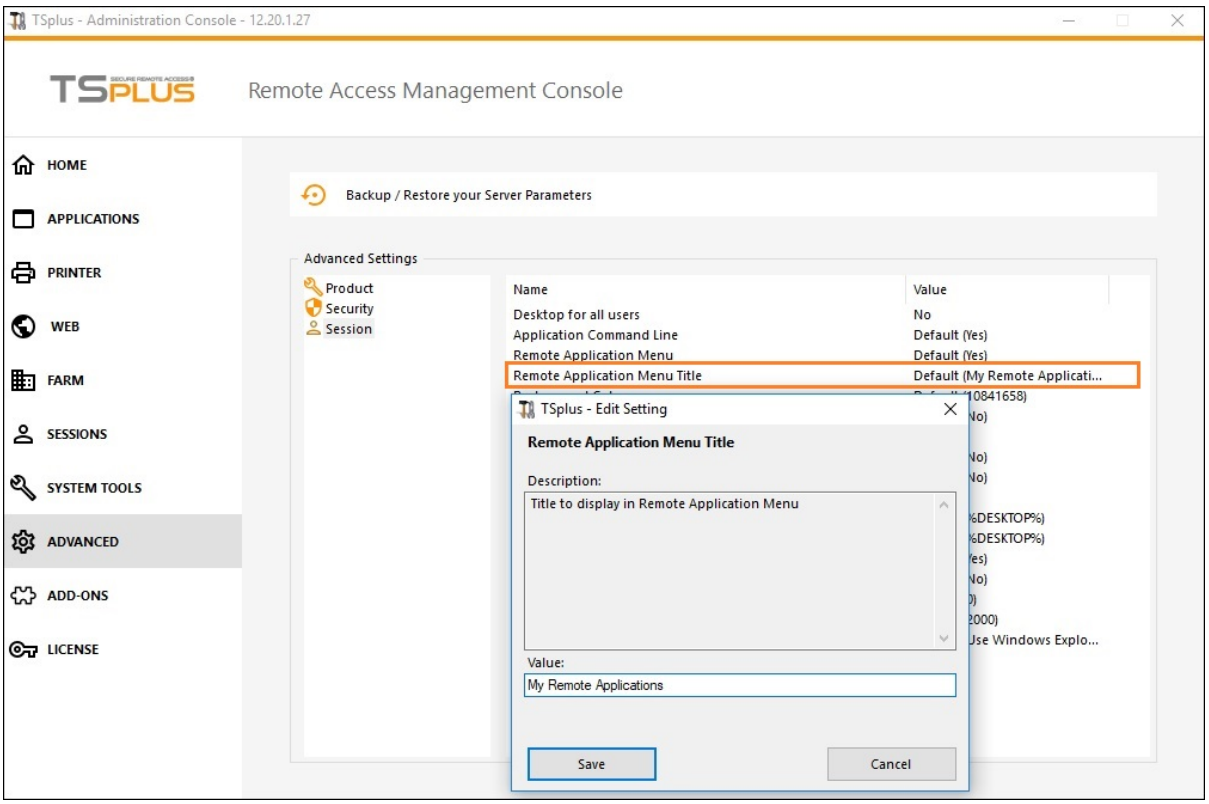
Ejemplo: La usuaria “Laura” está utilizando TSplus para acceder a su aplicación remota. Para hacerlo, está usando un cliente generado llamado **LauraPortableClient.exe** Cuando lo ejecuta en su PC, obtiene el siguiente resultado:



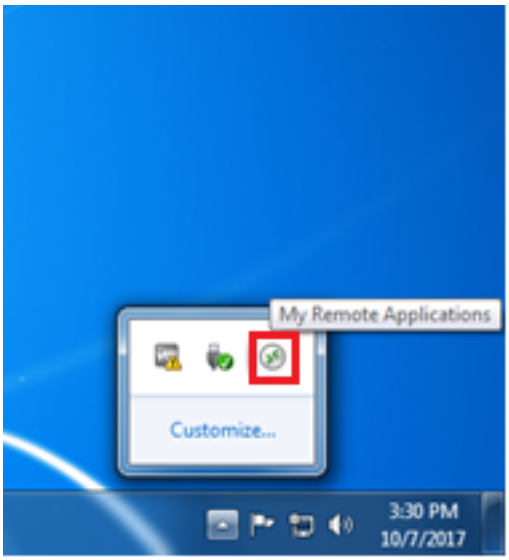
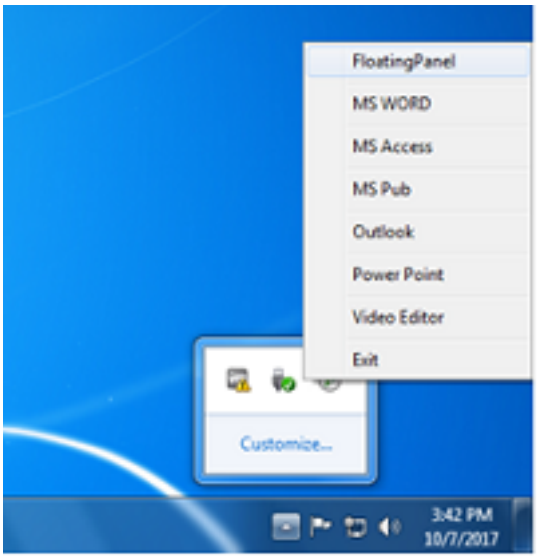
Sin embargo, el administrador le proporcionó uno nuevo, creado con la versión TSplus 10.50. Tendrá que ejecutarlo al menos una vez para beneficiarse de la nueva. **Función RemoteApp en el cliente** Cuando el administrador está agregando/eliminando una aplicación a un usuario, dicho cambio se establecerá en el lado del servidor en el próximo inicio de sesión. Esto significa que la sesión actual no reflejará tal modificación. La pestaña Avanzada de AdminTool tiene una opción para habilitar o deshabilitar esta función de RemoteApp en el cliente, por defecto, está habilitada.



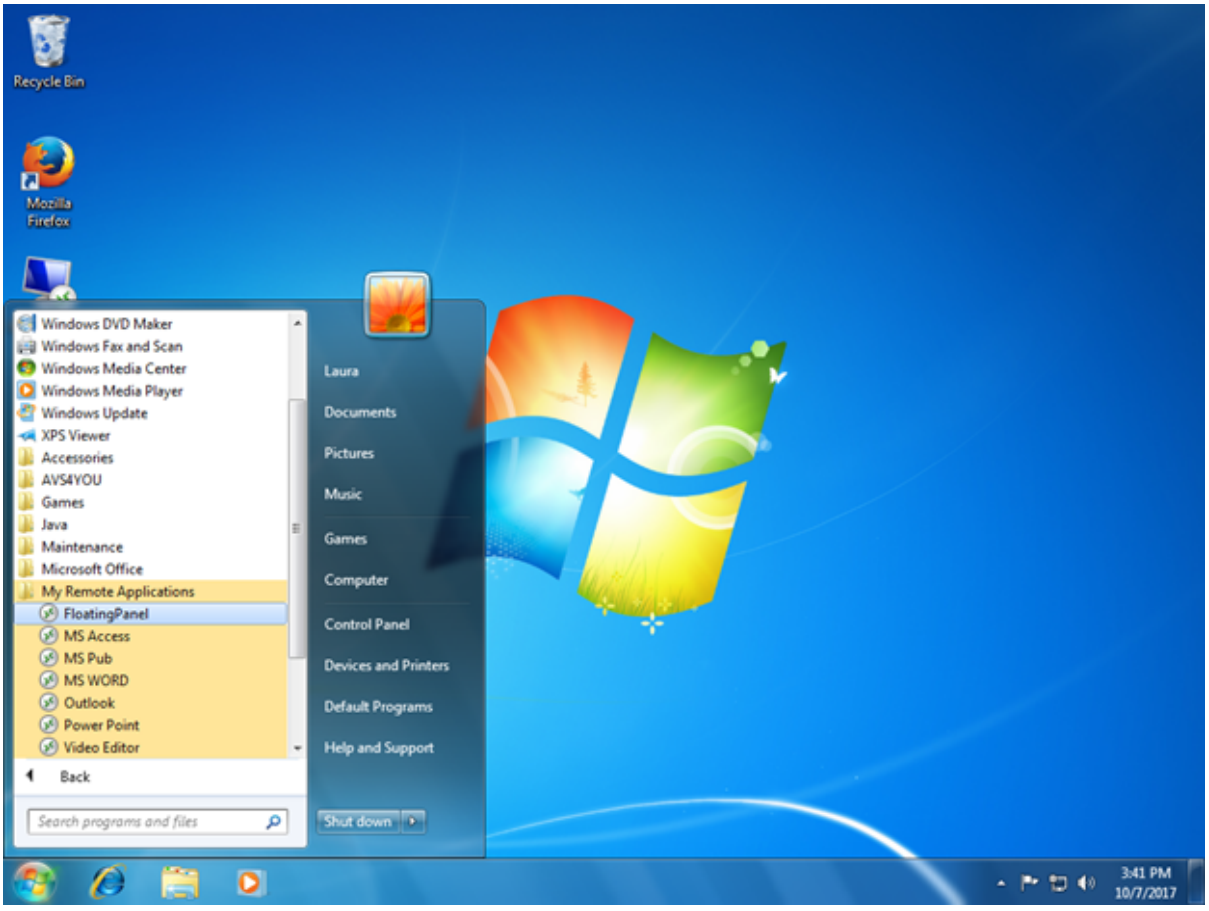
Puedes cambiar el nombre del menú como desees, haciendo clic en el Título del Menú de Aplicaciones Remotas a continuación y añadiéndolo en el cuadro de valor:



¿Qué sucederá en su PC cuando ejecute una vez su nuevo cliente generado: Verá un nuevo ícono en el área de notificaciones de su barra de tareas local?

Mi nuevo ícono de Aplicaciones Remotas	Menú de lista de aplicaciones
	

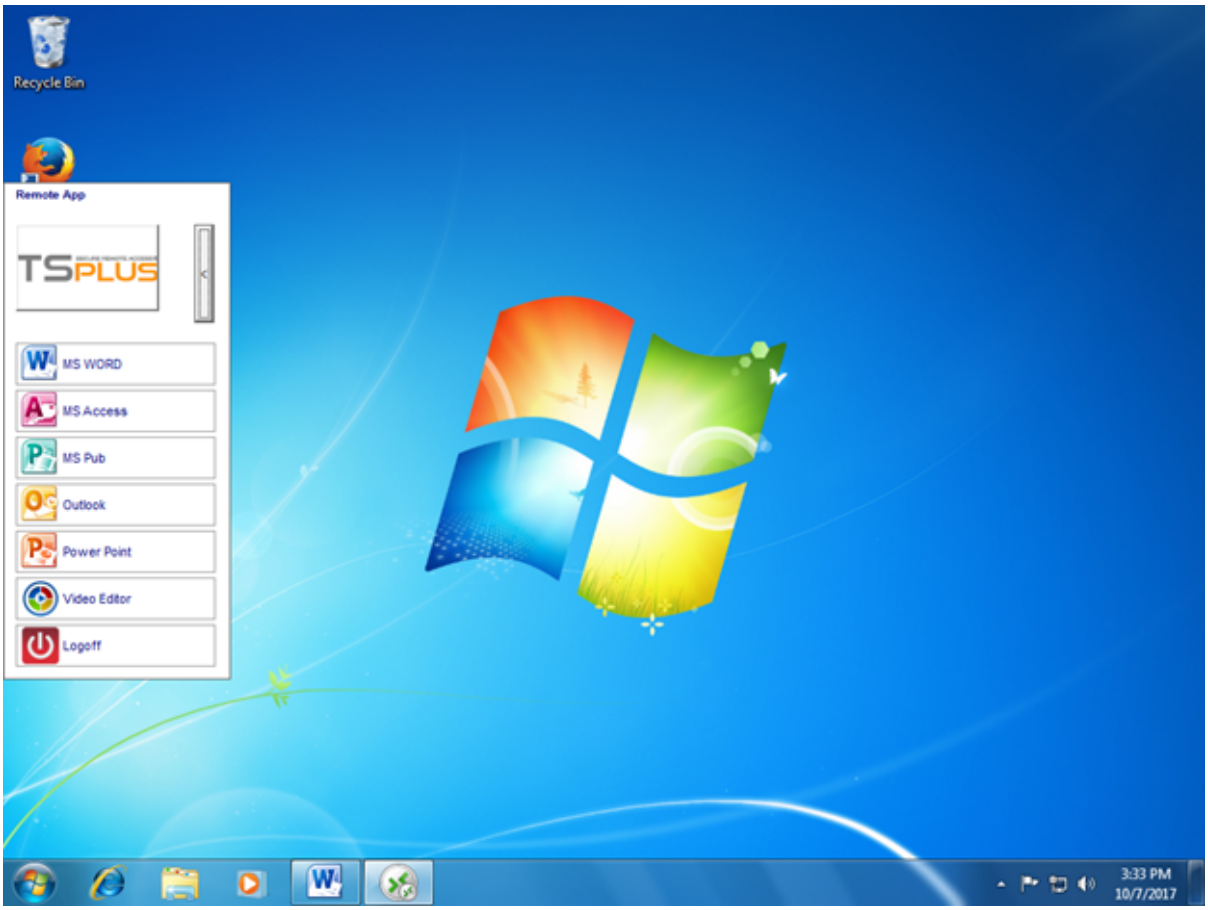
Ella también verá una nueva entrada en la lista de programas de su menú de inicio llamada **Mis Aplicaciones Remotas** :



Ella ahora podrá seleccionar una de estas aplicaciones listadas y comenzarla como una

RemoteApp. No necesitará usar el cliente generado LauraPortableClient.exe proporcionado.

Por ejemplo, si ella selecciona el Panel Flotante, obtendrá este resultado:

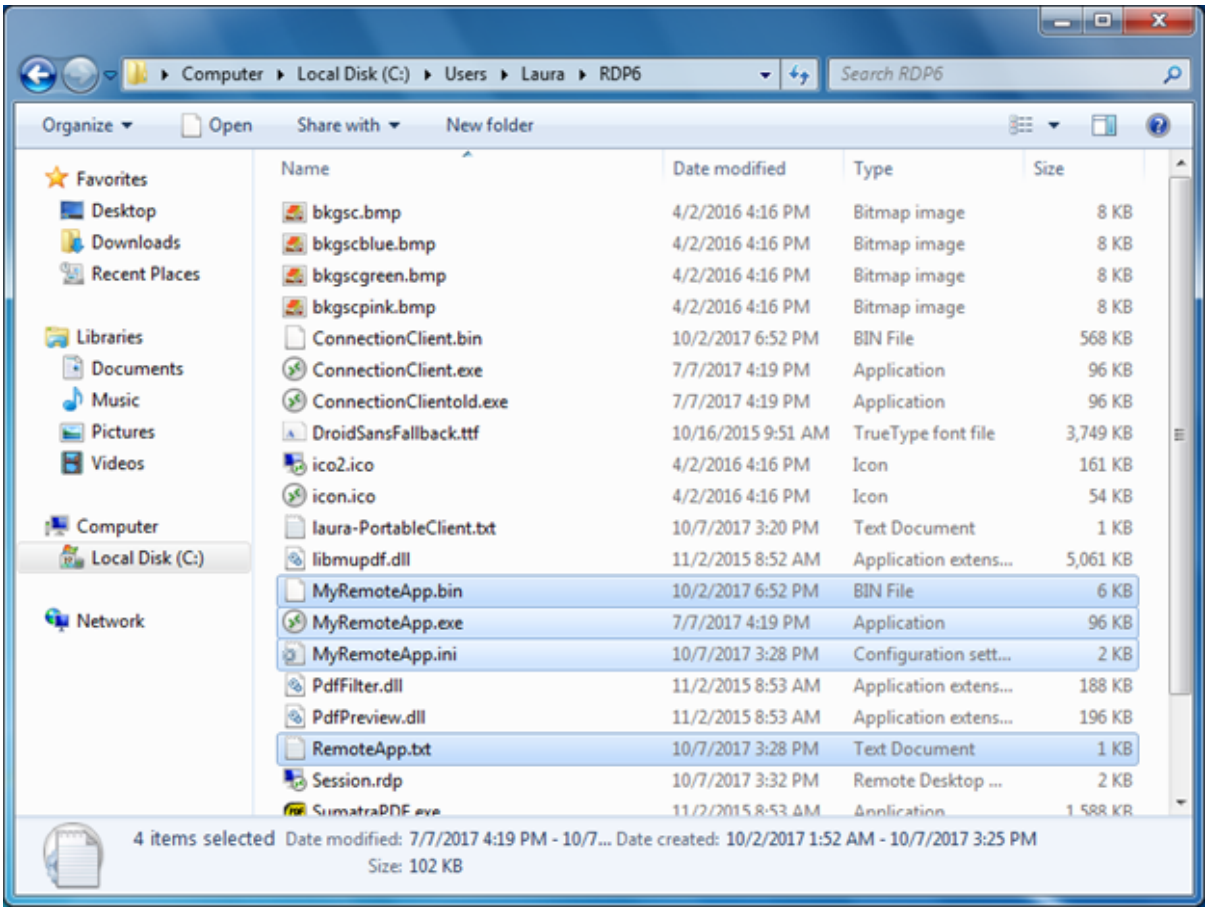


Antecedentes técnicos detrás de esta nueva tecnología.

El nuevo cliente generado de la versión 10.50 está agregando varios archivos en la carpeta C:\Users%UserName%\RDP6 del perfil de usuario del PC local.

MyRemoteApp.exe y MyRemoteApp.bin son los códigos de programa que se inician para crear el nuevo ícono en el área de notificación y la nueva entrada en la lista de Todos los programas del botón de Inicio.

MyRemoteApp.ini es un archivo recibido del servidor. Proporciona los detalles de cada aplicación que están asignadas a este usuario en el lado del servidor. Se actualiza en cada nueva conexión al servidor. Por lo general, toma 30 segundos después de cada inicio de sesión recibir este archivo del servidor. RemoteApp.txt proporciona el nombre del último cliente generado que se inició en este PC.



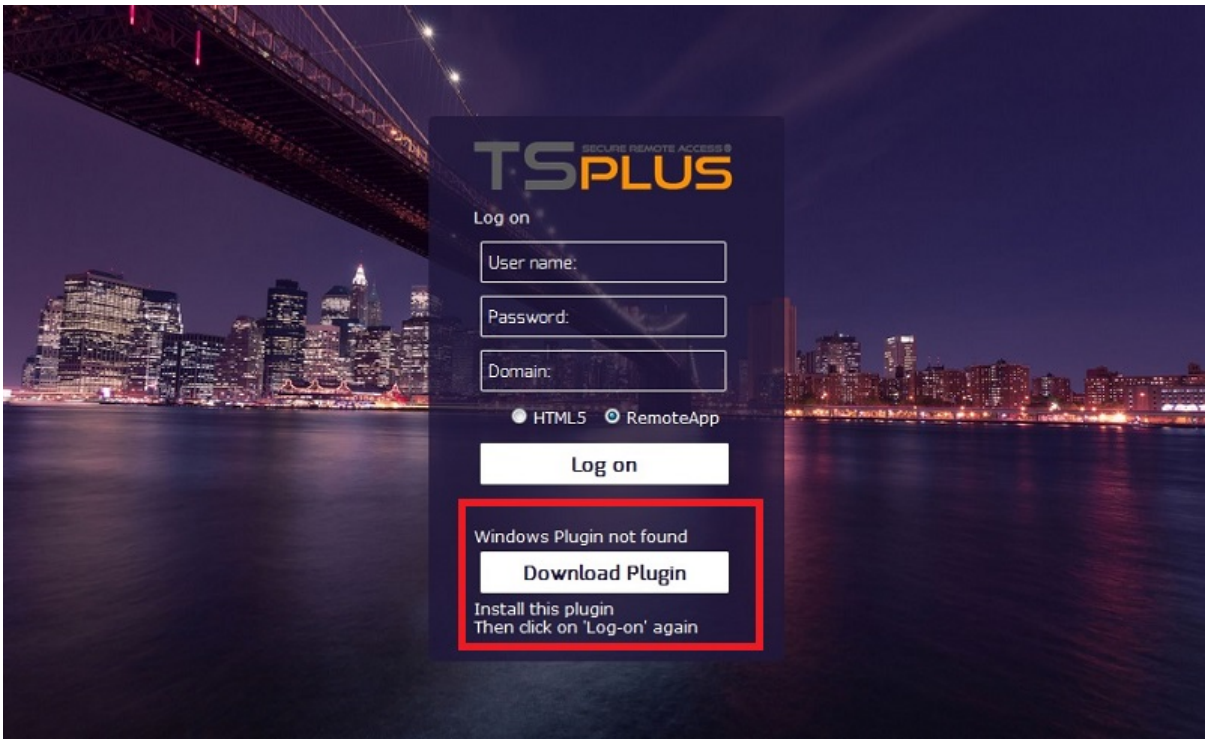
Comentarios:

Si el usuario tiene derechos de administrador en su propia PC, **MyRemoteApp.exe** se iniciará automáticamente en cada reinicio y el botón de Inicio también se actualizará. De lo contrario, el administrador debe ejecutar una vez el nuevo cliente generado "Como Administrador" para habilitar la nueva función. Al hacerlo, creará las entradas de registro adecuadas en HKLM. Si un usuario se conecta a solo un servidor, este nuevo sistema es perfecto. Sin embargo, si está utilizando varios clientes de conexión para abrir sesiones en diferentes servidores, debe tener en cuenta que el archivo **MyRemoteApp.ini** se actualizará con los valores de la última conexión. Puede ser confuso para el usuario y en tal caso de implementación recomendamos no usar esta nueva función.

Plugin de Aplicación Remota

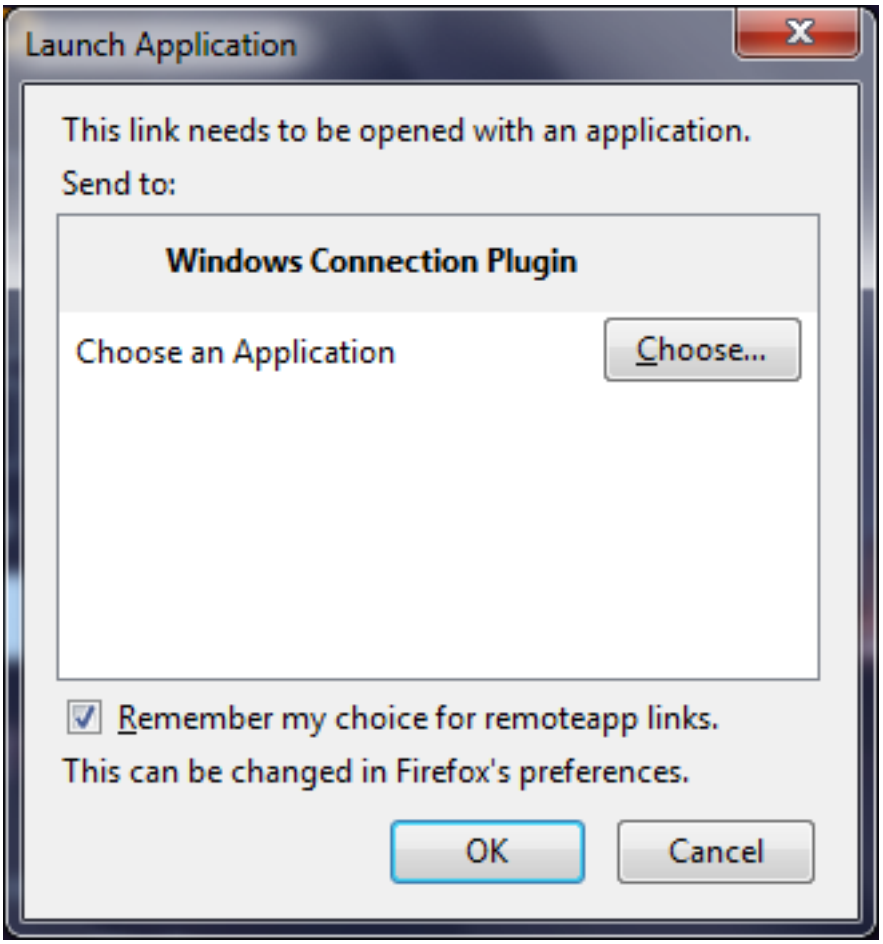
Desde la nueva versión 8.40 de TSplus, ya no es necesario instalar un complemento de Java en el navegador del cliente.

Ahora puede acceder al cliente Windows RemoteApp descargando e instalando un pequeño complemento de Windows a través del Portal Web. Esta operación es rápida y solo se necesita una vez por cliente.



También puede instalarlo en la carpeta C:\Program Files (x86)\TSplus\Clients\www\RemoteAppClient.

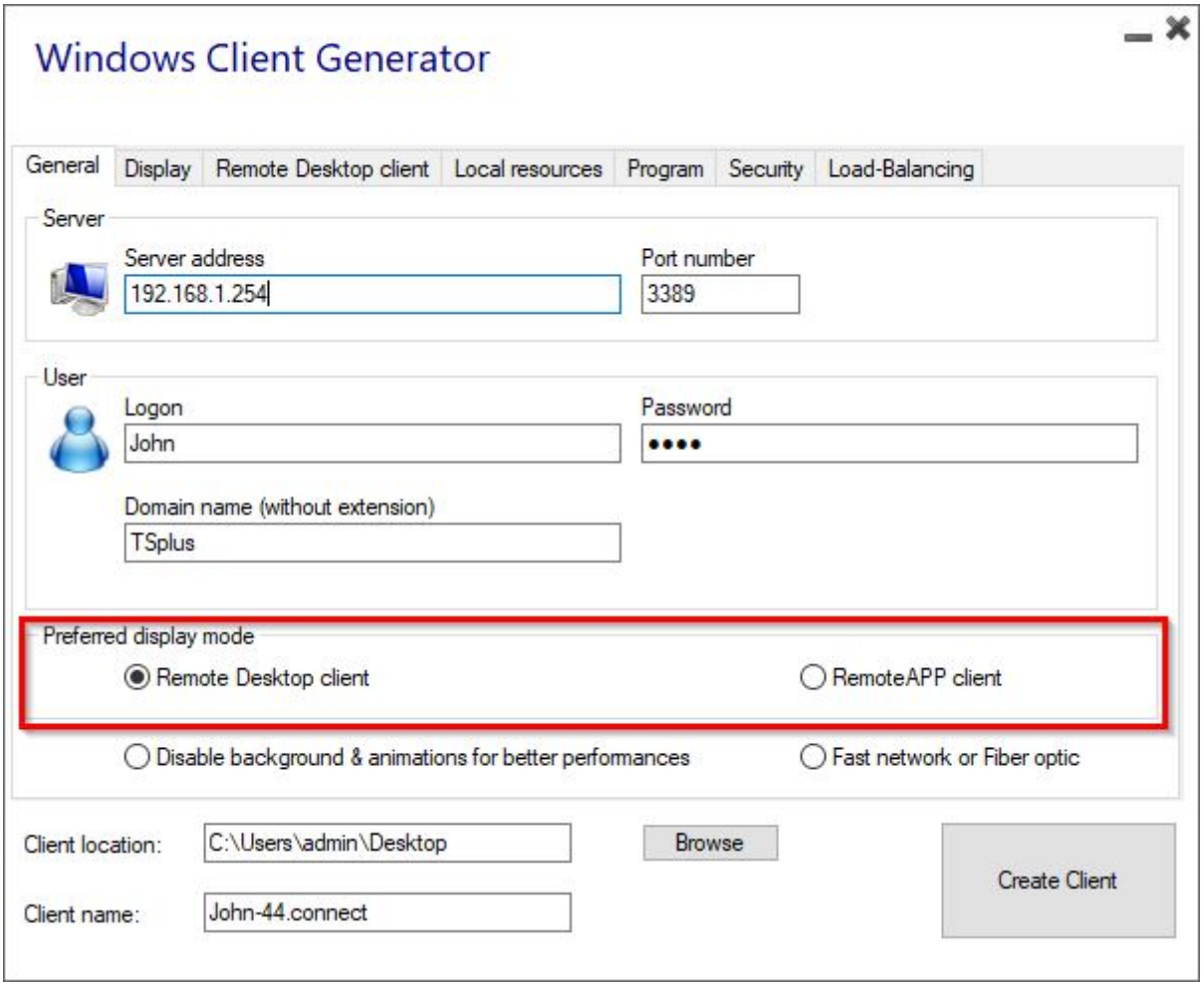
Al utilizar Firefox, este mensaje se mostrará en su primera conexión. Si elige la opción "recordar mis elecciones", la notificación se desactivará en futuras conexiones.



Nota Desde TSplus 12.40, la configuración del cliente RemoteApp y el El Programa de Configuración del Cliente se han fusionado y se pueden implementar con una sola configuración, por lo que si descargas la configuración del cliente RemoteApp, no será necesario descargar la del cliente de conexión.

Cliente de Conexión RemoteApp

Puedes elegir entre 2 modos de visualización en la pestaña general del generador de clientes:



###Cliente de conexión RemoteApp

El cliente de conexión RemoteApp no depende de la configuración del color de transparencia.

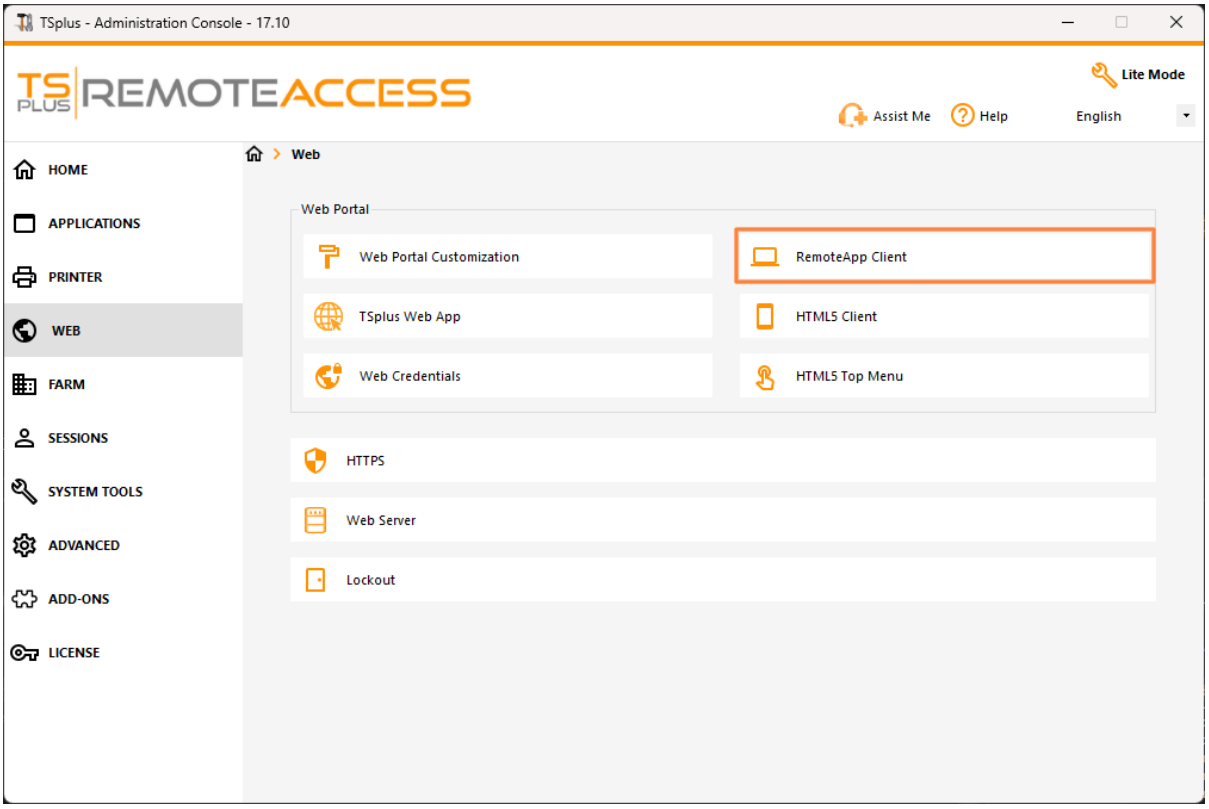
Esto permite una visualización perfecta de la aplicación, así como un comportamiento nativo de Windows.

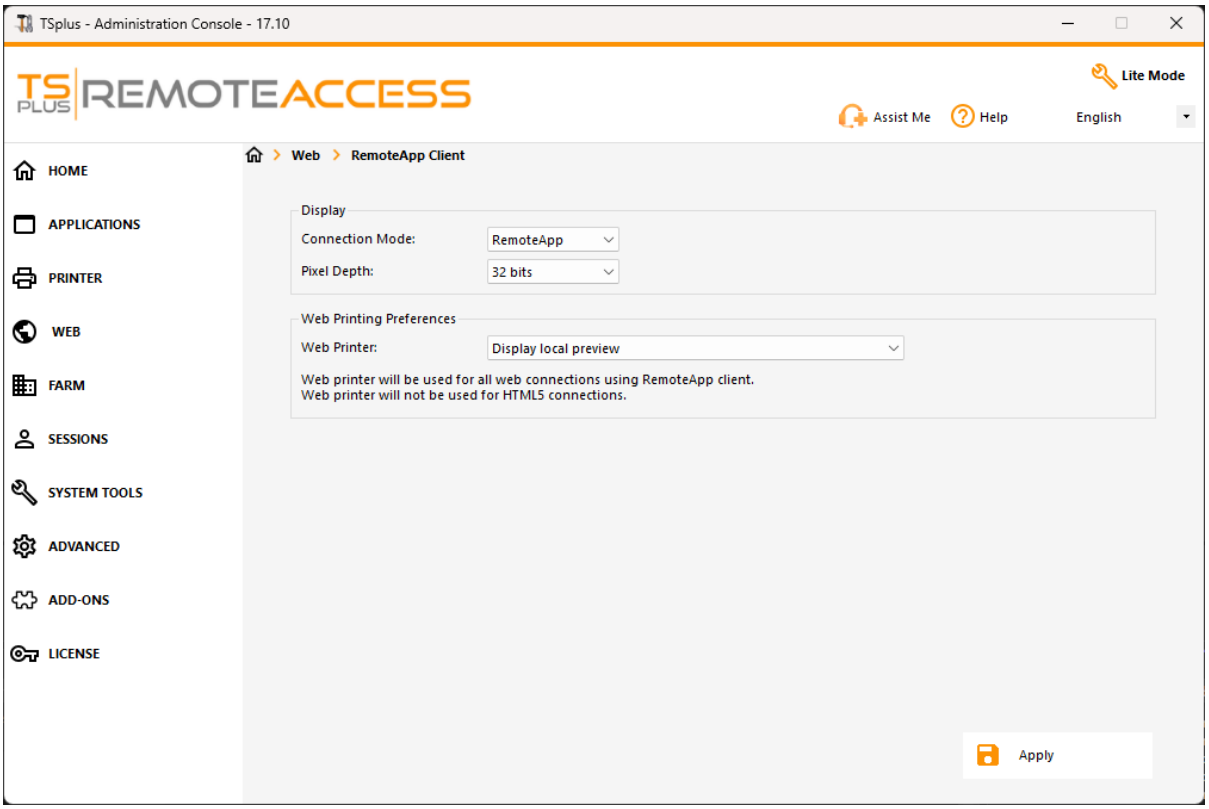
- En el lado del cliente, se requiere la instalación de RDP6 o superior.

- En el lado del servidor, TSplus debe estar instalado en una máquina que ejecute Windows 7 hasta Windows Server 2019.

Nota RemoteApp no es compatible con Windows 10 1803 y 1809 Home Windows 2019 Essentials Editions.

Puedes cambiar las preferencias de visualización y de impresión del cliente RemoteApp en la pestaña Web de la herramienta de administración:





Las aplicaciones minimizadas se pueden encontrar directamente dentro de la barra de tareas de Windows, como una aplicación local.

En este ejemplo, Firefox y Paint se inician localmente; Notepad, Word y Foxit se inician de forma remota.



Para el cliente de conexión Remoteapp, puede elegir publicar una única aplicación que se inicie sin problemas al iniciar sesión el usuario. También puedes publicar aplicaciones con el TSplus Remote Taskbar , el Panel Flotante o el Panel de Aplicaciones .

Ejecutar cliente de Windows en un entorno Proxy

Normalmente, el paquete SSH admite proxies HTTP(S) y esto debería ser suficiente para superar la mayoría de los proxies conocidos.

Sin embargo, existen casos muy difíciles en los que el entorno proxy no puede ser reconocido adecuadamente, está oculto de software de terceros o los servidores de destino están detrás de proxies inversos.

Para tales casos difíciles, el software contiene una solución que no es SSH llamada "modo de rescate".

Si puedes establecer una conexión HTML5, entonces puedes estar seguro de que este software te ayudará a establecer conexiones de socket nativas a través de Websocket (FF, Chrome, Opera, IE10, etc.) o XHR (IE6-IE9).

Ten cuidado, algunos proxies permiten Websocket/XHR tráfico solo a través de la capa HTTPS, así que usa la dirección https en lugar de http.

Si el proxy no solicita autenticación y puedes acceder a las páginas a través del navegador:

1. Abre http(s)://yourserver.com__/software/html5/jwres/__
2. Espere a que se establezca la conexión (y autorice la ejecución de Java si se le solicita)
3. Haz clic en el texto rojo “abrir el enlace” para abrir la página de acceso web en funcionamiento.
4. Utilice el acceso del cliente de Windows como de costumbre

Si las solicitudes de proxy requieren autenticación de proxy y puedes acceder a las páginas a través del navegador:

1. Abre http(s)://yourserver.com__/software/html5/jwres/__
2. Si el proxy solicita autenticación para applets de Java, presione "cancelar"
3. Haga clic en "Descargar LocalWebserver" y ejecútelo después de la descarga exitosa, eso iniciará el servidor http local en el puerto 18888.
4. Haga clic en "Forzar carga de applet desde http://localhost:18888 ", esto recargará la página con la carga de archivos JAR desde el servidor http local
5. Espere a que la conexión sea exitosa

6. Haz clic en el texto rojo “abrir el enlace” para abrir la página de acceso web en funcionamiento.
7. Utilice el acceso del cliente de Windows como de costumbre

Asegurando un servidor TSplus

Resumen

Asegurar cualquier servidor es una historia interminable donde cada experto podría añadir otro capítulo.

TSplus se beneficia de y es compatible con la infraestructura de seguridad existente en una empresa (Active Directory, GPOs, servidores HTTPS, sistemas de telecomunicaciones SSL o SSL, VPN, control de acceso con o sin tarjetas de identificación, etc).

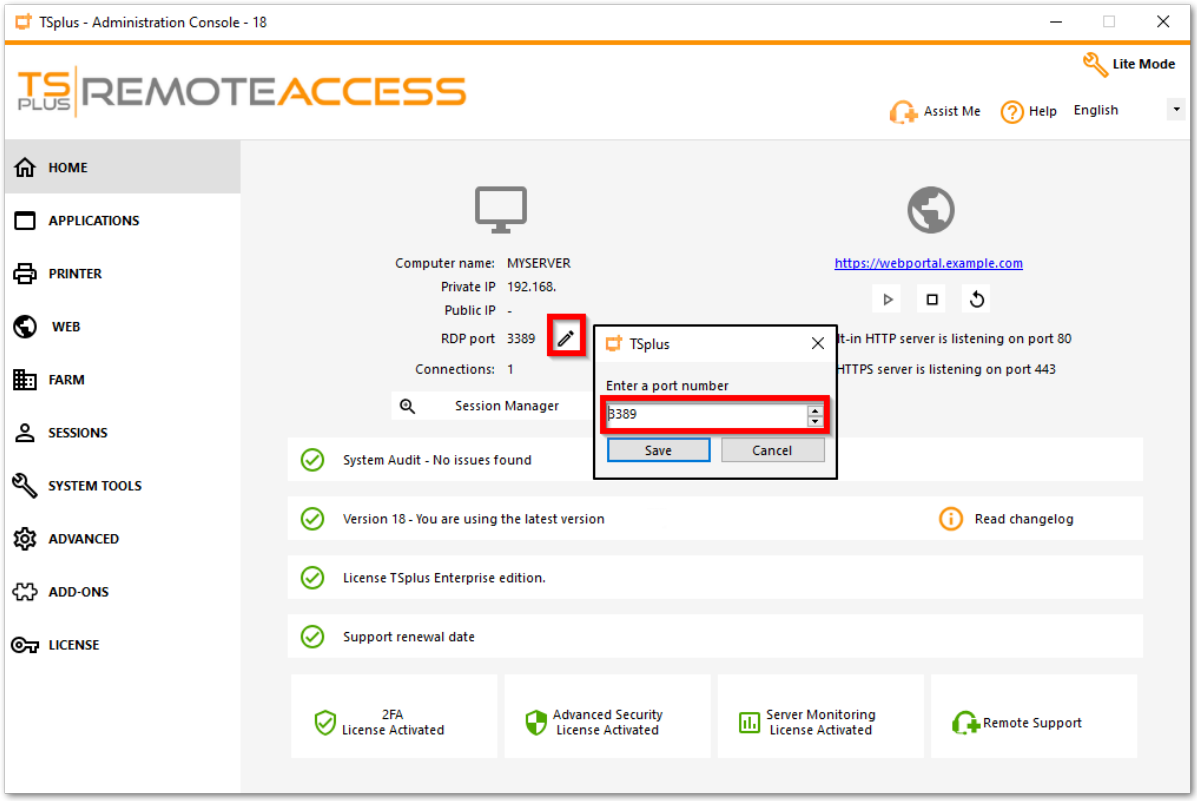
Para los clientes que desean asegurar fácilmente sus servidores, TSplus ofrece un conjunto de formas simples y efectivas de imponer buenos niveles de seguridad.

Con el AdminTool, puedes seleccionar un número de puerto TCP/IP diferente para que el servicio RDP acepte conexiones. El predeterminado es 3389.

Puedes elegir cualquier puerto arbitrario, asumiendo que no esté ya en uso en tu red y que configures el mismo número de puerto en tus firewalls y en cada uno de los programas de acceso de usuario de TSplus.

TSplus incluye una capacidad única de reenvío de puertos y túneles: independientemente del puerto RDP que se haya configurado, el RDP también estará disponible en el número de puerto HTTP y HTTPS.

Si los usuarios quieren acceder a su servidor TSplus desde fuera de su red, debe asegurarse de que todas las conexiones entrantes en el puerto elegido se reenvíen al servidor TSplus. En la pestaña de Inicio, haga clic en el botón de lápiz junto a "Puerto RDP":



Cambia el puerto RDP y guarda.

Opciones de seguridad del lado del servidor

El AdminTool te permite denegar el acceso a cualquier usuario que no esté utilizando un programa de conexión de TSplus generado por el administrador. En este caso, cualquier usuario que intente abrir una sesión con cualquier cliente de Escritorio Remoto que no sea el de TSplus (suponiendo que tenga la dirección del servidor correcta, el número de puerto, un inicio de sesión válido y una contraseña válida) será desconectado automáticamente.

El administrador puede decidir que solo los miembros del grupo de usuarios de Escritorio Remoto. se le permitirá abrir una sesión.

El administrador puede decidir que una contraseña es obligatoria para abrir una sesión.

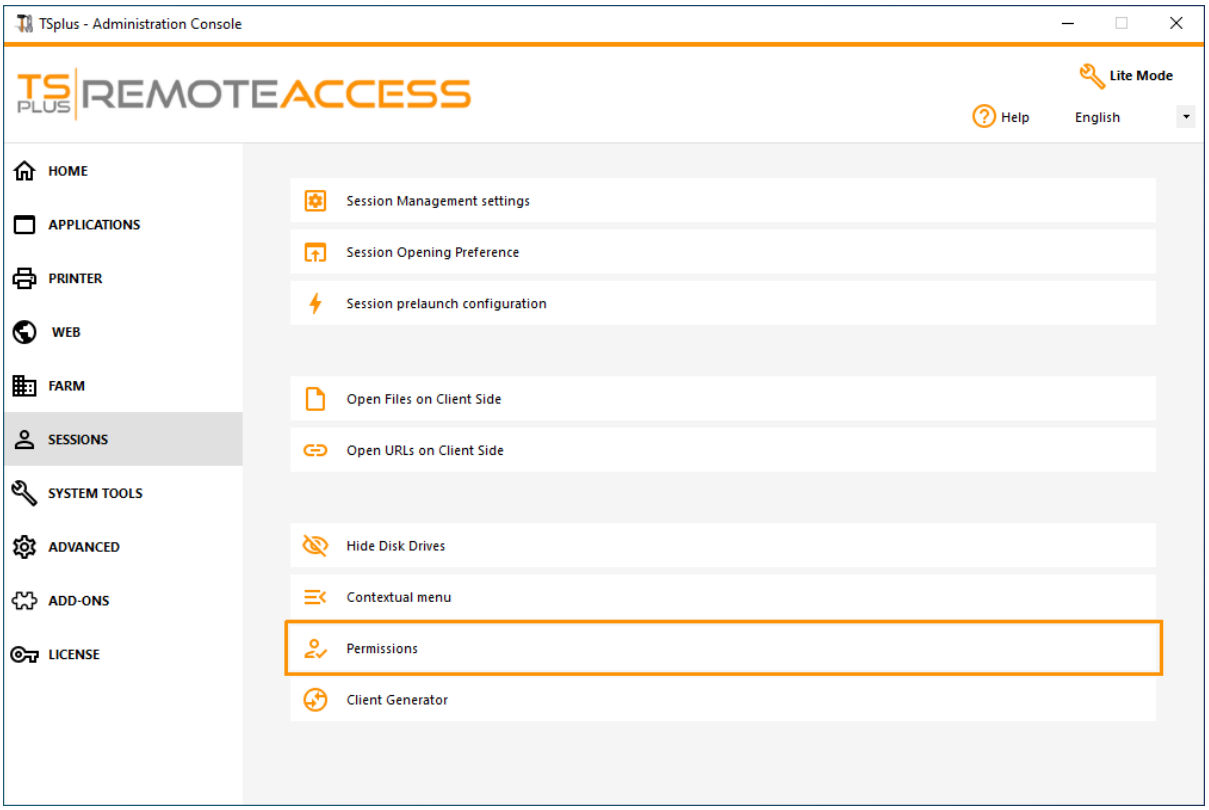
A través de la configuración de la Política de Grupo local aplicable, el administrador puede especificar si se debe imponer un nivel de cifrado para todos los datos enviados entre el cliente y el ordenador remoto durante una sesión de Servicios de Terminal.

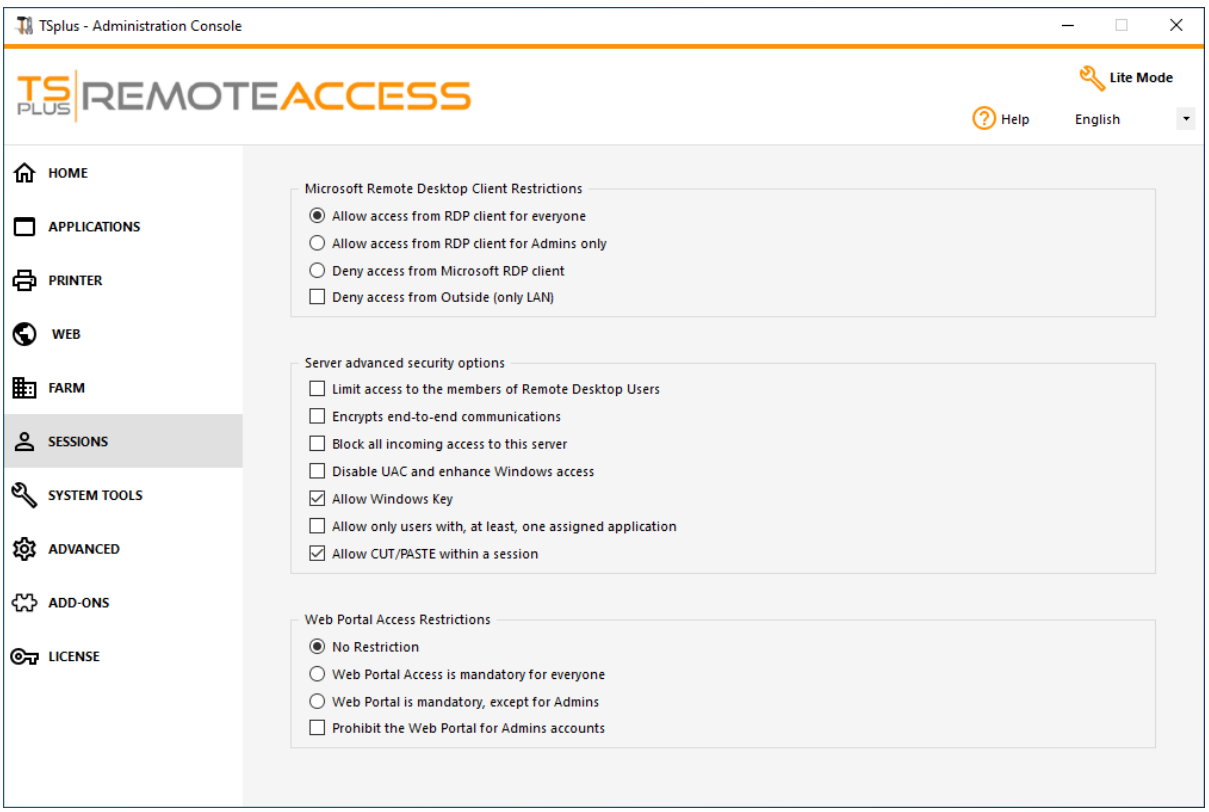
Si el estado está configurado como Habilitado, la encriptación para todas las conexiones al servidor se establece al nivel decidido por el administrador. Por defecto, la encriptación se establece en Alta.

El administrador también puede establecer como regla que solo los usuarios con un cliente de conexión de TSplus podrán abrir una sesión.

Cualquier acceso entrante con un RDP estándar o un acceso web será rechazado automáticamente.

Puedes encontrar múltiples opciones de seguridad avanzada si haces clic en la pestaña Sesiones - Permisos:



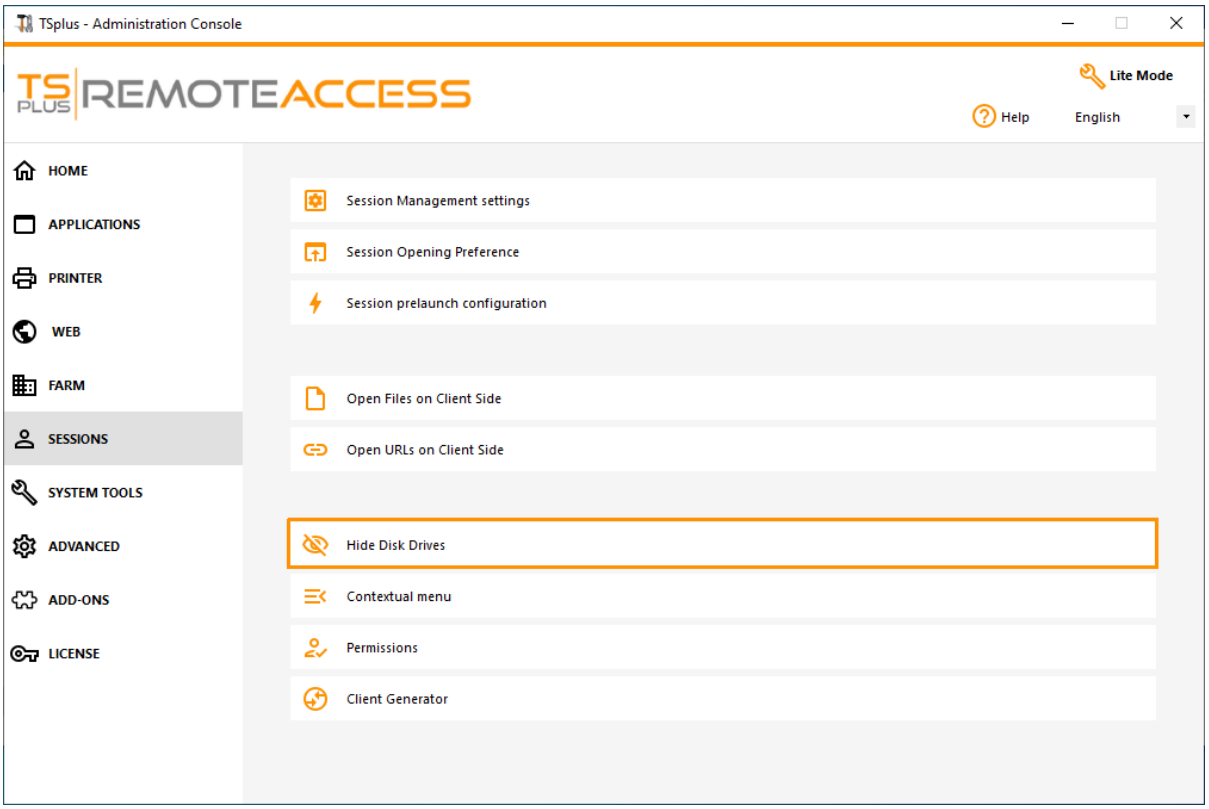


- **Permitir acceso desde el cliente RDP de Microsoft para todos:** Permite a cada usuario conectarse utilizando mstsc.exe.
- **Permitir acceso desde el cliente RDP de Microsoft solo para administradores:** Permite solo a los administradores conectarse usando mstsc.exe.
- **Denegar el acceso desde el cliente RDP de Microsoft:** Evitar que alguien pueda conectarse utilizando mstsc.exe.
- **Denegar acceso desde el exterior:** Significa que solo las IPs privadas de la LAN podrán abrir una sesión.
- **Limitar el acceso a los miembros de los usuarios de Remote Desktop:** Este límite se aplica solo a este grupo local de usuarios (que puedes ver haciendo clic en el Usuarios y grupos tile .
- **Encripta las comunicaciones de extremo a extremo:** Alta cifra la comunicación cliente/ servidor utilizando cifrado de 128 bits. Utilice este nivel cuando los clientes que acceden al servidor terminal también admitan cifrado de 128 bits.
- **Bloquear todo el acceso entrante a este servidor:** Todas las sesiones activas permanecerán activas, mientras que todos los intentos de conexiones entrantes serán bloqueados. Asegúrese de que puede acceder físicamente a la consola del servidor si marca esta casilla. No utilice esta opción si su servidor está alojado en un entorno de Cloud.
- **Desactivar UAC y mejorar el acceso a Windows:** Desactiva los Controles de Cuentas de Usuario, elimina todos los mensajes de seguridad no deseados de Windows. limitación de usuarios (mensajes) al iniciar aplicaciones.
- **La casilla "Permitir tecla de Windows"** permitir el uso de las teclas de Windows y combinaciones dentro de una sesión de TSplus.
- **Permitir solo usuarios con al menos una aplicación asignada:** Usuario con una aplicación y más pueden abrir una sesión.
- **Permitir CORTAR/PEGAR dentro de una sesión:** desmarcar esta casilla desactivará los comandos CTRL C/CTRL V

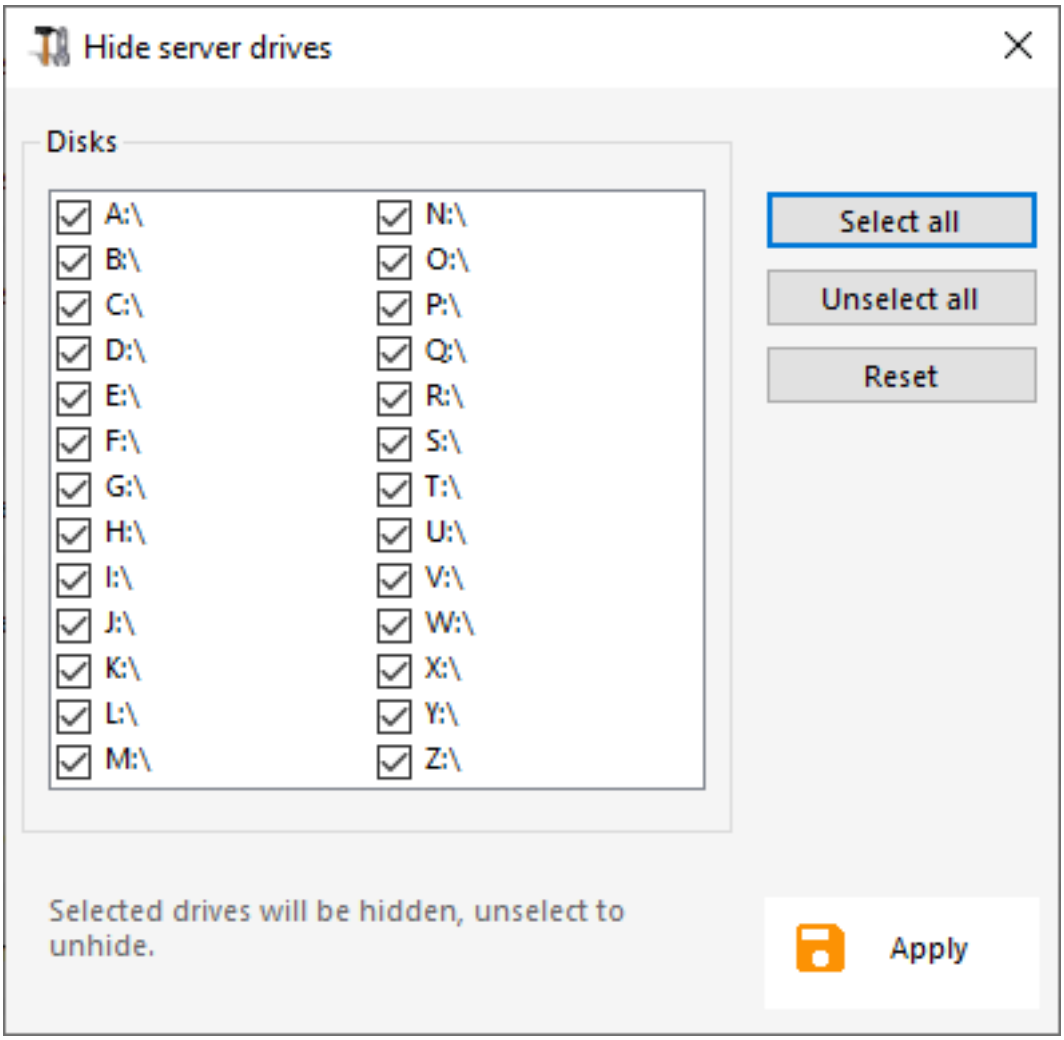
Restricciones de acceso al portal web

- Sin Restricción
- El Portal Web es obligatorio para todos: los usuarios solo pueden conectarse a través del Portal Web.
- El portal web es obligatorio, excepto para los administradores: los usuarios solo pueden conectarse a través del portal web, excepto los administradores.
- Prohibir el Portal Web para cuentas de Administradores: Los administradores no pueden conectarse a través del Portal Web.

El AdminTool incluye una herramienta que permite ocultar las unidades de disco del servidor para evitar que los usuarios accedan a carpetas a través de Mi PC o cuadros de diálogo estándar de Windows. En la pestaña de Sesiones, haga clic en "Ocultar unidades de disco".



Esta herramienta funciona a nivel global. Esto significa que incluso el administrador no tendrá acceso normal a las unidades después de que se hayan aplicado los ajustes. En el ejemplo a continuación, se han seleccionado todos los controladores con el botón "seleccionar todo", que marcará todas las casillas correspondientes a las unidades que estarán ocultas para todos.



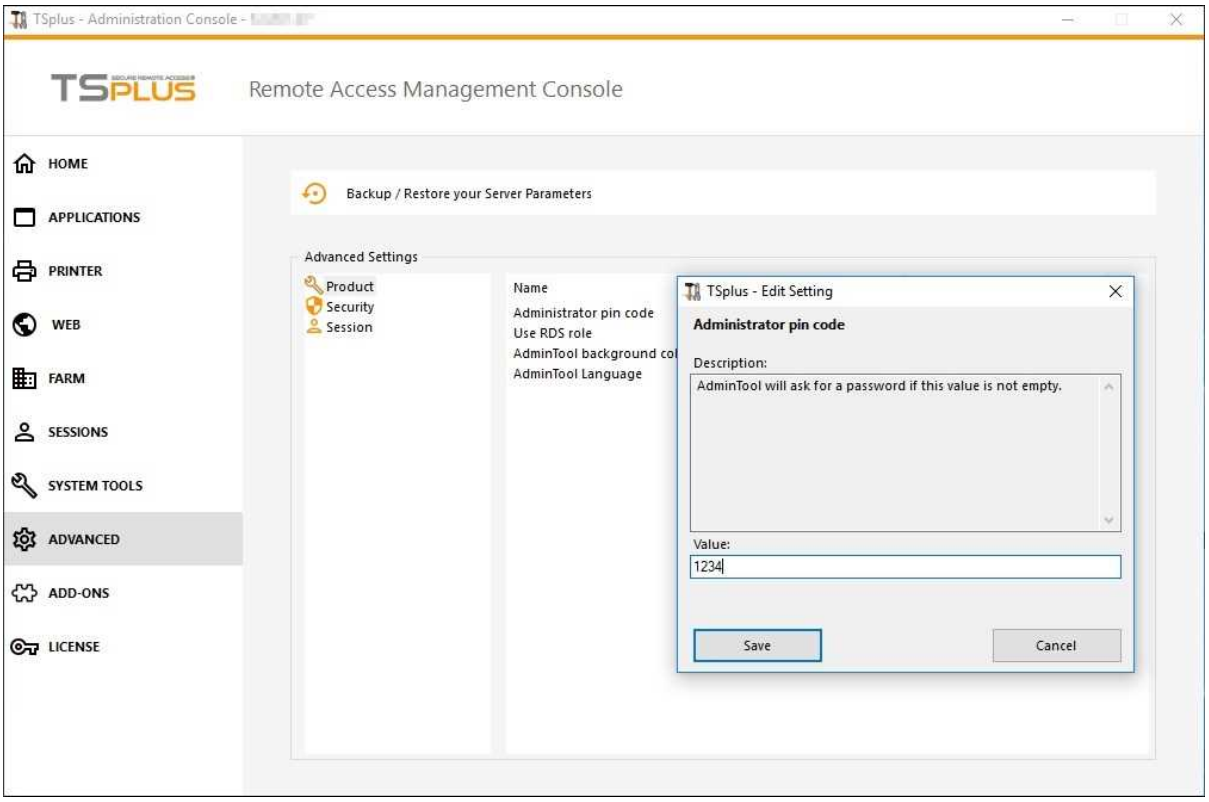
Notas: Esta funcionalidad es poderosa y no desactiva el acceso a las unidades de disco. Solo impide que el usuario las muestre.

La herramienta marca las unidades de disco como ocultas, pero también agrega la propiedad OCULTO a todas las carpetas raíz y a la lista de usuarios en Documentos y Configuración.

Si el administrador quiere ver estos archivos, debe:

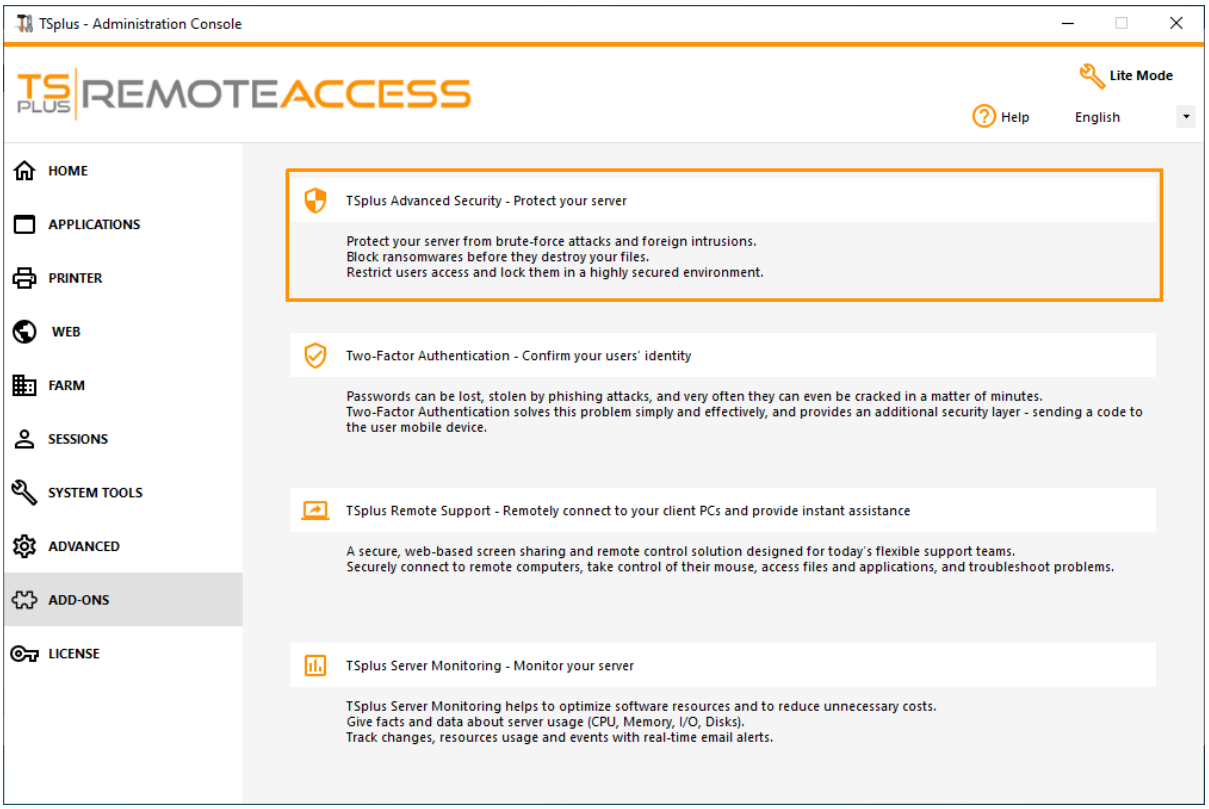
1. Escriba la letra de la unidad de disco. Por ejemplo: **D:** que te llevará a la unidad D:.
2. Activar **MOSTRAR ARCHIVOS Y CARPETAS OCULTOS** en las propiedades de vista de la carpeta.

El Administrador puede asegurar el acceso a la Herramienta del Administrador configurando un código PIN que se solicitará en cada inicio, en la pestaña Avanzada de la AdminTool, bajo la Configuración del Producto:

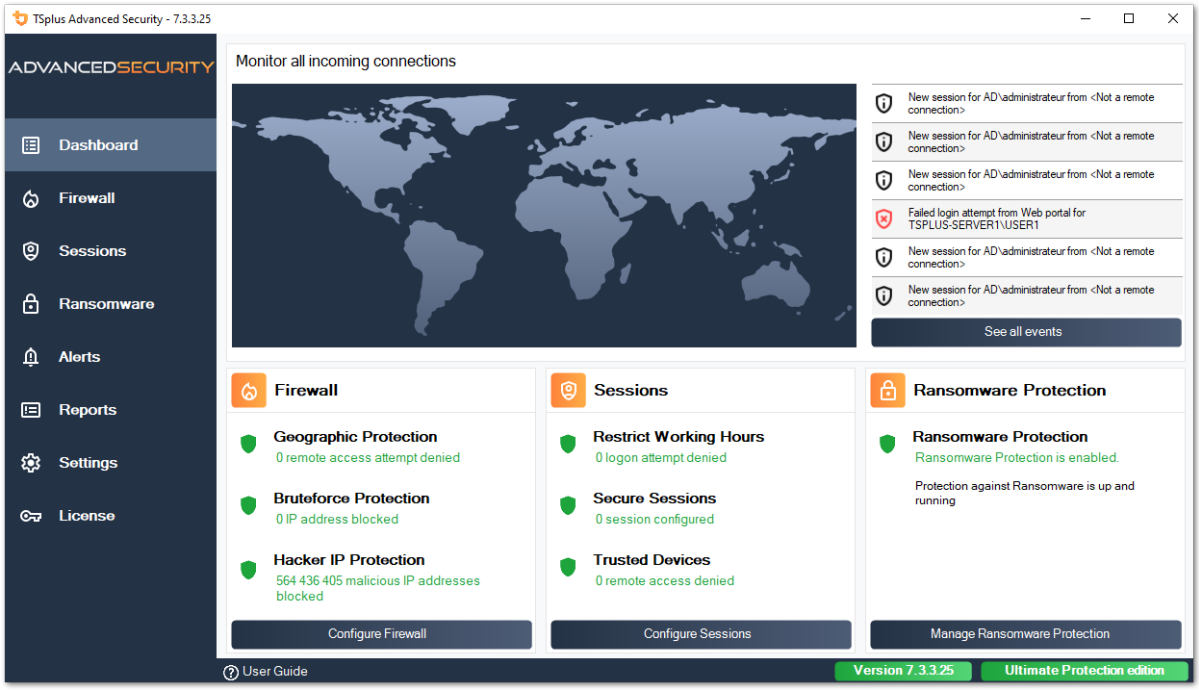


TSplus Advanced Security Ultimate

Desde la versión 11.40 de TSplus, encontrará una herramienta de complemento de seguridad única, que puede iniciar en la pestaña de complementos:



Lo que trae características potentes, documentadas en esta página .



El rol de Protección contra Fuerza Bruta en el Portal Web se describe en esta página .

Autenticación de Dos Factores

Desde la versión 12 de TSplus, puedes habilitar la autenticación de dos factores como un complemento para tu Portal Web de TSplus.



Más información sobre esta increíble nueva función se puede encontrar en esta página .

Certificados SSL

El proceso de certificados SSL se detalla en estas páginas:

- TSplus proporciona una herramienta fácil de usar para generar un certificado SSL gratuito y válido: Certificado SSL gratuito y fácil de instalar
- HTTPS y certificados SSL de terceros .

- Elija su Conjuntos de cifrado para mejorar la seguridad .

Opciones de seguridad del programa de acceso de TSplus:

El generador de clientes de TSplus ofrece la capacidad, en su pestaña de Seguridad, de bloquear el cliente de TSplus a:

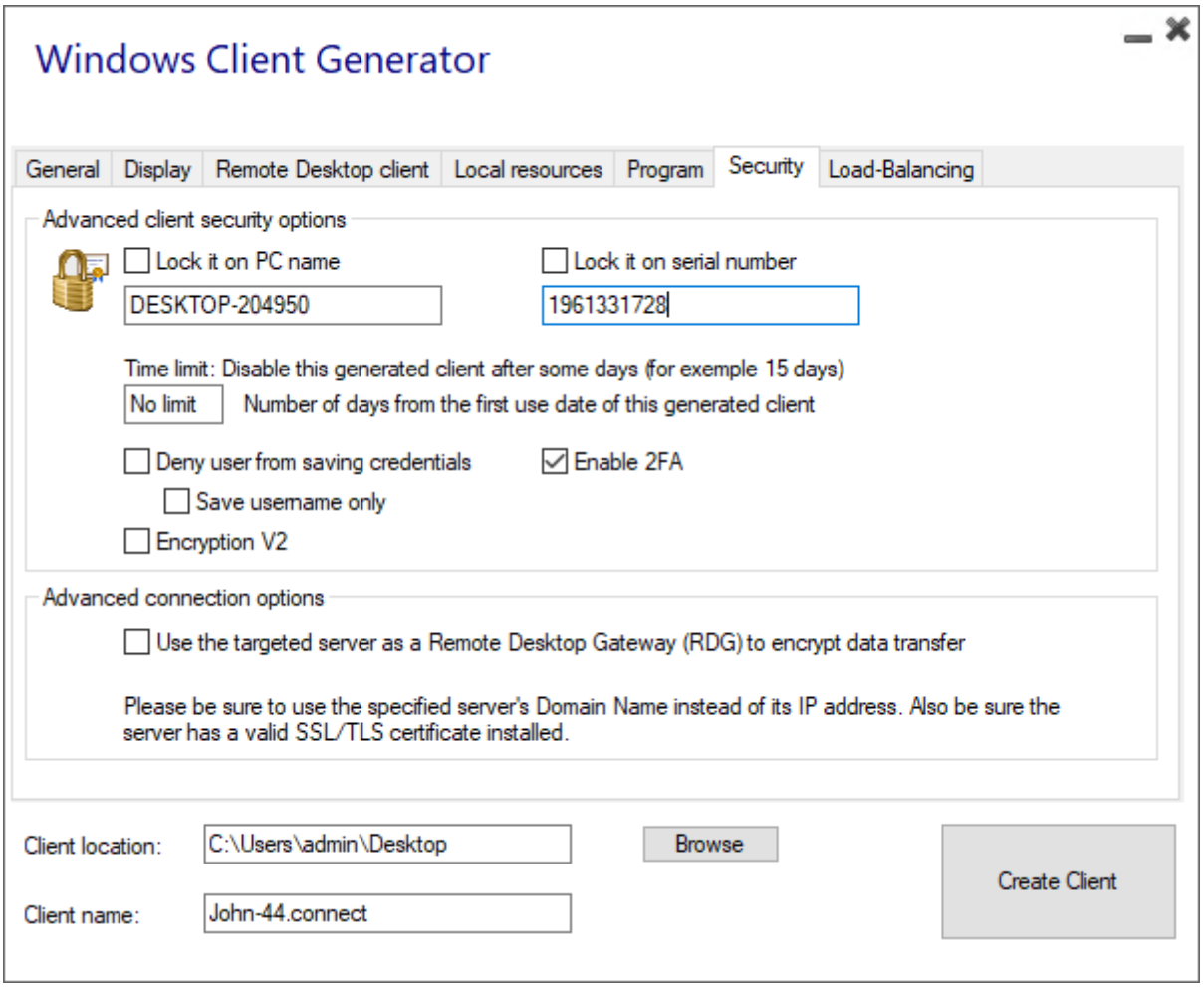
- Un nombre de PC específico. Significa que este programa no podrá iniciarse desde ningún otro PC.

- Un número de serie de unidad física (HDD de PC o memoria USB). Esta es una forma muy fácil y poderosa de establecer un alto nivel de seguridad.

  La única forma de conectarse es con un cliente específico, y este cliente específico solo puede iniciarse en una memoria USB específica o en el disco duro de un PC.

  Algunos de nuestros clientes están entregando llaves USB con lectura de huellas dactilares a cada uno de sus usuarios y cada programa generado está bloqueado al número de serie del dispositivo.

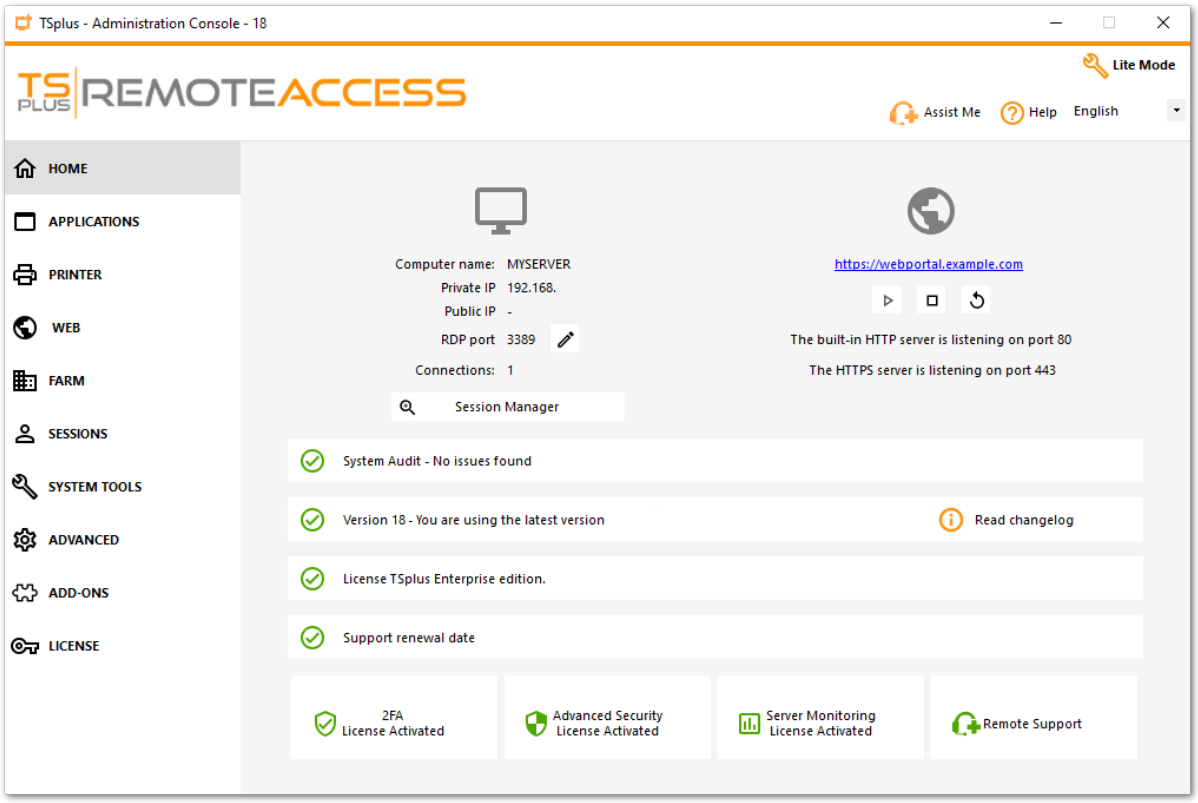
  De esta manera, pueden restringir el acceso al programa del cliente en sí, así como asegurarse de que no se pueda copiar del USB y utilizar en otro lugar.



Para más información sobre las características de seguridad, consulte Documentación del Generador de Clientes Portátiles de TSplus y nuestras preguntas frecuentes.

Gestión del Servidor

En la pestaña de Inicio de AdminTool, puedes ver toda la información necesaria sobre tu servidor TSplus:



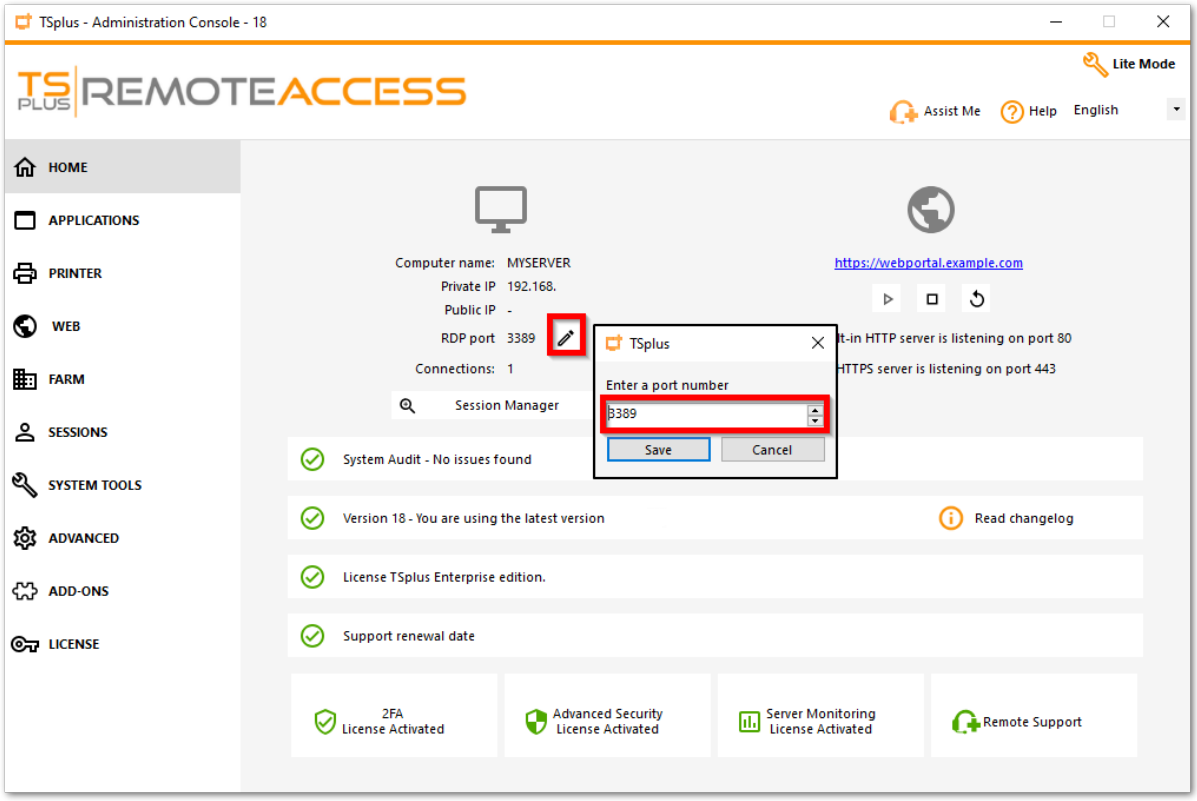
Cambiando el número de puerto RDP y configurando el firewall

Con el AdminTool, puedes seleccionar un número de puerto TCP/IP diferente para que el servicio RDP acepte conexiones. El predeterminado es 3389. Puedes elegir cualquier puerto arbitrario, siempre que no esté ya en uso en tu red y que configures el mismo número de puerto en tus firewalls y en cada uno de los programas de acceso de usuario de TSplus.

TSplus incluye una capacidad única de reenvío de puertos y túneles: independientemente del puerto RDP que se haya configurado, el RDP también estará disponible en el número de puerto

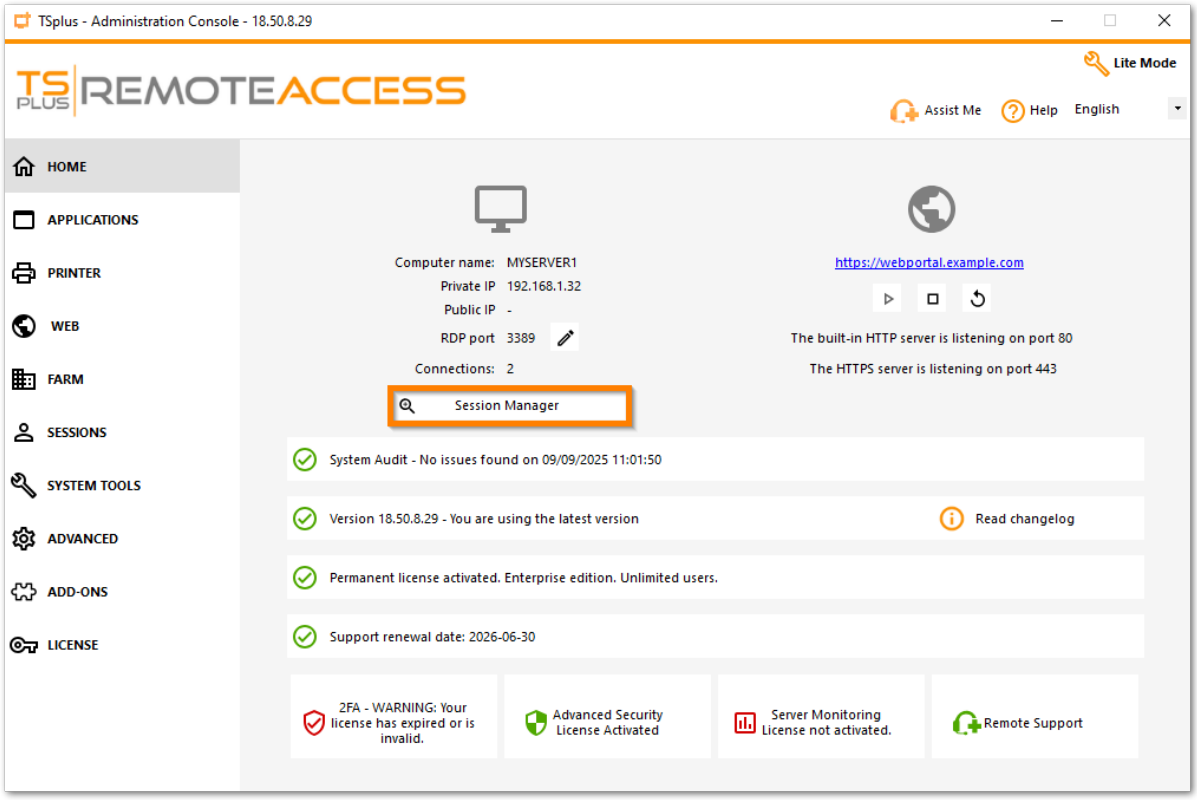
HTTP y HTTPS.

Si los usuarios quieren acceder a su servidor TSplus desde fuera de su red, debe asegurarse de que todas las conexiones entrantes en el puerto elegido se reenvíen al servidor TSplus.

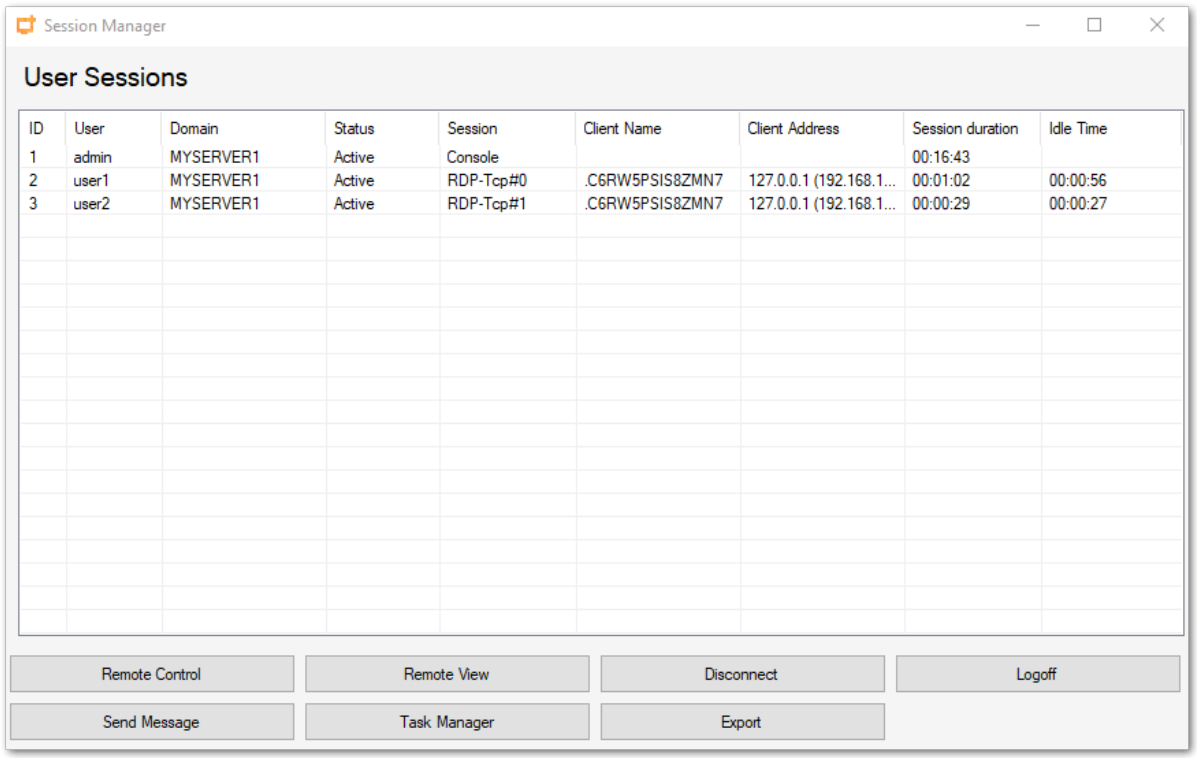


Gestión de usuarios y sesiones

El administrador de sesiones se encuentra justo debajo del puerto RDP:



Puedes mostrar el administrador de tareas de tu servidor, y tienes la posibilidad de activar un control remoto, desconectar, cerrar sesión o enviar un mensaje a tus usuarios.



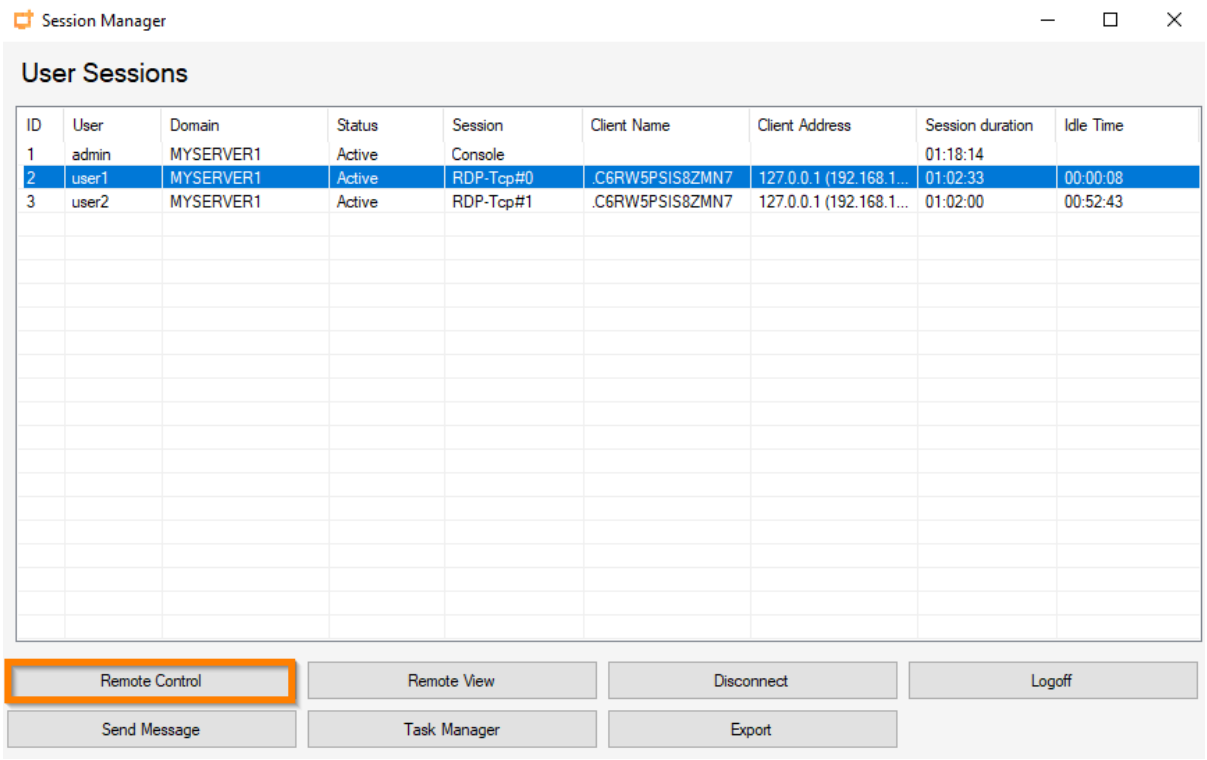
Puedes activar el control remoto a través de una sesión remota con una cuenta de administrador en los siguientes sistemas operativos:

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows 7
- Windows 8.1
- Windows 10 pro y superior

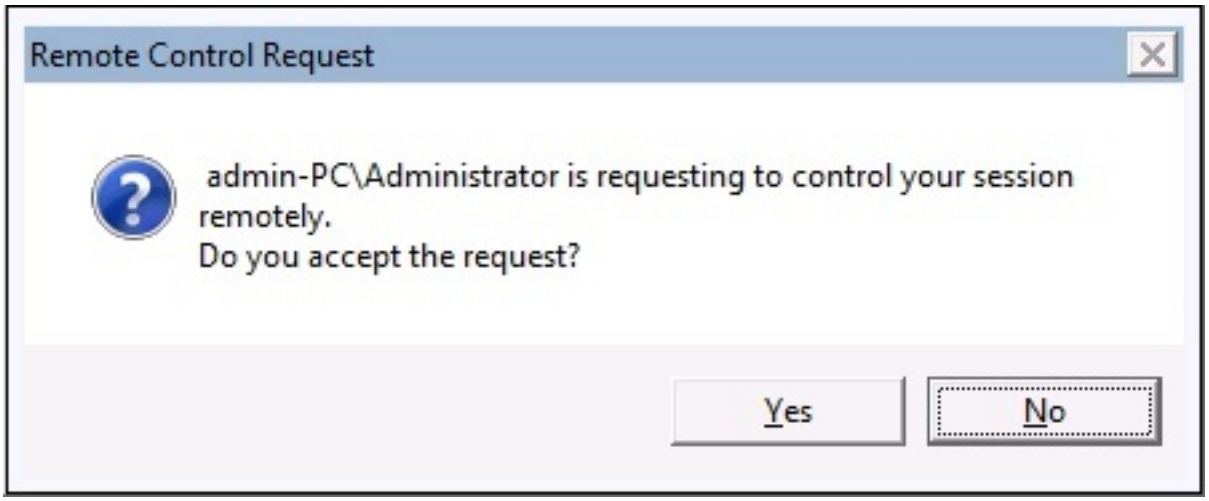
En Windows XP, 2003, Vista y 2008 no hay botón de control remoto.

En Windows 2012 y 8 aparece un mensaje que le aconseja actualizar a 2012 R2 o 8.1.

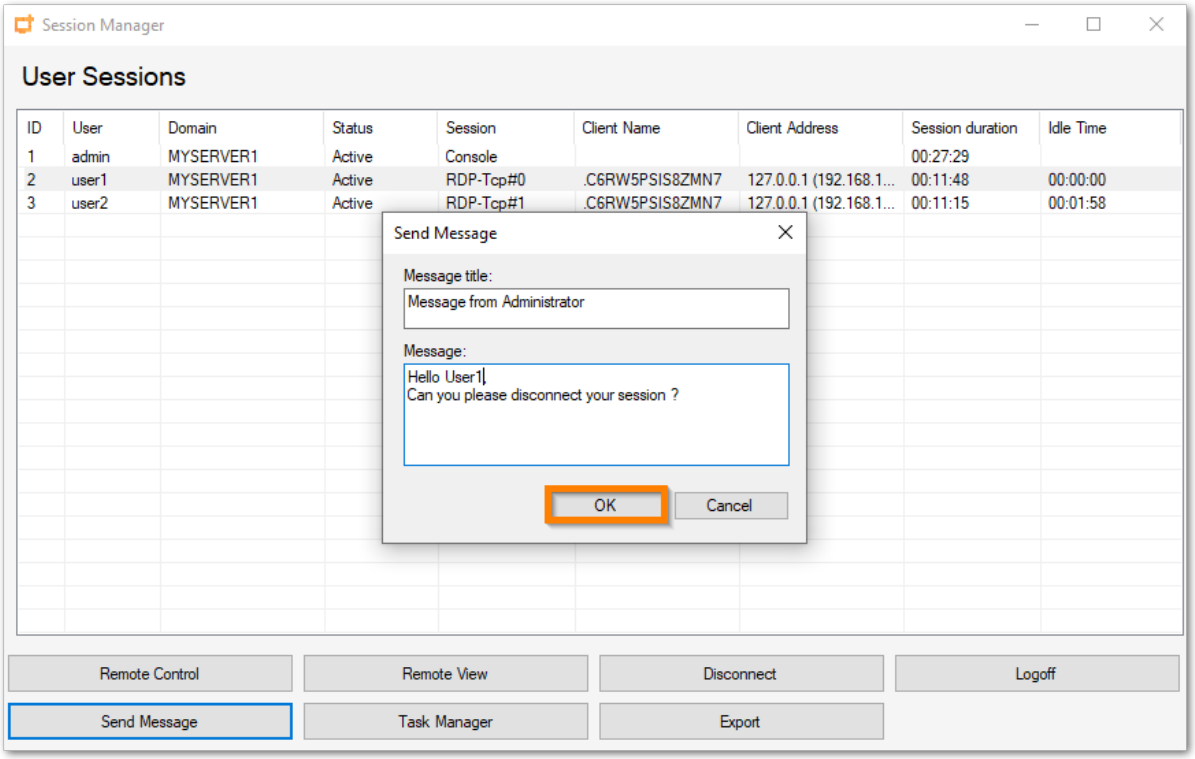
Cuando activas el control remoto para la sesión de un usuario, aparece este mensaje, indicando el atajo de teclado para finalizar la sesión:



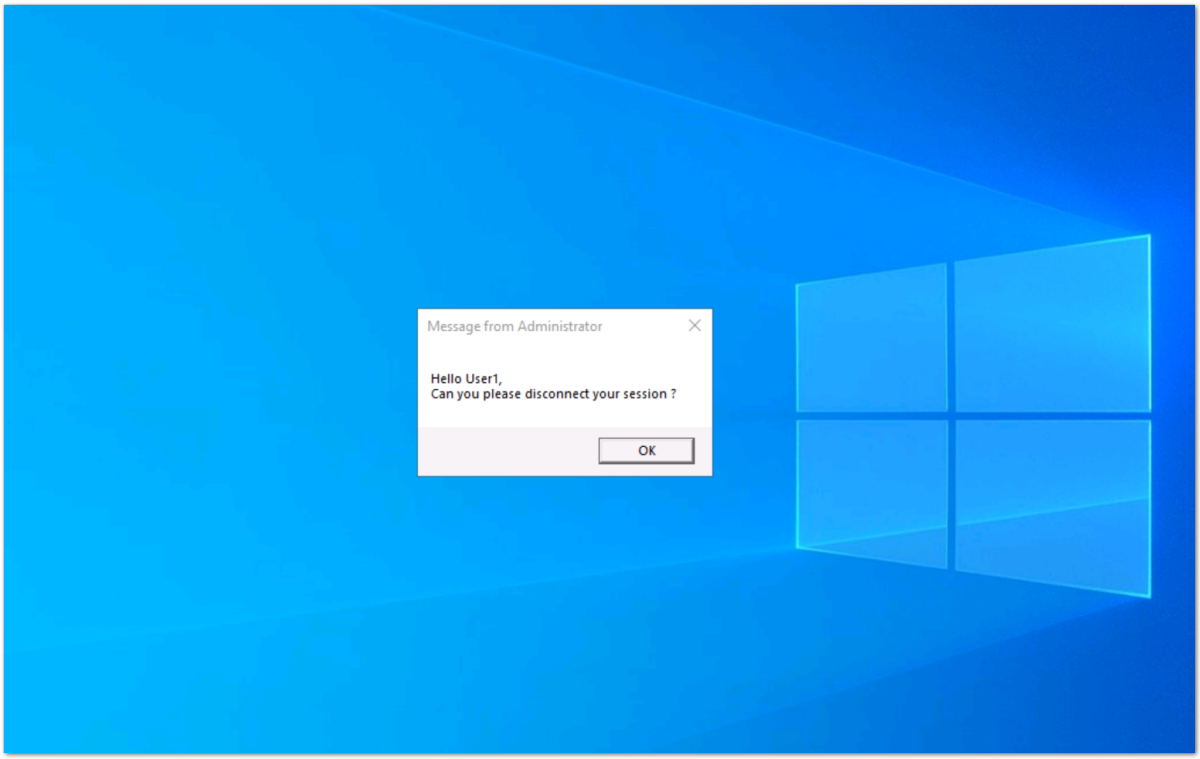
En el lado del cliente, este mensaje aparece para aceptar el control remoto:



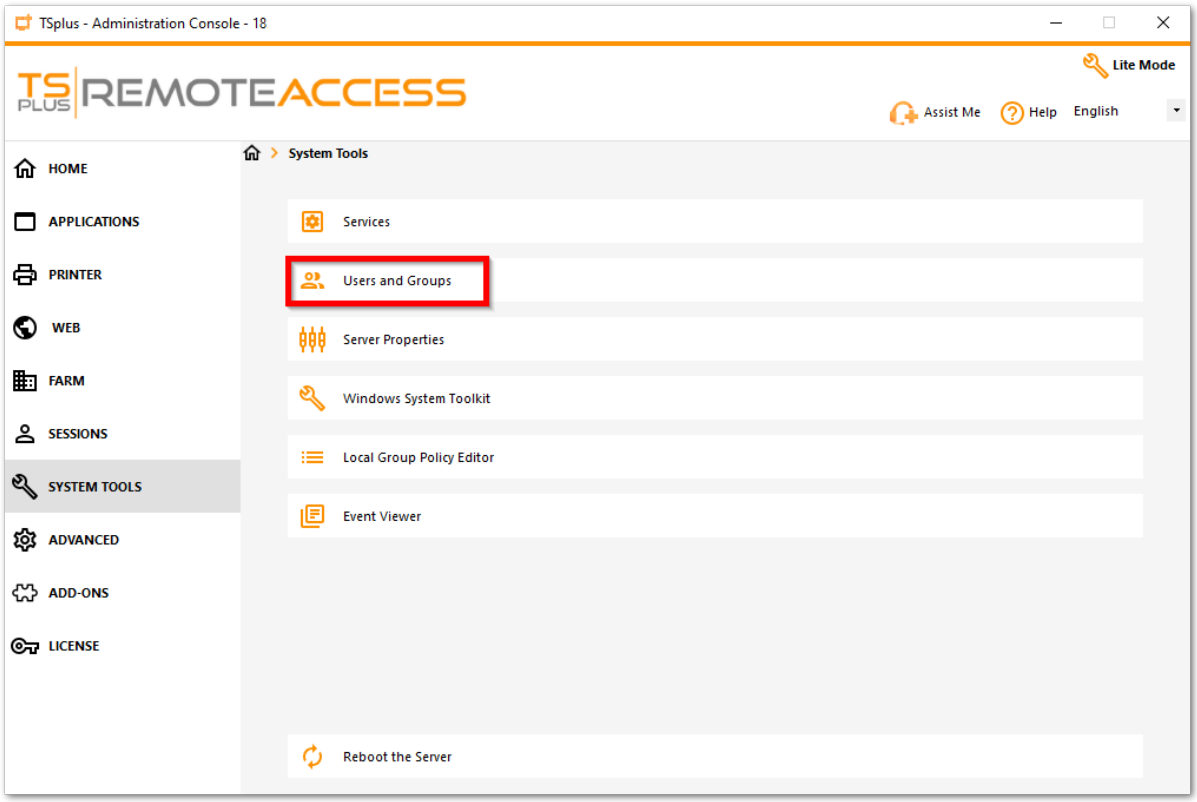
También puedes enviar un mensaje a tu usuario:



Mensaje enviado en el lado del servidor



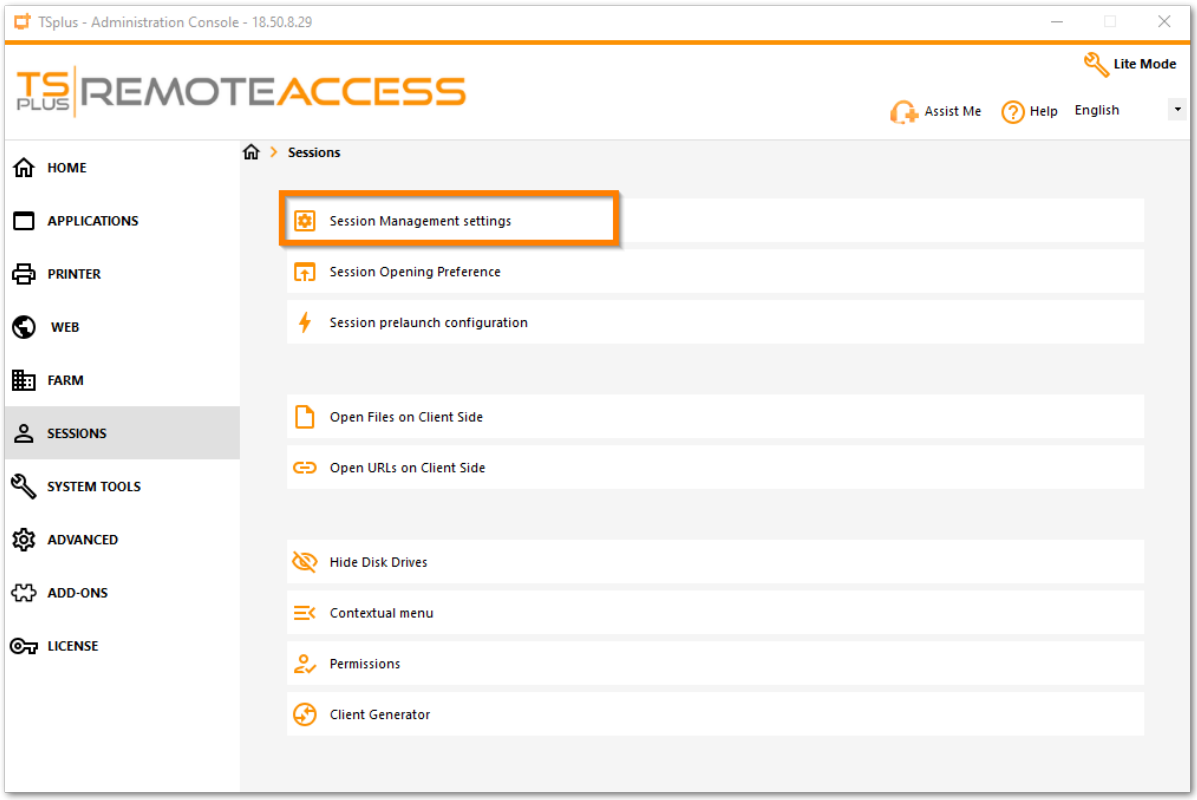
Mensaje que aparece en el lado del cliente

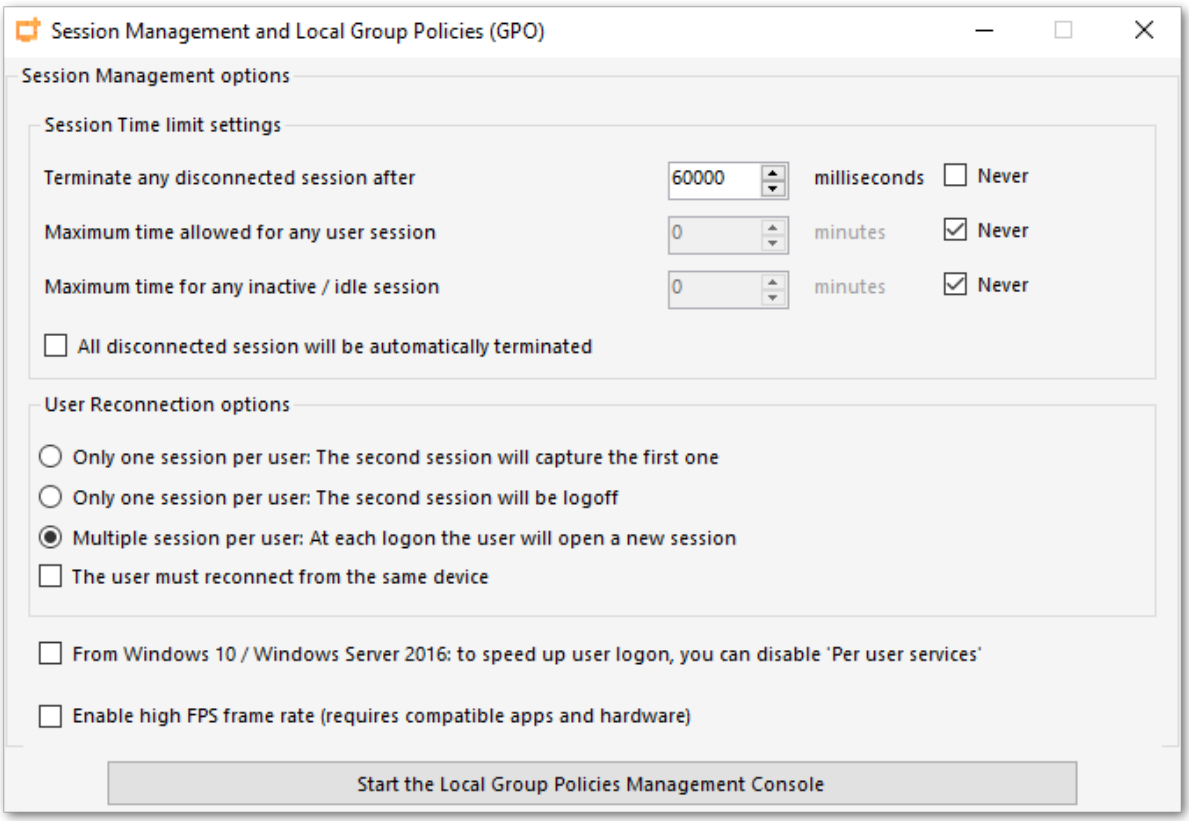


Ver esta documentación para más información.

- Con la pestaña de Configuración de Gestión de Sesiones (GPO), puede establecer varias

configuraciones de conexión para cada sesión y usuario:



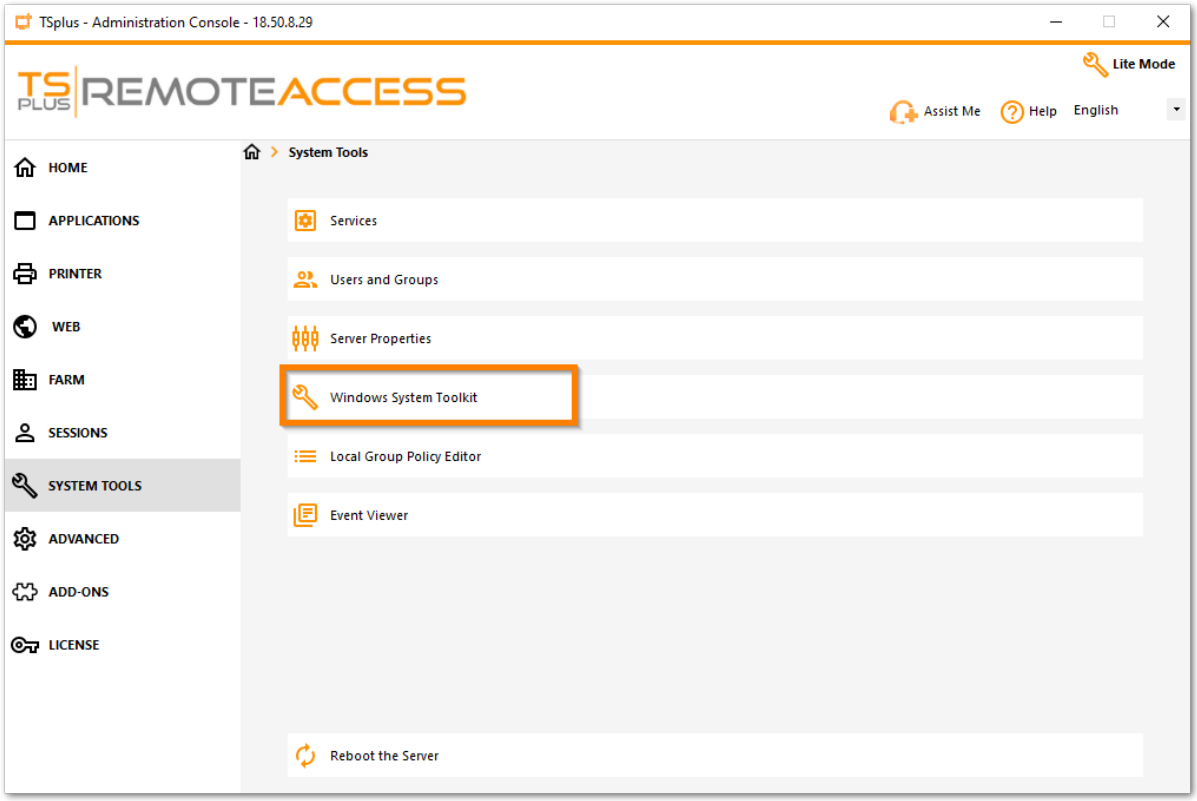


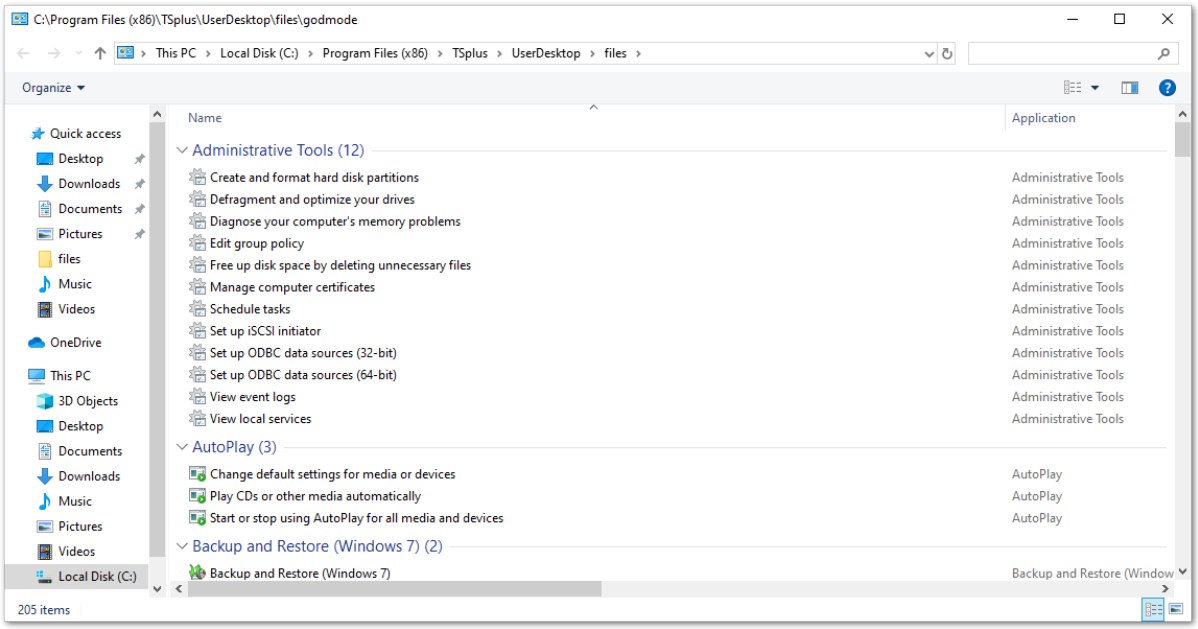
Windows Server 2016 introdujo un nuevo "Servicio por usuario", que hace que los servicios

inicien todos los procesos por usuarios, lo que ralentiza el tiempo de inicio de sesión de los usuarios.

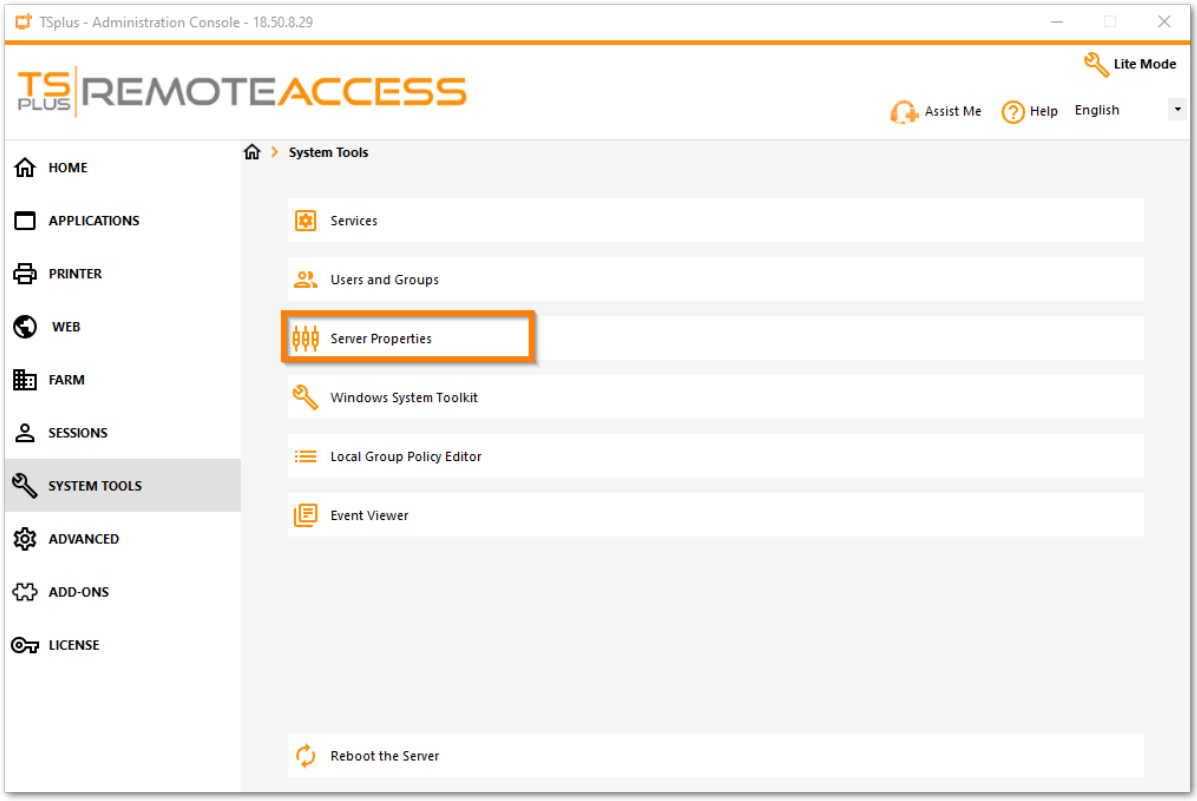
Desde el lanzamiento de TSplus 11.70, puedes **deshabilitar servicios por usuario para acelerar el inicio de sesión de los usuarios** .

- El Kit de Herramientas de Windows es un panel de control mejorado que resume todas las herramientas de administración de Windows.

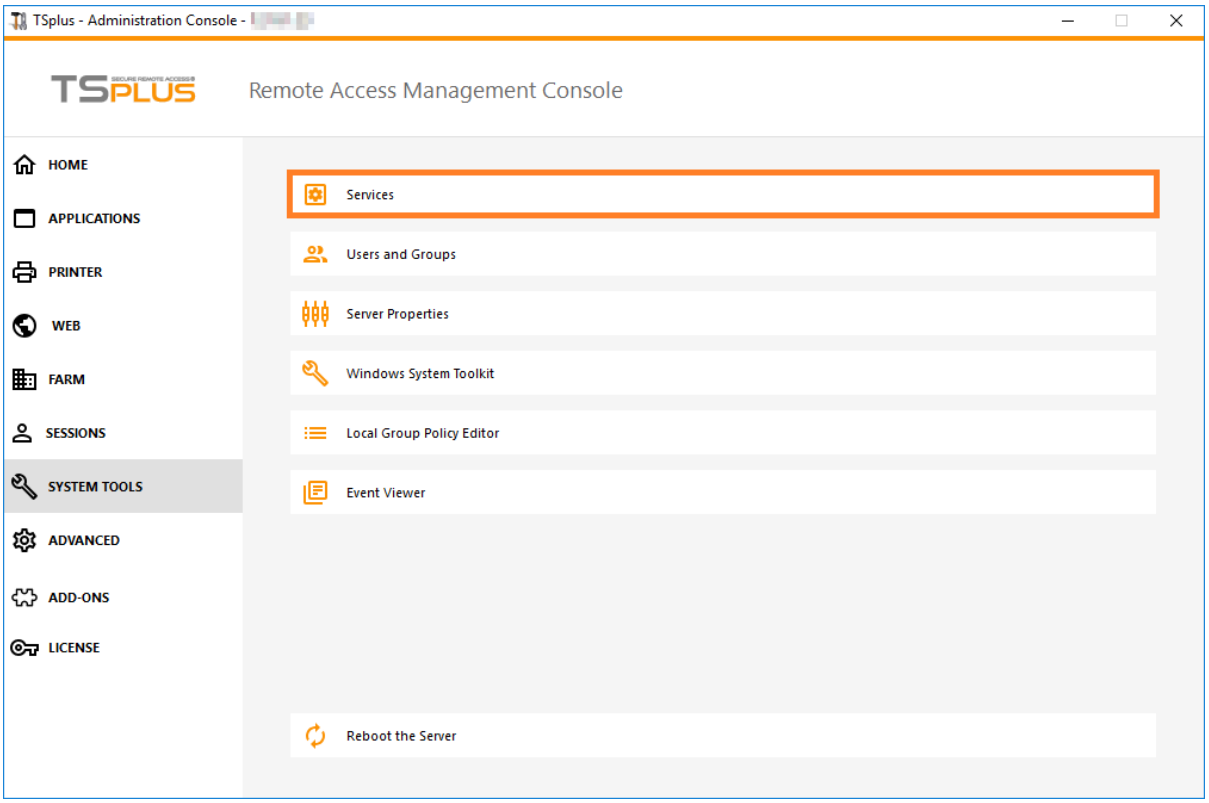




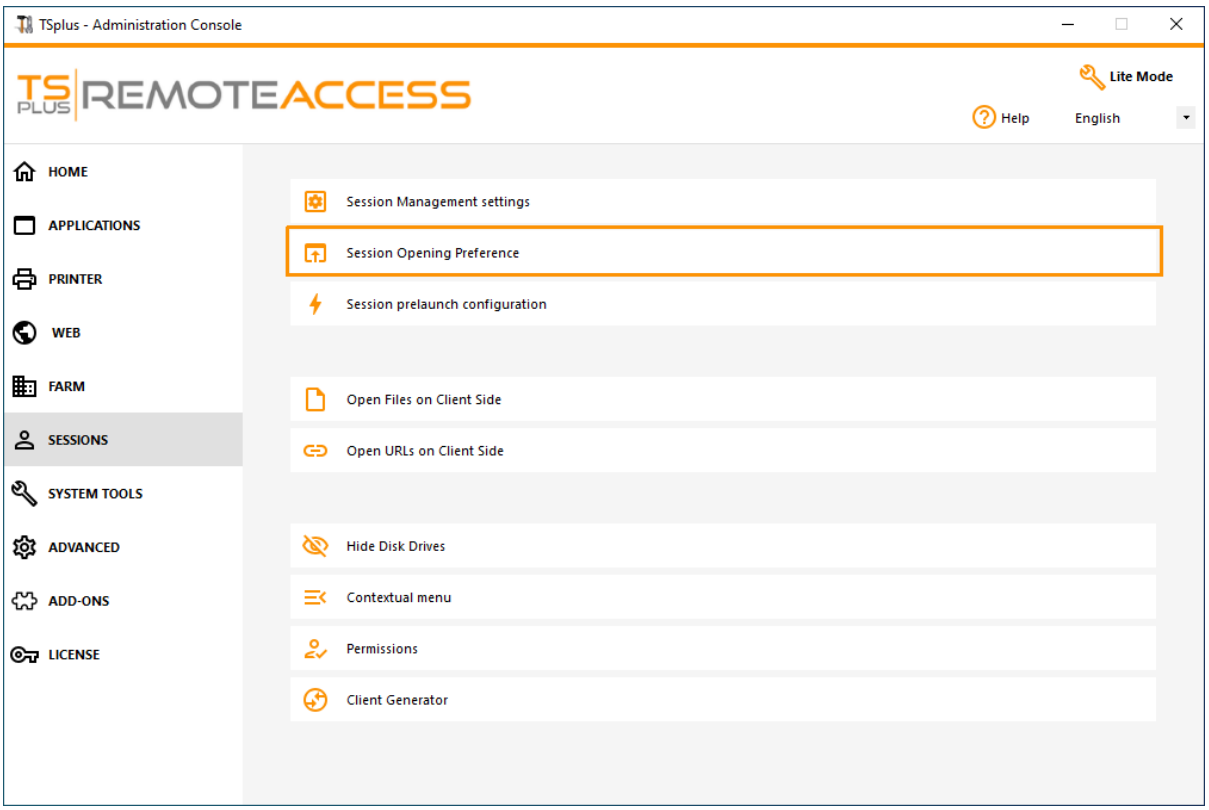
- También puede abrir la pestaña "Propiedades del servidor" para tener una visión general del panel de control.



- Puedes ver todos los servicios en tu servidor y su estado en el mosaico de Servicios.

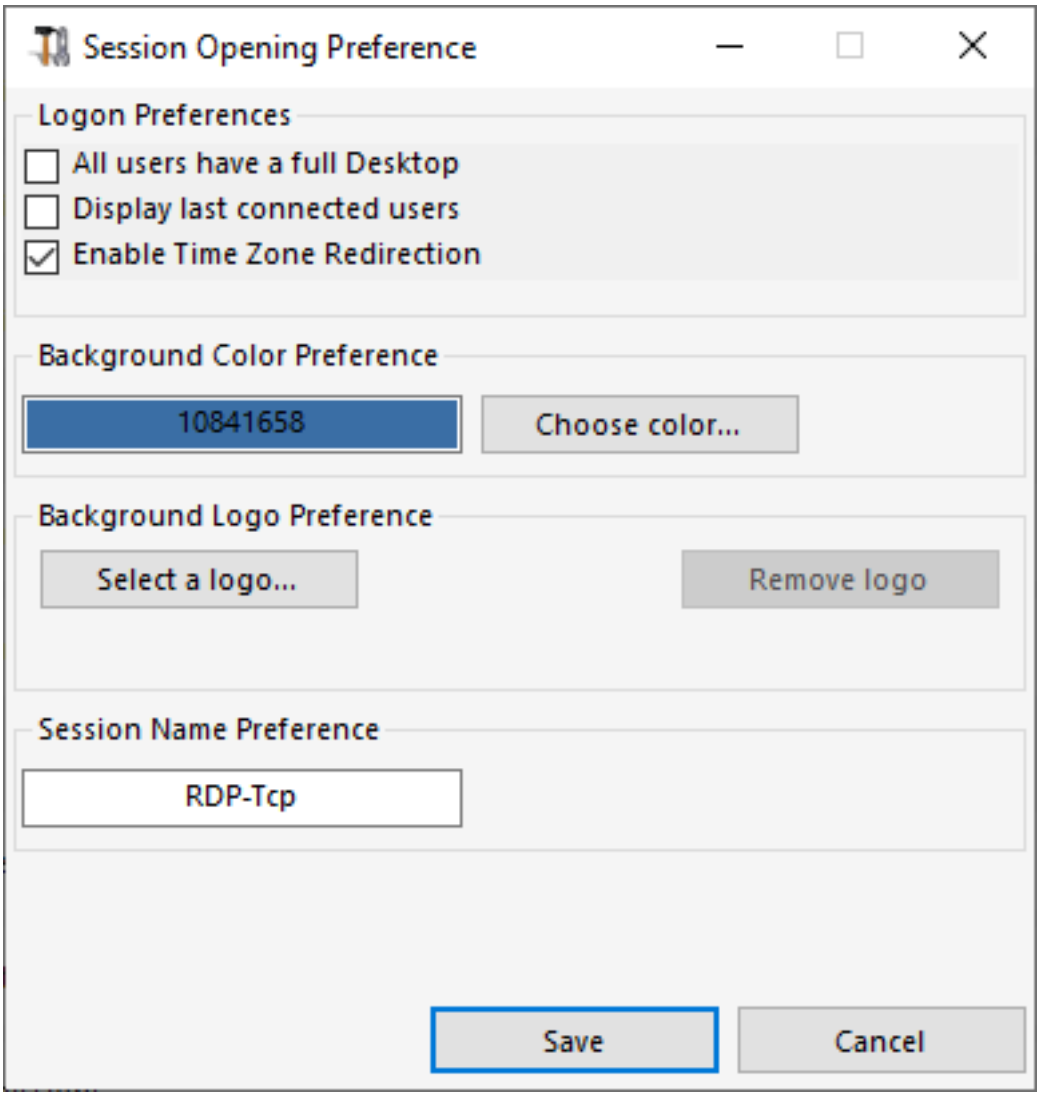


La preferencia de apertura de sesión te permite elegir tu preferencia de sesión de shell, tus preferencias de inicio de sesión, el color de fondo de tus sesiones, agregar tu propio logo y renombrarlo a tu gusto.



Por defecto, estas preferencias de inicio de sesión están habilitadas:

- El “ **Mostrar barra de progreso durante el inicio de sesión** ”.
- “ **Habilitar la redirección de zona horaria** que permite que la computadora cliente redirija su configuración de zona horaria a la sesión de Servicios de Escritorio Remoto. Si habilita esta configuración de política, los clientes que son capaces de redirección de zona horaria envían su información de zona horaria al servidor.



También puedes **configurar un escritorio completo** para todos sus usuarios y **obtener una pantalla de los últimos usuarios conectados** marcando las casillas correspondientes. Puedes **personaliza las sesiones de tus usuarios** agregando un nuevo color de fondo, otro logo o ninguno y utilizando el nombre de sesión de su elección.

- Desde el lanzamiento de TSplus 11.70, puedes usar **TSplus WinXshell** como una alternativa a la shell de Windows.

Tras la actualización de Windows del 10 de octubre, los administradores que permitieron a sus usuarios iniciar un Escritorio Remoto vieron el shell de Windows como un problema.

El problema principal reside en el problema de apertura de sesión/pantalla negra cuando se

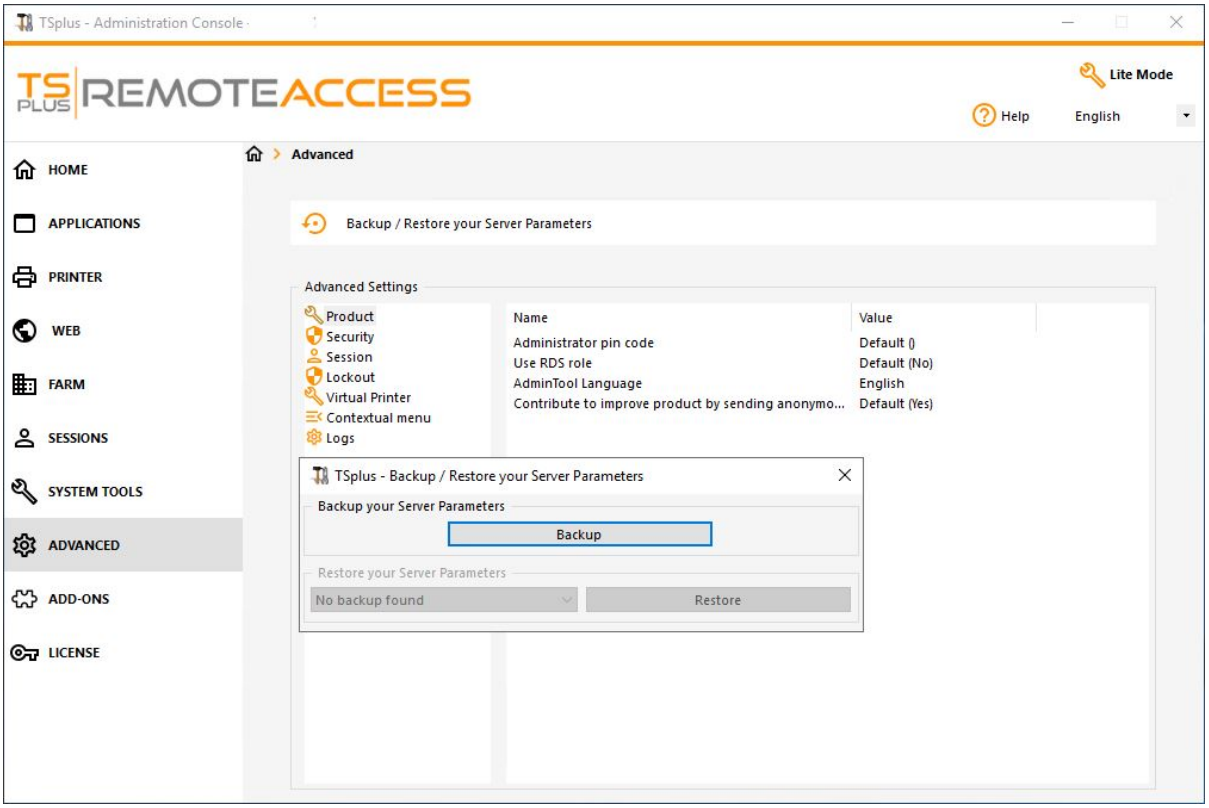
asigna un escritorio completo a múltiples usuarios en Windows 10 y Server 2016.

Proporciona características y una experiencia gráfica similar a la shell de Windows 2016, como la visualización del botón de inicio de 2016 y la barra de tareas.

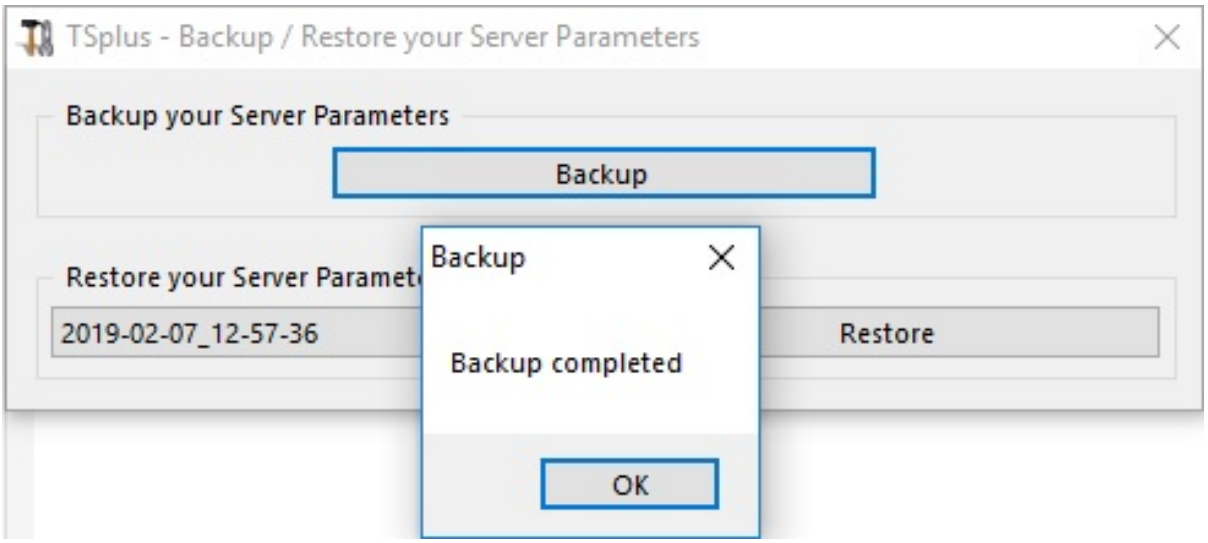
Es especialmente útil si usted **utilice sistemas operativos Windows 10 o Windows 16** , **gestionar 10 usuarios o más** y **desean asignarles un escritorio completo** .

Parámetros de copia de seguridad

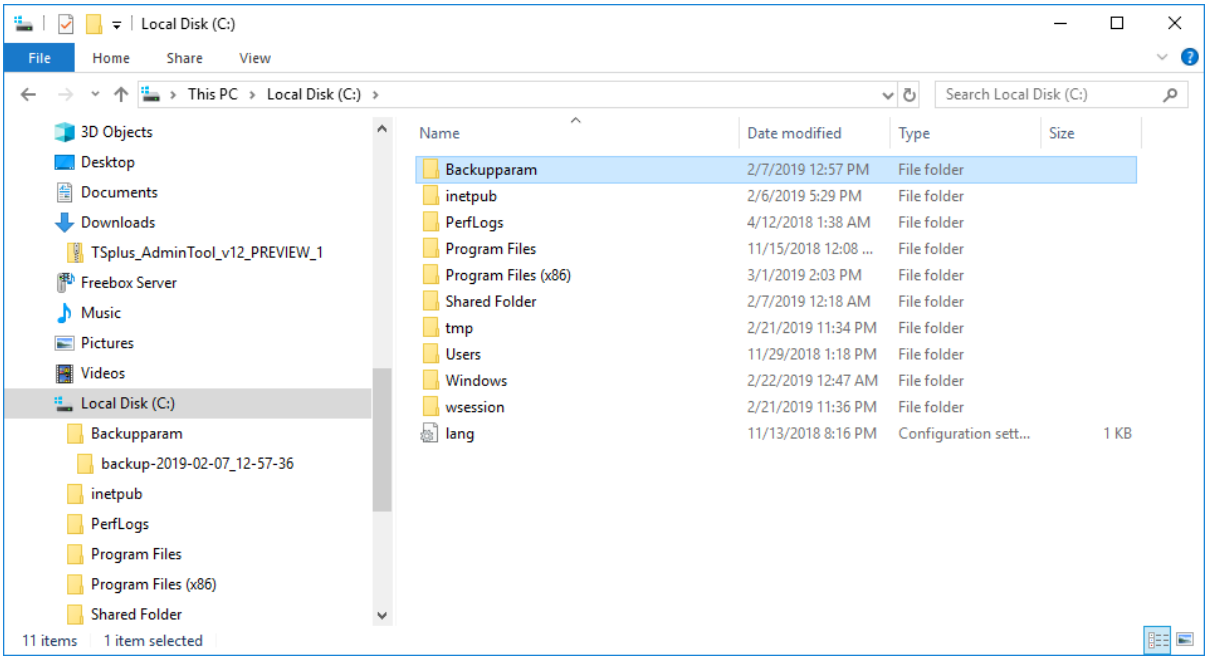
Puedes hacer una copia de seguridad o restaurar los parámetros de tu servidor haciendo clic en el mosaico del mismo nombre, en la pestaña Avanzado:



Haga clic en el botón de Copia de seguridad para hacer una copia de seguridad, que será fechada y añadida a la lista de sus puntos de restauración:



El archivo de respaldo se puede encontrar en la carpeta C:\Backupparam:



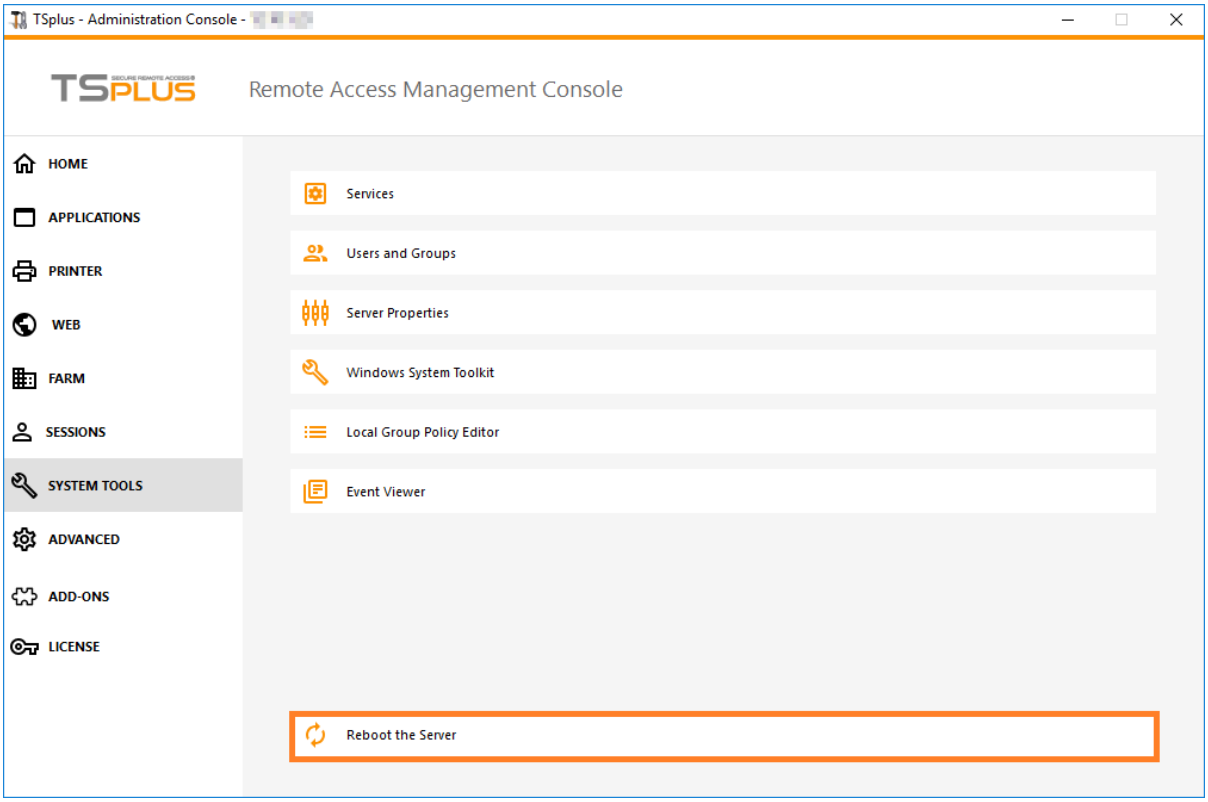
Copia la carpeta en el nuevo servidor después de instalar TSplus Remote Access y restaura la copia de seguridad.

Puedes comprobar con la prueba durante 15 días que el funcionamiento de las cuentas y el acceso es correcto antes de migrar tu licencia de forma definitiva.

Más información sobre esto documentación .

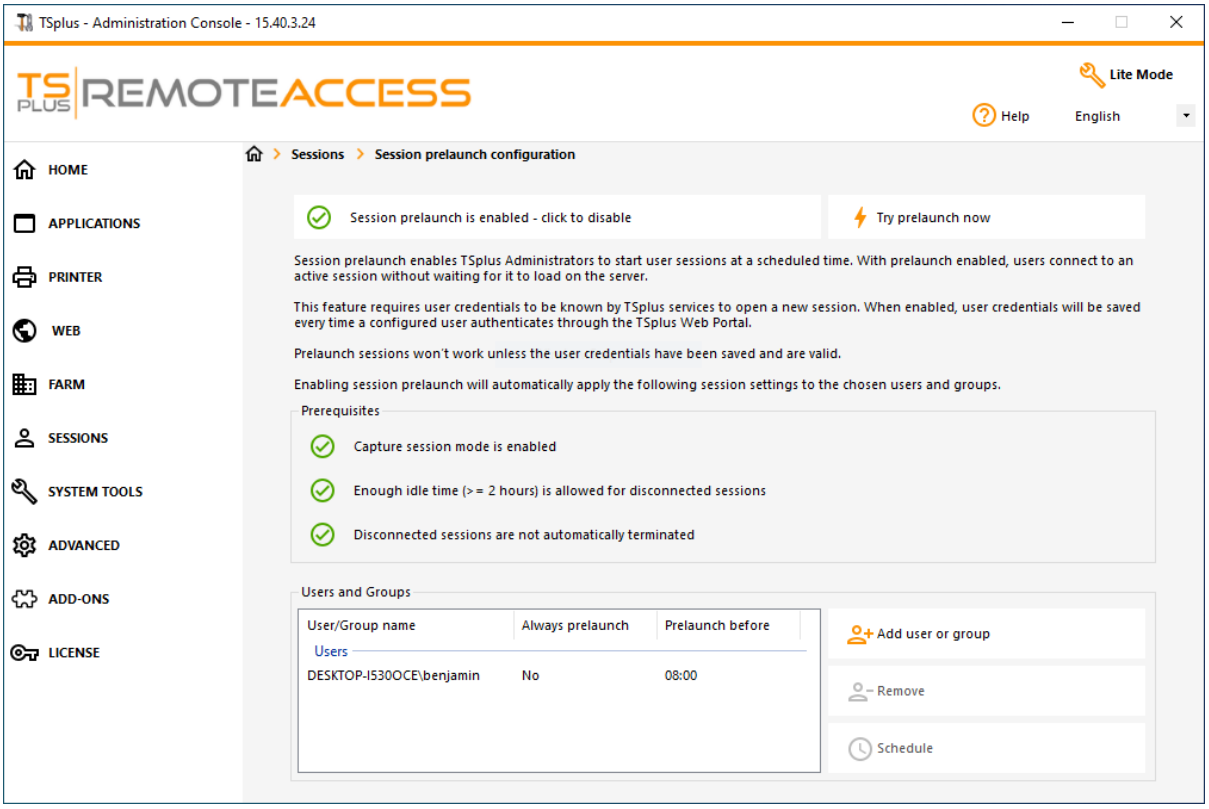
Reinicie su servidor

La pestaña "Reiniciar el servidor" te permite reiniciar tu servidor.


TSplus - Administration Console -
TSPLUS
Remote Access Management Console
HOME
APPLICATIONS
PRINTER
WEB
FARM
SESSIONS
SYSTEM TOOLS
ADVANCED
ADD-ONS
LICENSE
Services
Users and Groups
Server Properties
Windows System Toolkit
Local Group Policy Editor
Event Viewer
Reboot the Server

Prelanzamiento de sesión

Acceda al menú de configuración de Prelanzamiento de Sesión desde la pestaña Sesiones > Configuración de la herramienta de administración, haciendo clic en el mosaico “Configuración de Prelanzamiento de Sesión”.

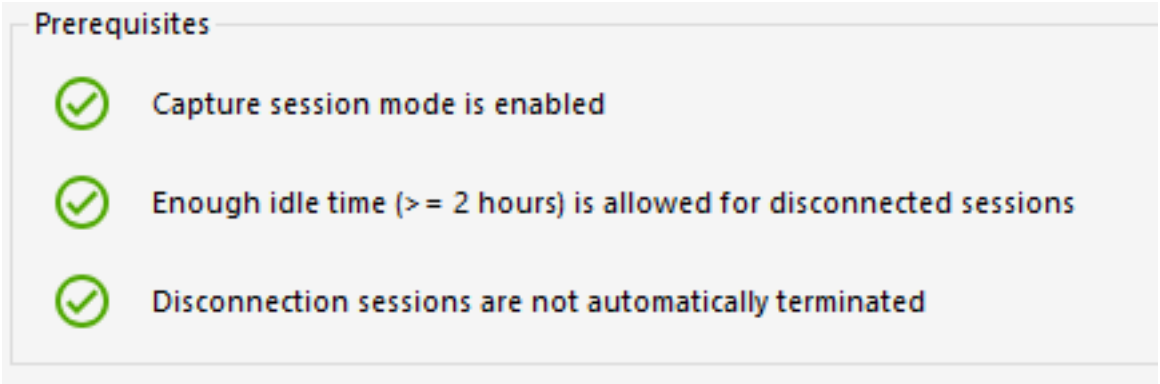


Resumen

La función de pre-lanzamiento de sesión permite a los administradores de TSplus Remote Access configurar las sesiones de usuario para que se inicien antes de un tiempo programado. La idea es preparar y cargar la sesión de cada usuario configurado con anticipación, de modo que, una vez que un usuario se conecte, capture su sesión específica. Esto puede reducir los tiempos de espera de conexión de minutos a segundos.

Requisitos

Prelaunch requiere que se cumplan múltiples requisitos previos.



1 - Para capturar una sesión, **el modo de captura de sesión debe estar habilitado.** Esto significa que no podrás beneficiarte de esta función si la configuración de múltiples sesiones es obligatoria para tus usuarios.

2 - Dado que la sesión preparada que se cargó con anticipación necesita estar presente (no desconectada) cuando el usuario se conecta y la captura, **se debe permitir un mínimo de 2 horas de tiempo de inactividad para la sesión desconectada.** Por supuesto, también puedes configurar la configuración de la sesión para que nunca cierre una sesión desconectada.

3 - Dado que la sesión preparada se desconecta una vez cargada para reducir el uso general de recursos, **las configuraciones de la sesión deben configurarse para no cerrar sesión automáticamente en las sesiones desconectadas.**

¡Nota importante! Cada usuario configurado necesitará autenticarse al menos una vez a través del Portal Web de TSplus después de que se habilite la función de pre-lanzamiento de sesión para que los servicios de TSplus puedan abrir la sesión del usuario configurado.

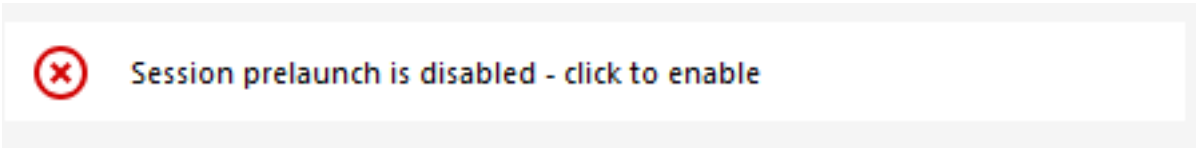
Compatibilidades de Prelanzamiento de Sesión

La preejecución de la sesión es compatible con sesiones HTML5 y sesiones RDP genéricas abiertas a través de un cliente generado o mstsc.

Sin embargo, no es compatible con la conexión de Remote App o conexiones RDP personalizadas realizadas para abrir un programa específico.
Como resultado, las conexiones que provienen del TSplus Web Application Portal no son compatibles.

Habilitar la función

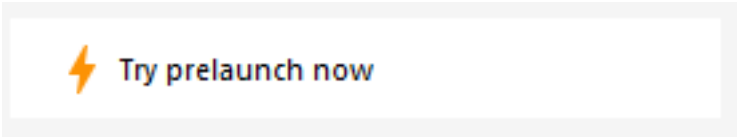
Para habilitar la función de preinicio de sesión, simplemente haga clic en el mosaico etiquetado como “El preinicio de sesión está deshabilitado - haga clic para habilitar” cerca de la parte superior de la ventana.



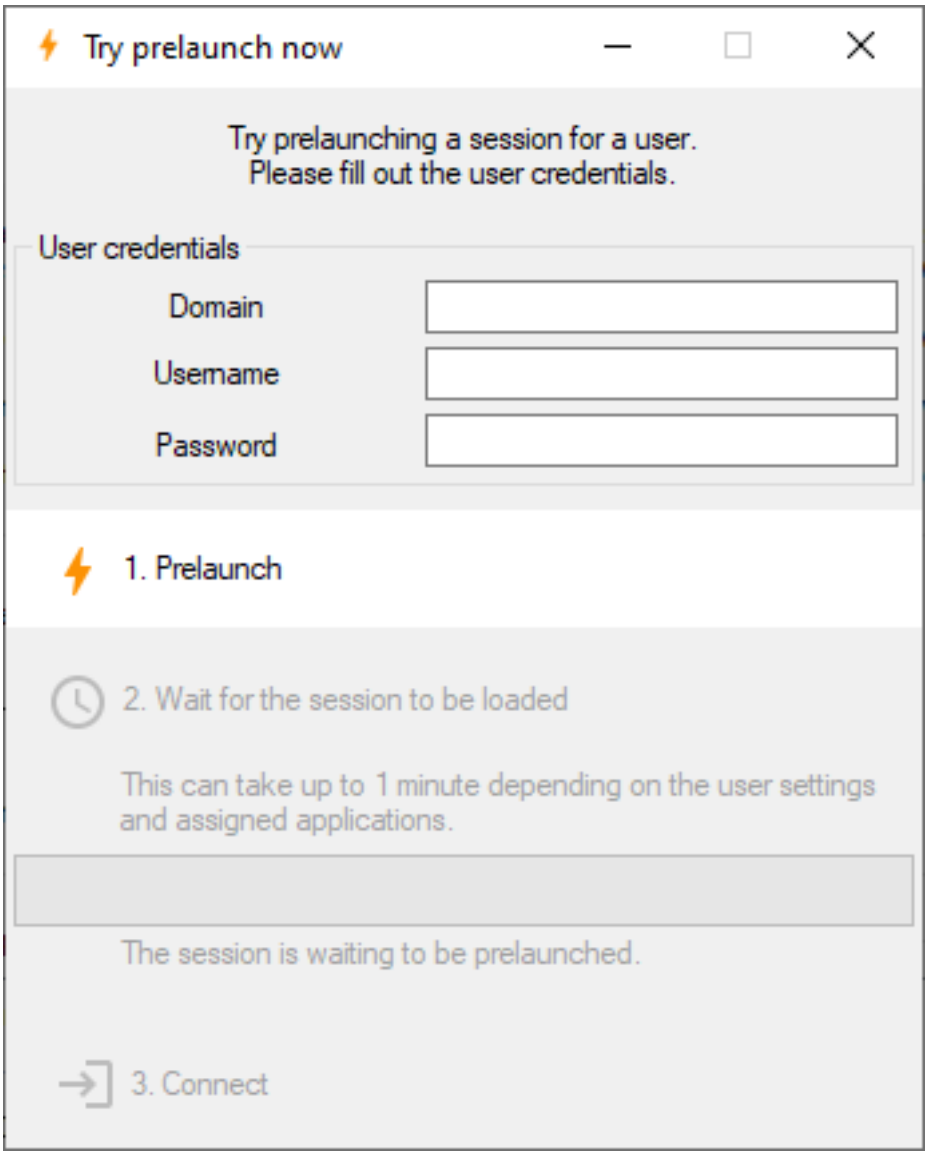
Si no se cumplen alguno de los requisitos previos al habilitar el Prelanzamiento de Sesión, se le preguntará si desea configurar automáticamente la configuración de la sesión para cumplir con los requisitos previos y utilizar la función. Tenga en cuenta que cambiar la configuración de la sesión puede requerir un reinicio.

Pruebe el prelanzamiento de la sesión

Una vez habilitado, podrá probar rápidamente la función haciendo clic en el botón “Probar pre-lanzamiento ahora” en la parte superior.



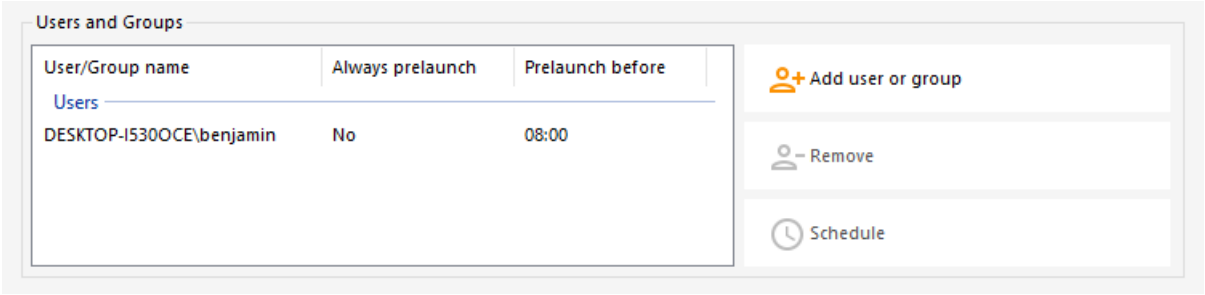
En la ventana que aparece, ingrese las credenciales del usuario para que los servicios de TSplus puedan preiniciar la sesión para este usuario específico.



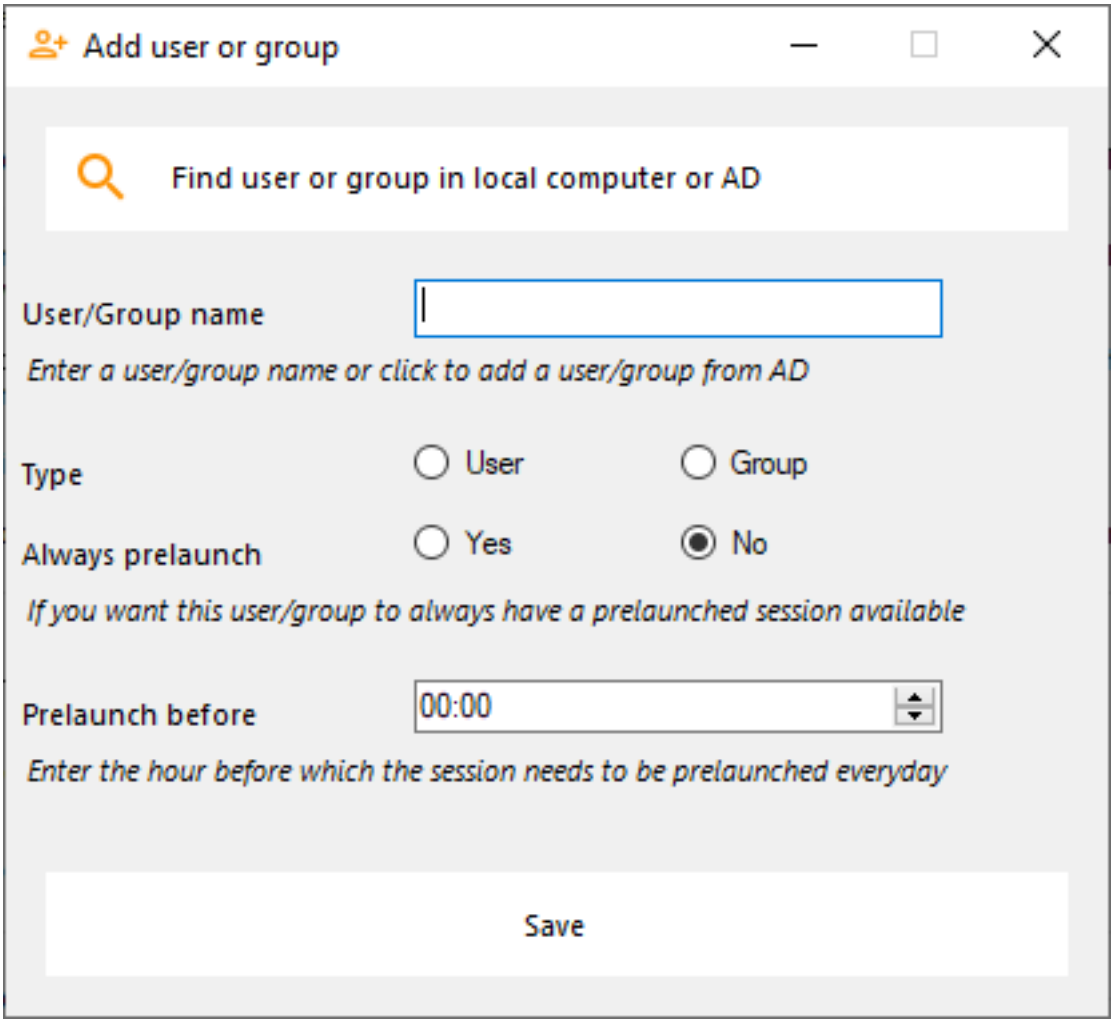
Haga clic en "Prelaunch" para iniciar y cargar una nueva sesión para este usuario.
Espera hasta que esté completamente cargado y luego haz clic en "Conectar" para capturar la sesión recién cargada.

Gestionar usuarios y grupos configurados

Para agregar usuarios y grupos de preinicio de sesión, simplemente haga clic en "Agregar usuario o grupo".
Para editar o remover un usuario configurado, seleccione el usuario/grupo correspondiente en la lista de usuarios/grupos configurados, luego haga clic en "Programar" para cambiar el tiempo de 'prelanzamiento antes', o en el botón "Eliminar" para quitar al usuario.



Después de hacer clic en "Agregar usuario o grupo", se le pedirá el nombre del usuario/grupo a configurar, así como el tiempo antes del cual la sesión debe ser cargada, llamado "prelanzamiento antes" aquí.
También puede configurar a este usuario/grupo para que siempre tenga una sesión preiniciada al conectarse en lugar de tener que programarla seleccionando "Sí" en la opción "Siempre preiniciar".



Cómo configurar el soporte de proxy inverso de Apache para Websockets

1. primero que todo cambia la siguiente variable a falso www\software\html5\settings.js > W.xhrreverse = false; (si no lo cambias a falso, siempre intentará xhr en lugar de websockets, lo que ya no queremos)

2. instalar Apache con soporte proxy_wstunnel (¡las versiones anteriores de Apache sin proxy_wstunnel no son compatibles!)

3. permitir en la configuración de Apache (httpd.conf, etc.) los siguientes módulos. LoadModule proxy_module modules/mod_proxy.so LoadModule proxy_http_module modules/mod_proxy_http.so LoadModule proxy_wstunnel_module modules/mod_proxy_wstunnel.so

4. supongamos que desea acceder al portal principal de html5 a través de la subcarpeta “/html5/” Como ejemplo http://your_ip_or_domain.net/html5/ Y Tsplus está instalado en la intranet en el servidor “intranetxyz” entonces agregue a la configuración (httpd.conf, etc.) lo siguiente

   ProxyPass /html5 http://intranetxyz:80 ProxyPassReverse /html5 http://intranetxyz:80

   ProxyPass “ws://intranetxyz:80/socket.io/websocket_https”

   ProxyPass “ws://intranetxyz:80/socket.io/websocket”

   ProxyPass “ws://intranetxyz:80/socket.io/flashsocket_https”

   ProxyPass “ws://intranetxyz:80/socket.io/flashsocket”

5. Reinicie Apache para que los cambios surtan efecto.

Autenticación de dos factores

La autenticación de dos factores añade una capa adicional de seguridad y **previene el acceso a la sesión de sus usuarios incluso si alguien conoce su contraseña** .

Se utiliza una combinación de dos factores diferentes para lograr un mayor nivel de seguridad:

1. algo que conocen, **una contraseña** .

2. algo que tienen, un **dispositivo - como un teléfono inteligente - con una aplicación de autenticación instalada.** .

Puedes usar una de las siguientes aplicaciones de autenticación para continuar. Estas aplicaciones están disponibles en una amplia gama de plataformas:

- Authy
- Google Authenticator
- Microsoft Authenticator

Cada vez que un usuario inicie sesión en su sesión remota, necesitará su contraseña y un código de verificación disponible en su teléfono móvil. Una vez configurada, la aplicación de autenticación mostrará un código de verificación para permitirle iniciar sesión en cualquier momento. Funciona incluso si su dispositivo está desconectado.

O bien puedes decidir recibir códigos de verificación por **SMS** En este caso, tendrás que crear una cuenta gratuita en Twilio .

El **Los códigos 2FA generados son TOTP** (código de acceso de un solo uso basado en el tiempo), y por lo tanto son de un solo uso.

Por lo tanto, no es posible reutilizar un código de 2FA que ya ha sido utilizado. Esto previene el robo y luego el uso de un código de 2FA al observar al usuario mientras ingresa su código.

Requisitos

La autenticación de dos factores requiere TSplus Remote Access **Web Móvil** o **Empresa** Ediciones.

La autenticación de dos factores es compatible con:

- TSplus Remote Access **Portal web** , para conexiones tanto de HTML5 como de Remoteapp
- TSplus Connection Client, para clientes generados desde la versión 15.30.3.15, con soporte de 2FA habilitado explícitamente. Ver Soporte del Generador de Clientes Portátiles para la Autenticación de Dos Factores
- 2FA está relacionado con usuarios de Windows y no con credenciales web.

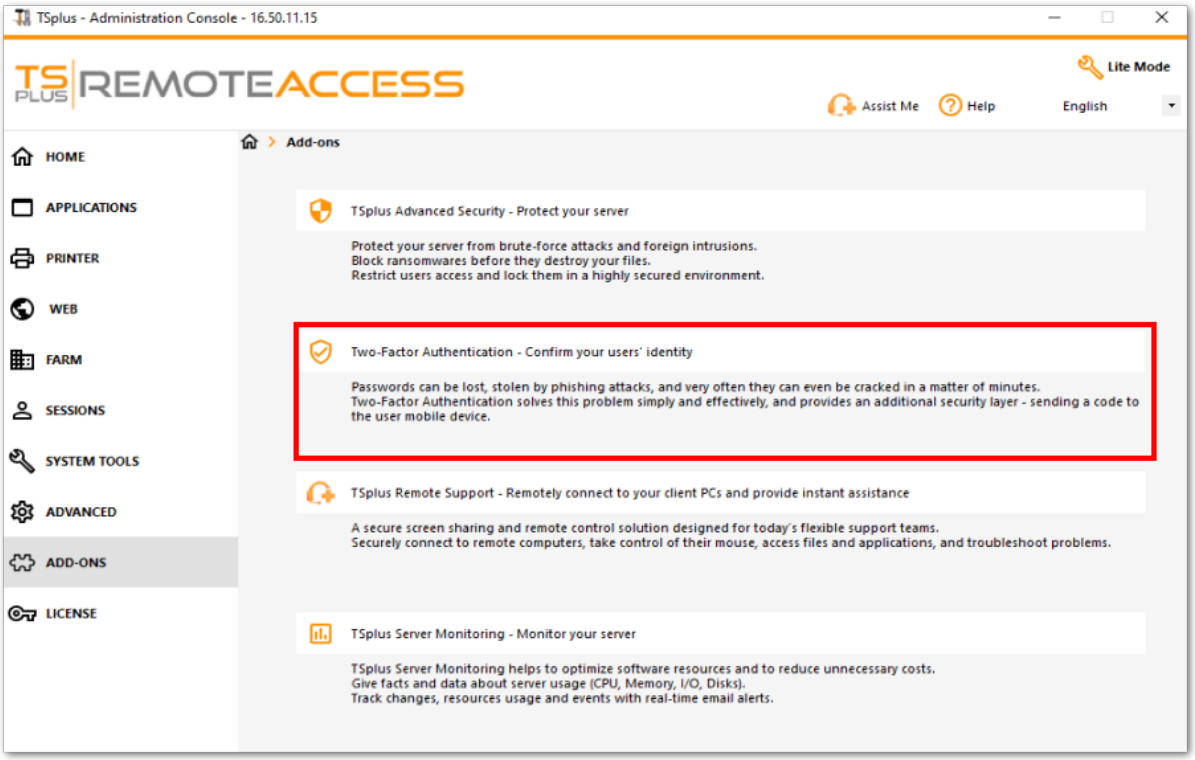
Este modo de autenticación no admite el inicio de sesión a través del cliente estándar de Microsoft Remote Desktop (mstsc.exe).

Para proporcionar una solución aún más segura, se deniegan las conexiones RDP para los usuarios con 2FA habilitado.

Como requisito previo, el servidor TSplus y los dispositivos deben estar a tiempo. Vea el Sincronización de tiempo y Configuraciones secciones para más información de configuración.

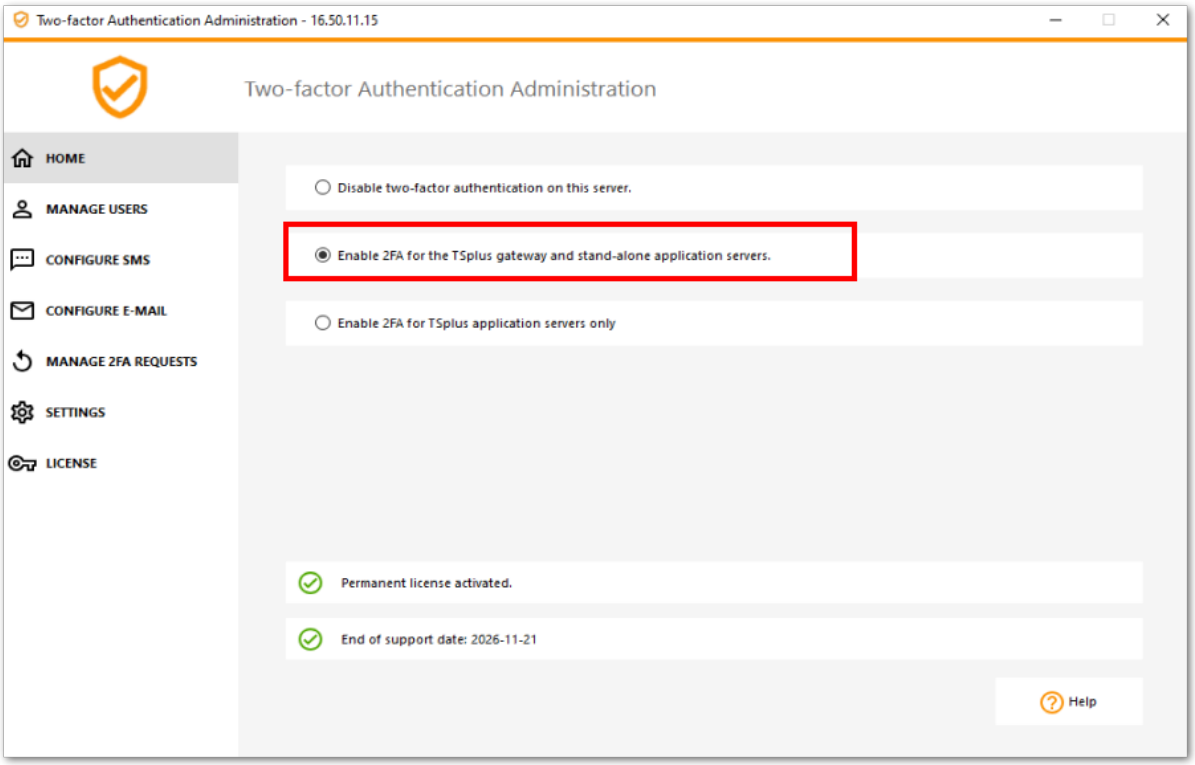
Activando la licencia del complemento de Autenticación de Dos Factores

La función de Autenticación de Dos Factores se puede encontrar en la pestaña de Complemento de AdminTool:



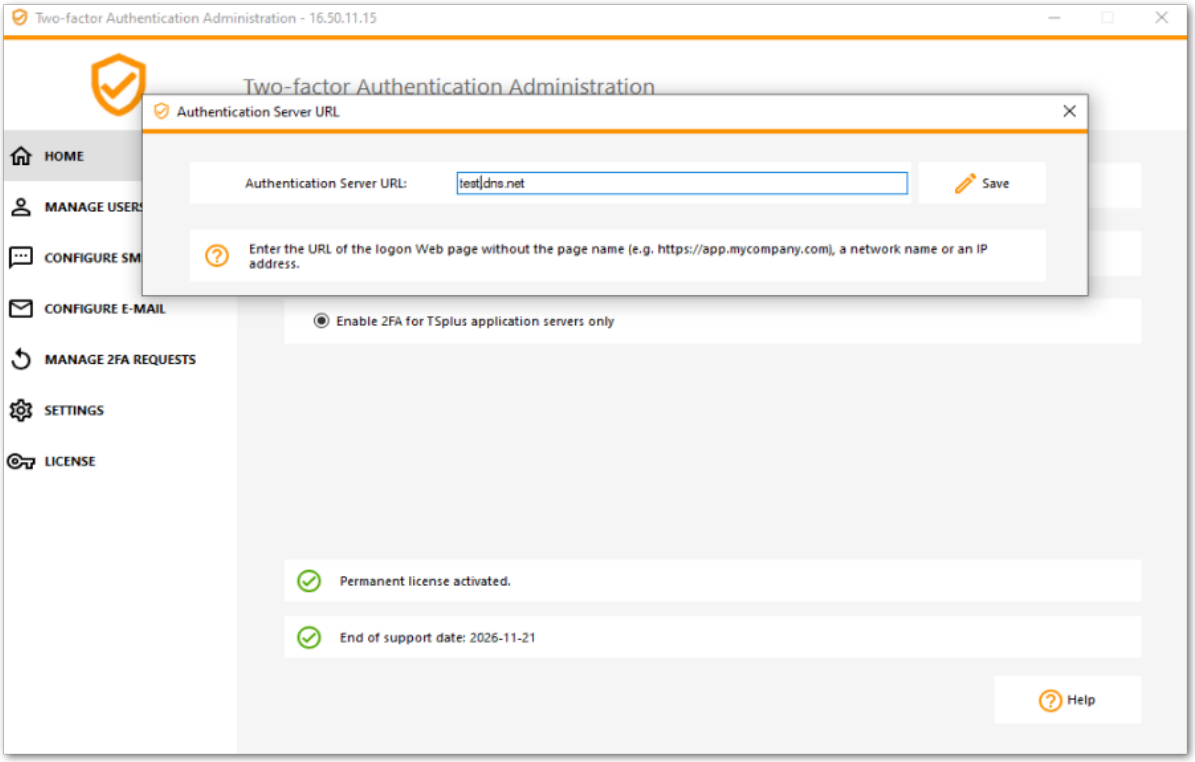
Realice los siguientes pasos para habilitar la autenticación de dos factores para su servidor o implementación de TSplus. Si su implementación de TSplus está configurada para usar múltiples servidores, realice esta tarea en el servidor de TSplus expuesto como el único punto de entrada para los usuarios o que tenga el rol de proxy inverso.

1. Abra la aplicación de administración de la autenticación de dos factores. Se muestran el estado de la autenticación de dos factores y el estado de la licencia:

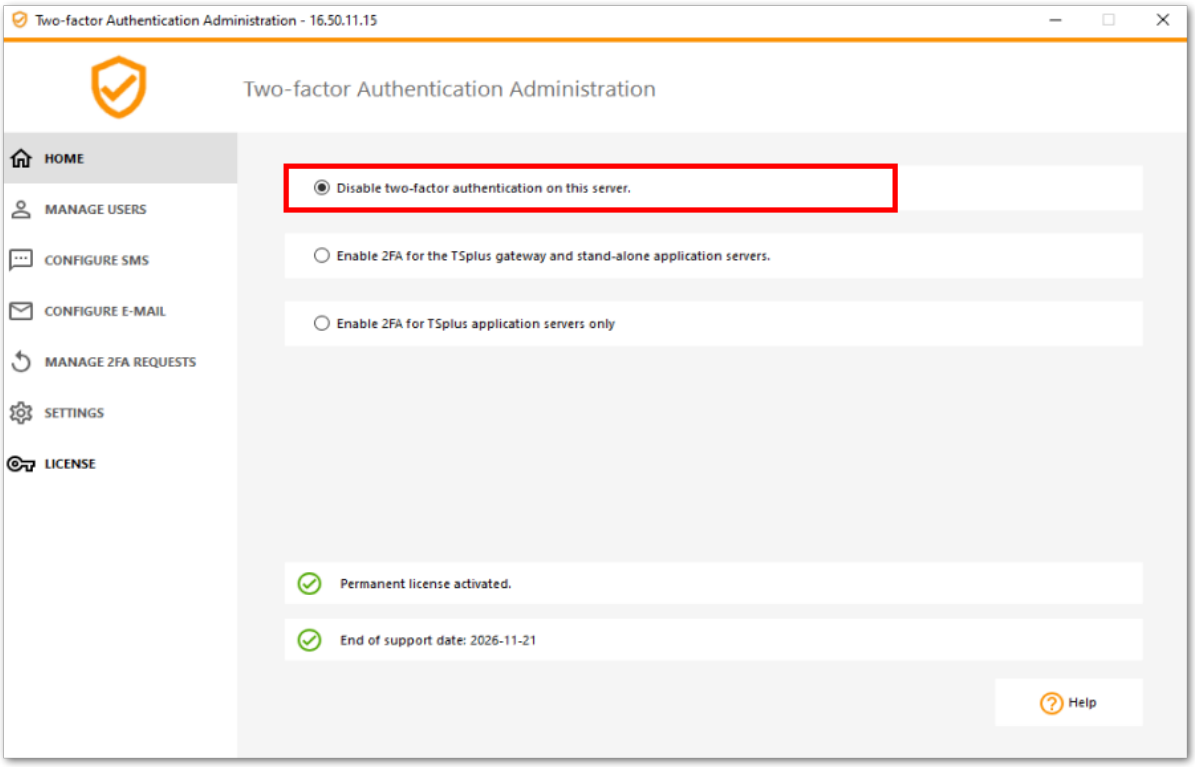


Por defecto, 2FA está habilitado para el portal TSplus y los servidores de aplicaciones independientes.

Puedes habilitarlo solo para los servidores de aplicaciones de TSplus, ingresando la URL del servidor de autenticación:



O desactívelo:

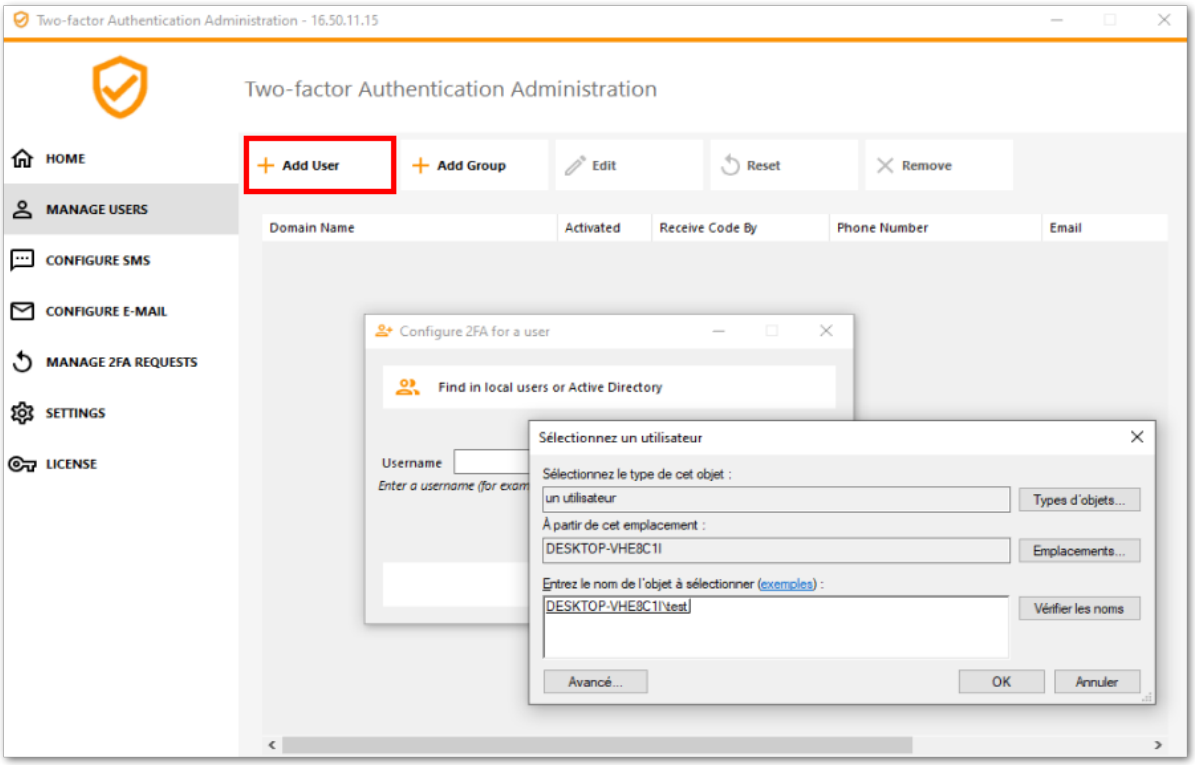


Agregar usuarios y grupos

Una vez que se habilita la autenticación de dos factores, puede configurar a los usuarios para la autenticación de dos factores.

1. Desde la aplicación de administración de la autenticación de dos factores, haga clic en el Administrar usuarios tab.

2. Luego, haga clic en Agregar para seleccionar usuarios y/o grupos de usuarios. El Seleccionar usuarios o grupos se abre la caja.



3. Agrega tantos usuarios y grupos como sea necesario y luego haz clic OK Los usuarios y grupos se añaden a la lista y se habilitan para la autenticación de dos factores.

Aquí están los comandos para agregar usuarios/grupos
3 tipos de argumentos posibles:

solo el nombre de dominio
TwoFactor.Admin.exe /addusers nombreDominio1

- agrega al usuario con los valores predeterminados (método de recepción = app, campos de correo electrónico y teléfono no ingresados)

el nombre de dominio y el método de recepción
TwoFactor.Admin.exe /addusers domainName1;SMS

- agrega al usuario con el método de recepción deseado, pero no intenta activarlo

el nombre de dominio, el método de recepción, el campo Teléfono (incluso si está vacío), el campo Correo electrónico (incluso si está vacío)
*TwoFactor.Admin.exe /addusers domainName1;SMS;+33606060606; username1@truc.net nombreDeDominio2;CorreoElectrónico;; username2@truc.net domainName3;SMS; +33606060607;domainName4

- El mismo comportamiento que en el HMI, cuando añadimos un usuario, luego lo editamos con la información correcta: intentamos activar al usuario.

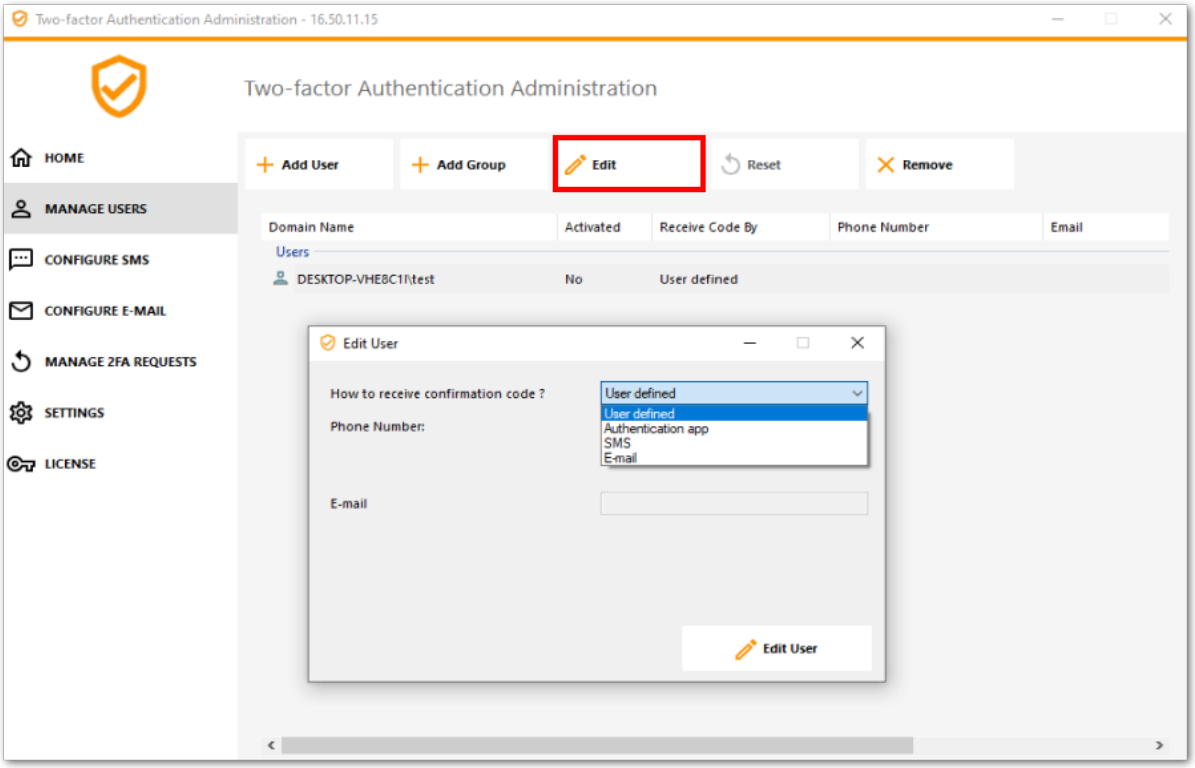
Como se muestra en el último ejemplo, se pueden indicar varios usuarios (separados por un

espacio). Los diferentes campos de un usuario están separados por un punto y coma.

Para grupos individuales:
TwoFactor.Admin.exe /addgroups grupo1 grupo2 grupo3

Editar usuarios

En el mismo mosaico, puedes editar la forma en que los usuarios reciben los códigos de verificación seleccionando un usuario y haciendo clic en el botón "Editar":

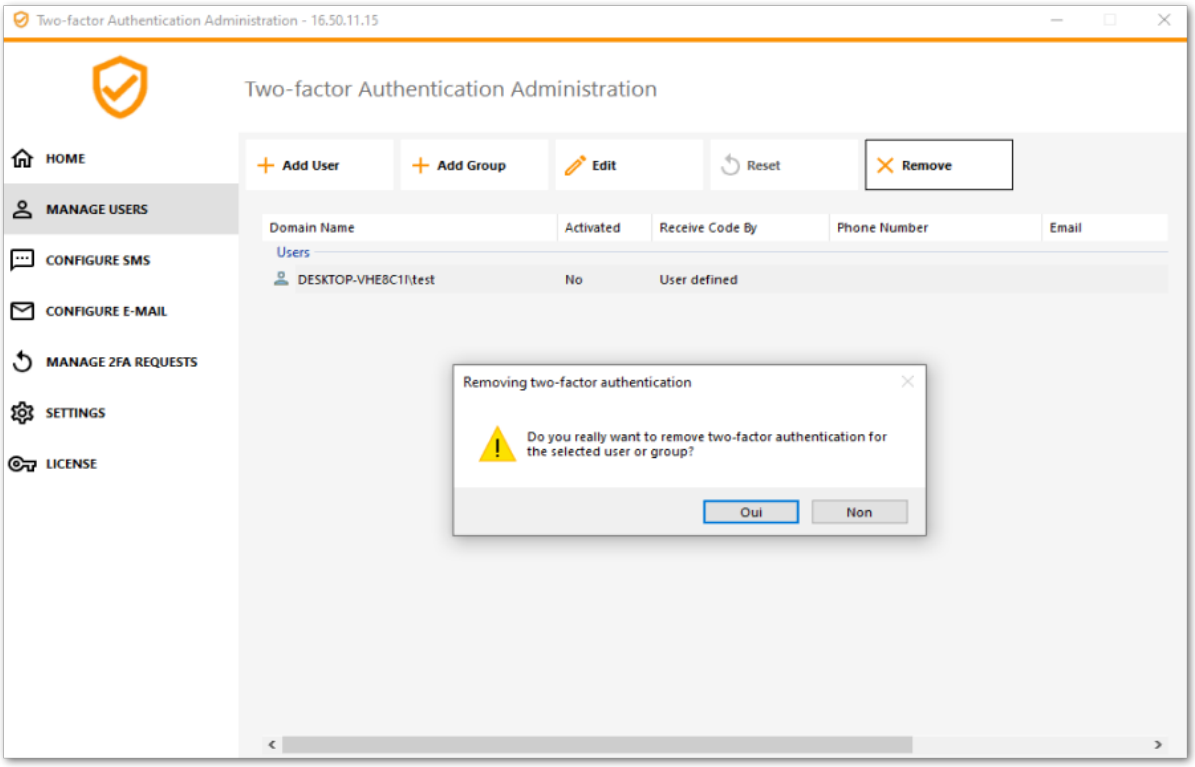


El usuario recibe códigos de verificación en la aplicación de autenticación por defecto. Puede elegir que los reciba por SMS o CORREO ELECTRÓNICO seleccionando la opción.

Seleccionó SMS y agregó el número de teléfono del usuario en el campo o seleccionó EMAIL y agregó el correo electrónico del usuario.

Eliminar usuarios y grupos

Para eliminar usuarios o grupos, seleccione el usuario o el grupo y luego haga clic en Eliminar
Se muestra un mensaje de confirmación.



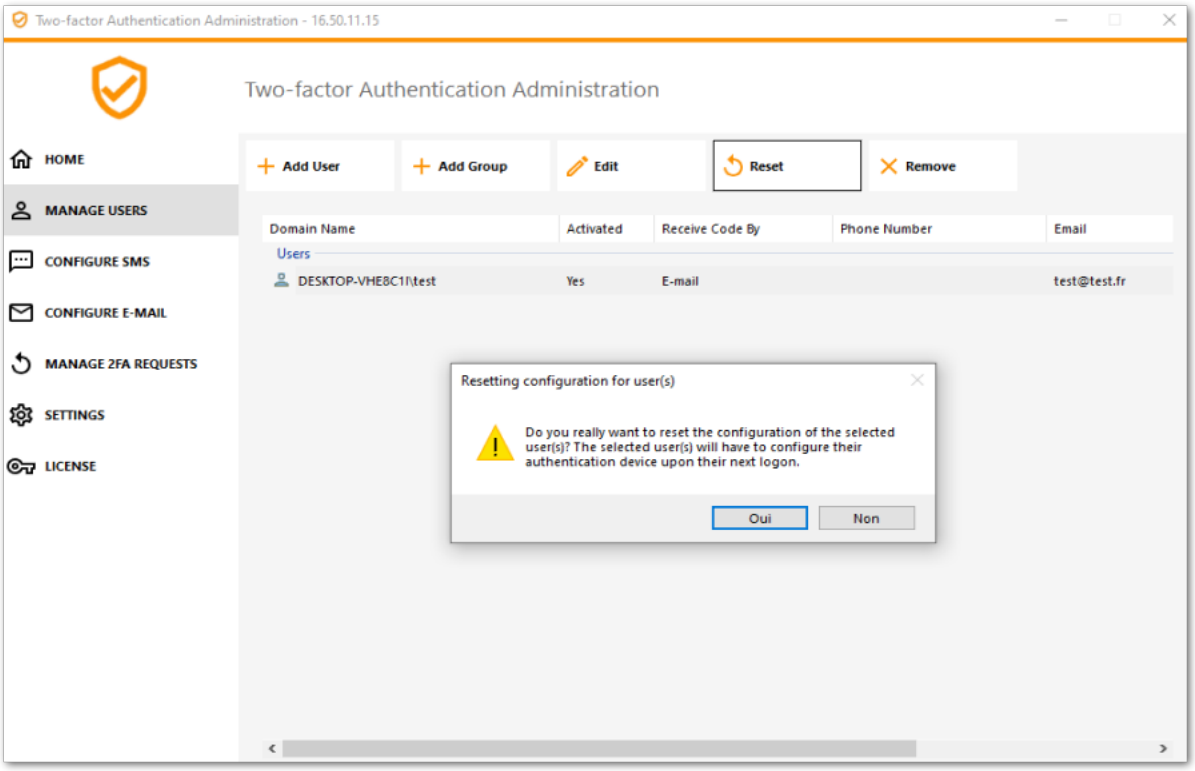
Haga clic Sí El usuario o el grupo se elimina de su lista y ya no podrá conectarse utilizando la autenticación de dos factores.

Restablecer configuración para usuarios

En caso de pérdida del dispositivo de autenticación de un usuario, o si el usuario necesita mostrar nuevamente el código QR secreto, debe restablecer la configuración de autenticación del usuario.

1. Desde la aplicación de administración de la autenticación de dos factores, haga clic en el Administrar usuarios tab.

2. Seleccione uno o varios usuarios activados y luego haga clic en Restablecer Se muestra un mensaje de confirmación.



3. Haga clic Sí Los usuarios seleccionados recibirán un nuevo código QR en el próximo inicio de sesión y deberán escanearlo en la aplicación de autenticación de su dispositivo.

También puedes modificar el número de teléfono del usuario, para que pueda recibir un código de verificación en su nuevo dispositivo.

Inscribir usuario para la autenticación de dos factores

Una vez que un usuario ha sido habilitado para usar la autenticación de dos factores, se mostrará un mensaje de activación en su próximo inicio de sesión exitoso desde el portal web de TSplus.



Para completar los pasos requeridos, tienes dos opciones: generar códigos a través de una aplicación de autenticación o hacer que el usuario reciba códigos por SMS.

Recibir códigos con una aplicación de autenticación

El usuario debe instalar una aplicación de autenticación en un dispositivo portátil, como su teléfono inteligente.

Puedes usar una de las siguientes aplicaciones de autenticación para continuar. Estas aplicaciones están disponibles en una amplia gama de plataformas:

- Authy
- Google Authenticator

- Microsoft Authenticator

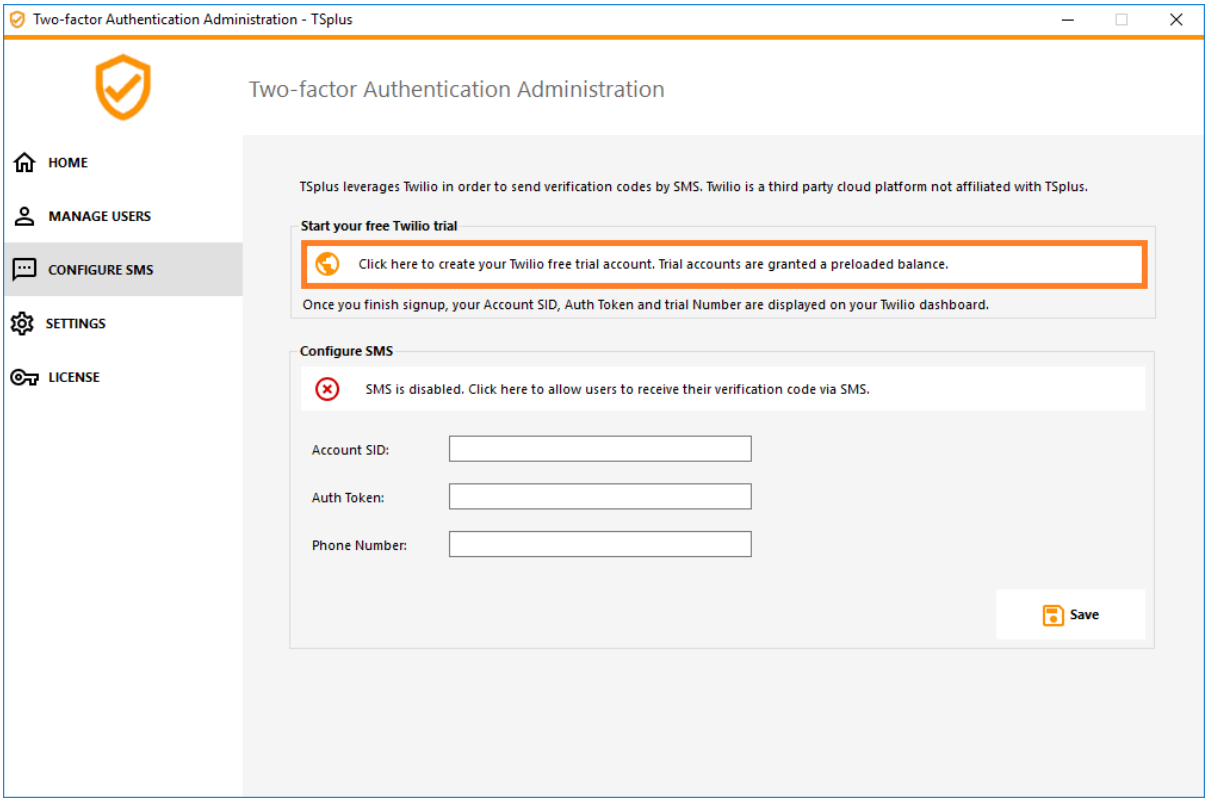
Por favor, utiliza la documentación de cada aplicación para más detalles sobre cómo proceder para agregar tu cuenta de TSplus.

Configurar SMS

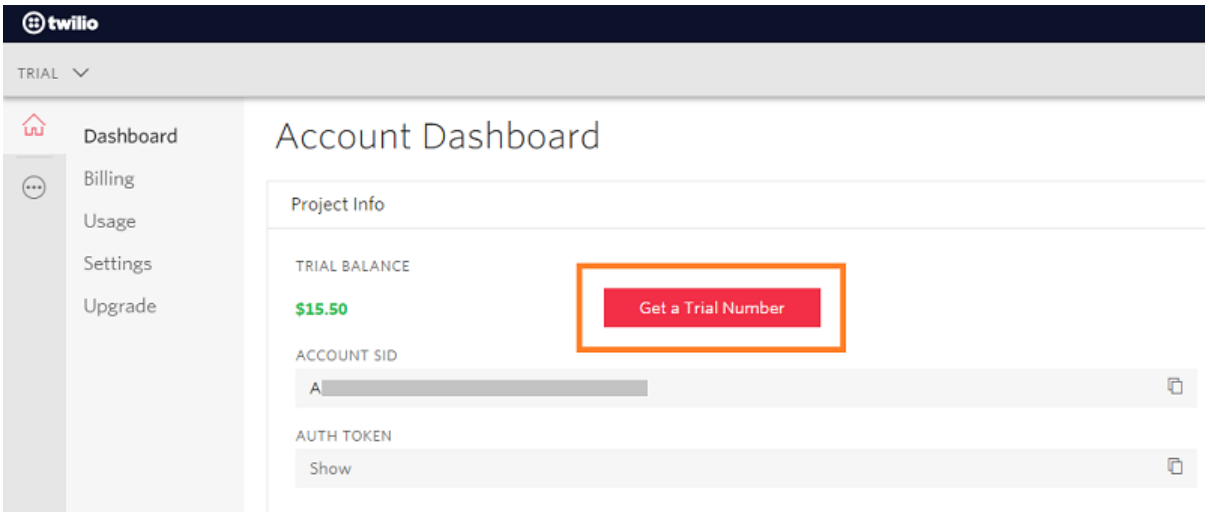
Para que el usuario reciba códigos de verificación por SMS, primero debe habilitarlo. Haga clic en el Configurar SMS tab:

TSplus aprovecha Twilio para enviar códigos de verificación por SMS. Twilio es una plataforma en la nube de terceros, no afiliada a TSplus.

1. Solo crea una cuenta gratuita en Twilio al hacer clic en el botón a continuación “Comience su prueba gratuita con Twilio”:

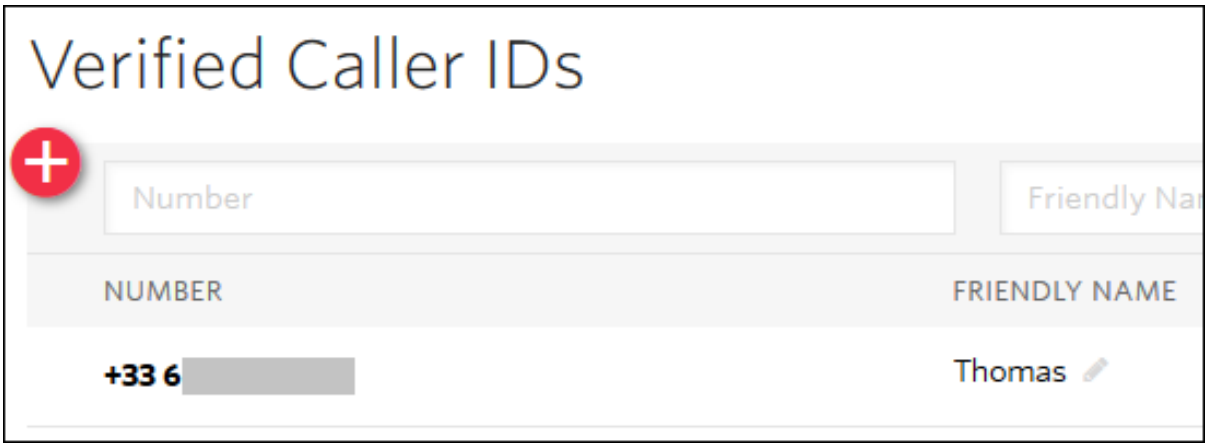


2. En tu Tablero de cuenta de Twilio deberá activar su número de prueba:

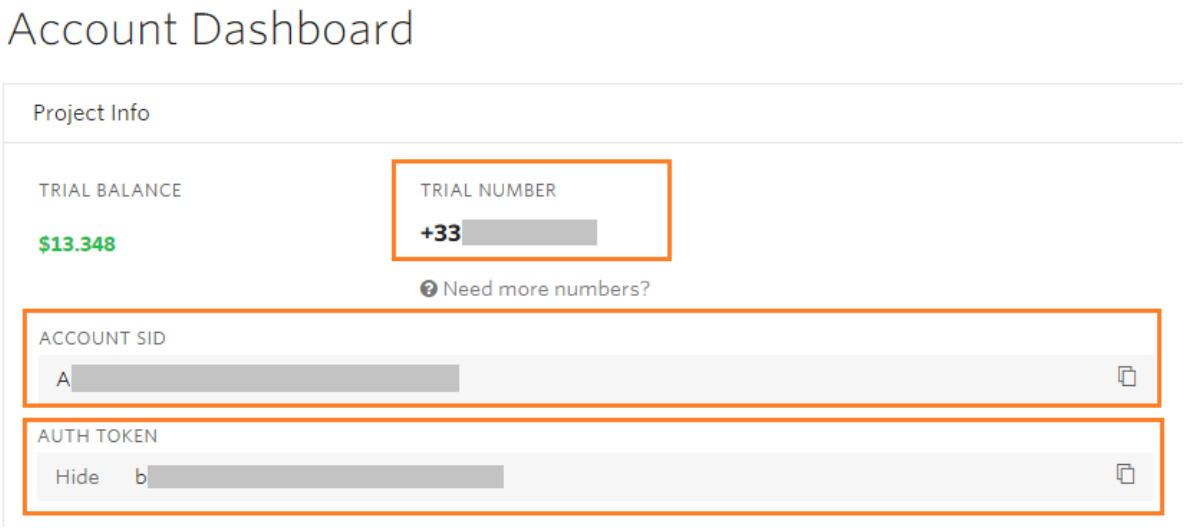


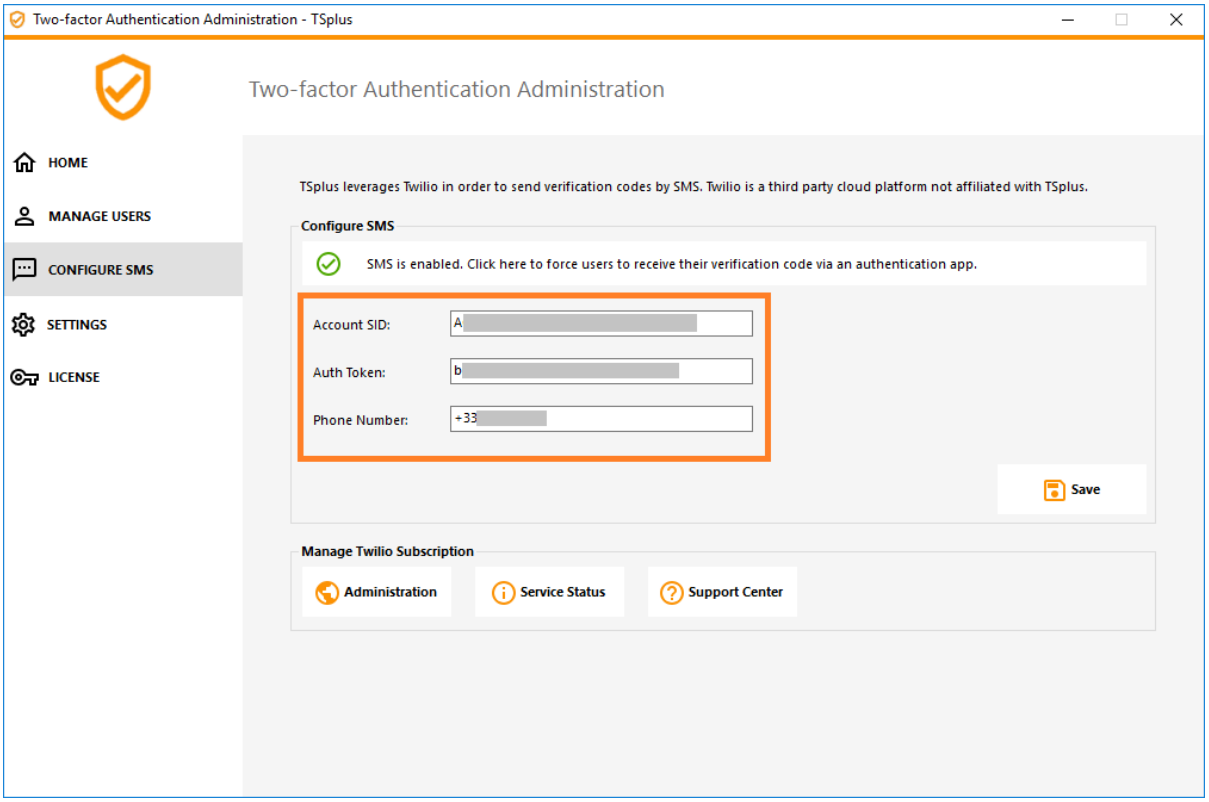
3. El siguiente paso solo es necesario para las versiones de prueba. Permite a Twilio verificar el número de teléfono real al que se enviarán los SMS.

Ingrese este número en el menú “Números de Teléfono” - “IDs de Llamante Verificados” tab :

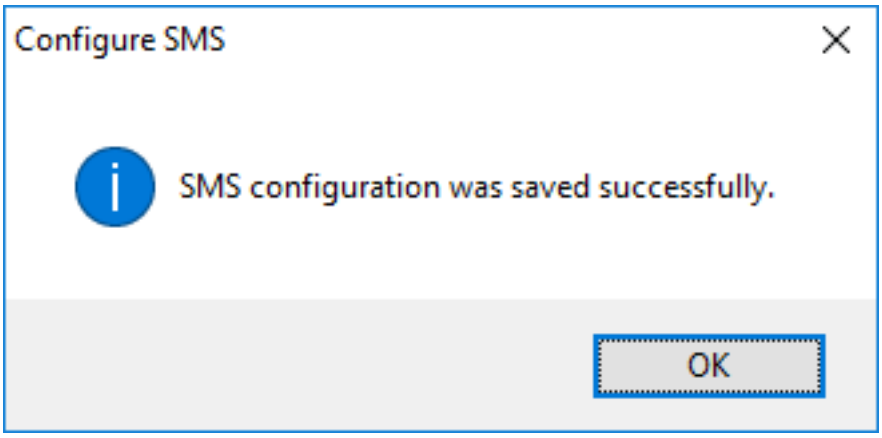


4. Podrás ingresar tu SID de cuenta, Token de autenticación y **Número de prueba** como el número de teléfono en el Configurar SMS pestaña de TSplus:





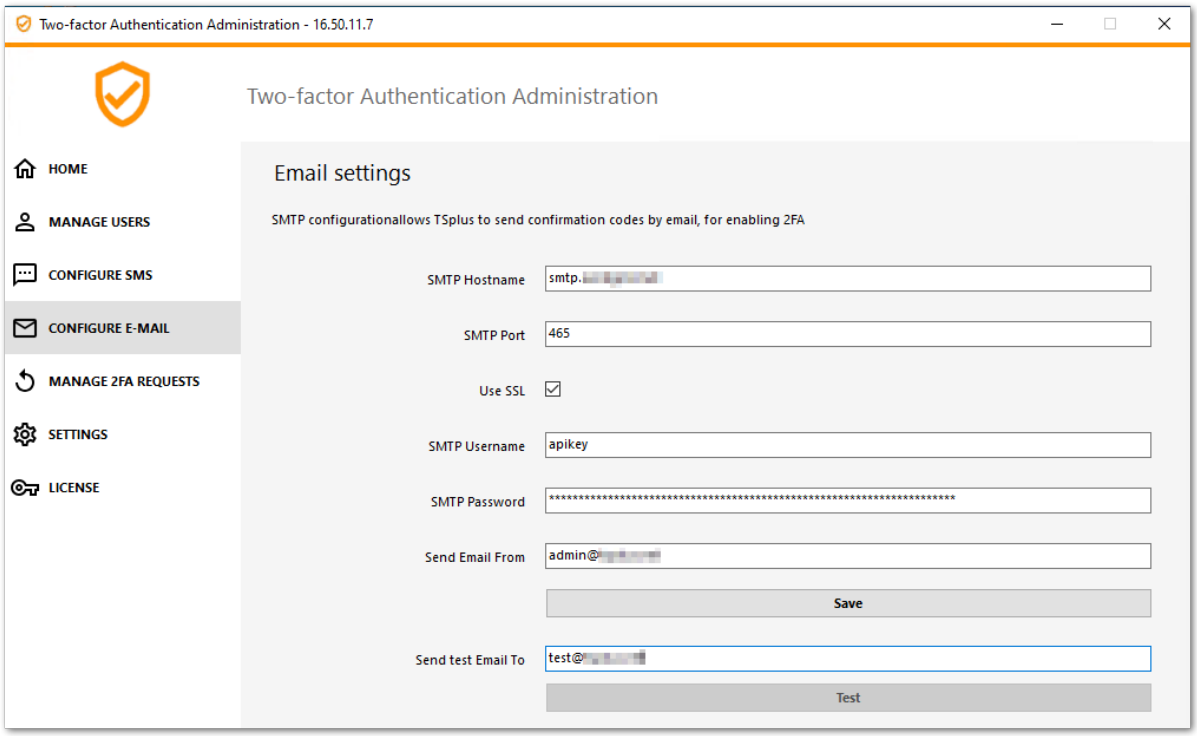
Luego, haga clic en Guardar. Se mostrará el siguiente mensaje:



Puedes gestionar tu suscripción de Twilio en el Gestionar la suscripción de Twilio sección, en la parte inferior de la Configurar SMS Administra tu cuenta, consulta el estado del servicio o contacta con el centro de soporte de Twilio simplemente haciendo clic en los botones correspondientes.

Configurar CORREO ELECTRÓNICO

Para que el usuario reciba códigos de verificación por CORREO ELECTRÓNICO, primero debe configurar su correo SMTP.



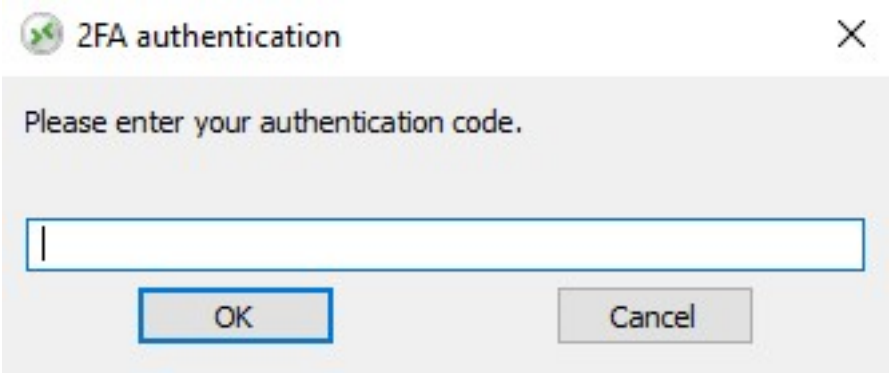
Iniciar sesión utilizando la autenticación de dos factores

Una vez que un usuario ha configurado su cuenta de TSplus en su aplicación de autenticación, podrá conectarse utilizando su contraseña y el código proporcionado por su aplicación de autenticación, por SMS o correo electrónico.

Desde el portal web de TSplus Remote Access:



Desde el cliente generado por TSplus:



Los servidores de aplicaciones TSplus y los dispositivos cliente deben compartir la misma hora. Esto significa que la hora y la fecha del servidor deben estar sincronizadas con un servidor de tiempo. Los dispositivos cliente también deben tener sincronización de tiempo, independientemente de la zona horaria en la que estén configurados.

Si una solicitud de autenticación proviene de un dispositivo cuya fecha y hora no están sincronizadas, o si la fecha y hora del servidor no están sincronizadas, esta solicitud puede ser rechazada.

La validación de la información entre el dispositivo y el servidor se relaciona con la hora UTC.

En el **Configuraciones** sección, el parámetro de discrepancia se utiliza para gestionar el período de validez del código, en intervalos de 30 segundos.

Ejemplo de validación o autenticación válida:

- el servidor está sincronizado con un servidor de tiempo, la zona horaria es UTC + 2, son las 2:30 p. m.
- el dispositivo está sincronizado con un servidor de tiempo, la zona horaria es UTC + 1, son las 1:30 p. m.
- el parámetro de discrepancia está configurado en 60, es decir, un período de validez del código de 30 minutos
- referido a la hora UTC, la hora del dispositivo y la hora del servidor son idénticas.

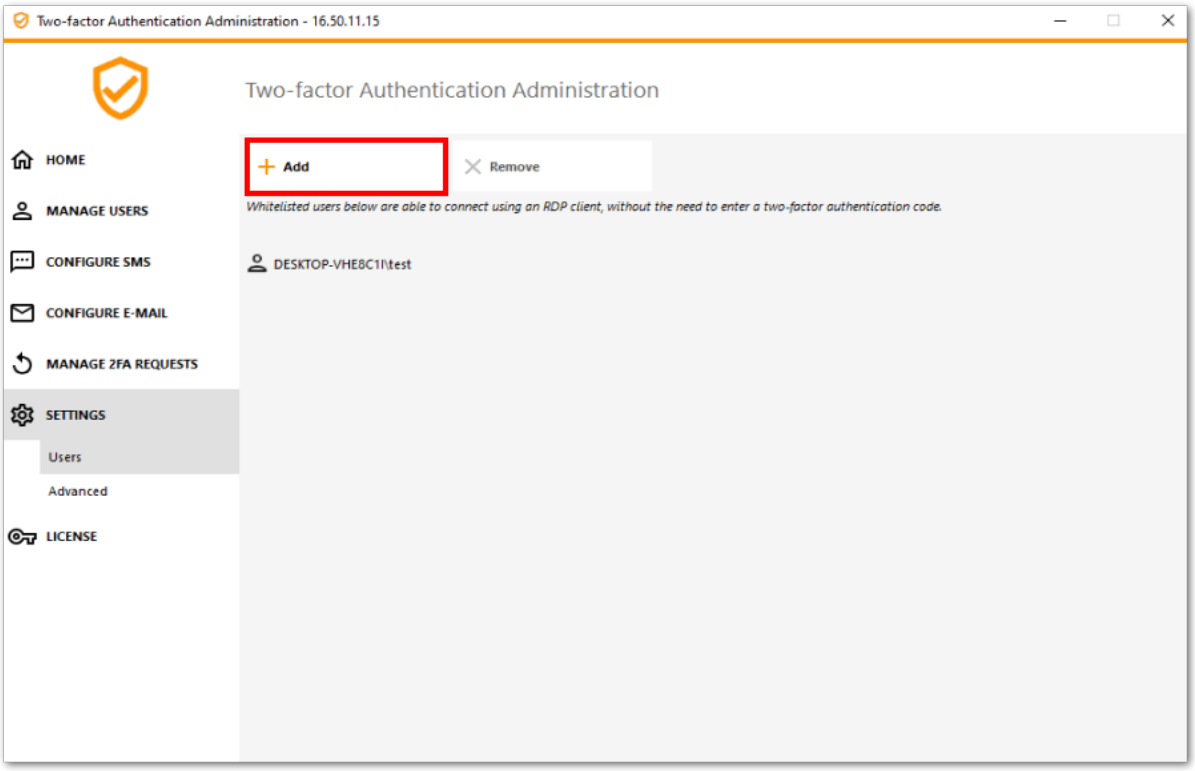
Ejemplo de validación o autenticación no válida:

- el servidor está sincronizado con un servidor de tiempo, la zona horaria es UTC + 2, son las 2:30 p. m.
- el dispositivo no está sincronizado con un servidor de tiempo, la zona horaria es UTC-1, la hora está configurada manualmente a la 1:30 p. m.
- el parámetro de discrepancia está configurado en 60, es decir, un período de validez del código de 30 minutos
- la hora del servidor referida a la hora UTC es 12:30 a. m.
- el tiempo comunicado por el Dispositivo, referido a la hora UTC es 2:30 pm
- la diferencia es de 120 minutos, por lo tanto, el código de validación es rechazado.

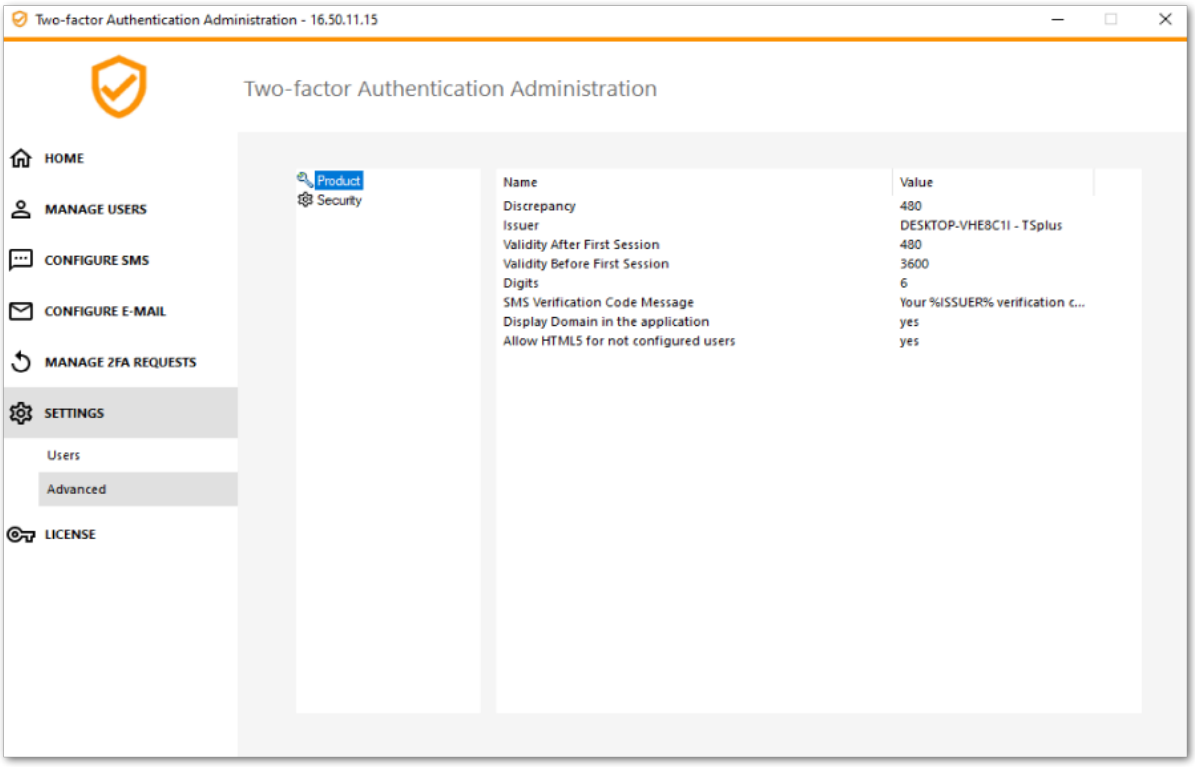
Configuraciones

La pestaña de Configuración te permite **permitir a los usuarios, para que se conecten utilizando un cliente RDP, sin necesidad de ingresar un código de autenticación de dos factores.**

Haga clic en el botón "Agregar" para añadir un usuario y elimine un usuario seleccionándolo y haciendo clic en el botón "Eliminar".



La pestaña Avanzado te permite configurar la autenticación de dos factores en ajustes detallados.

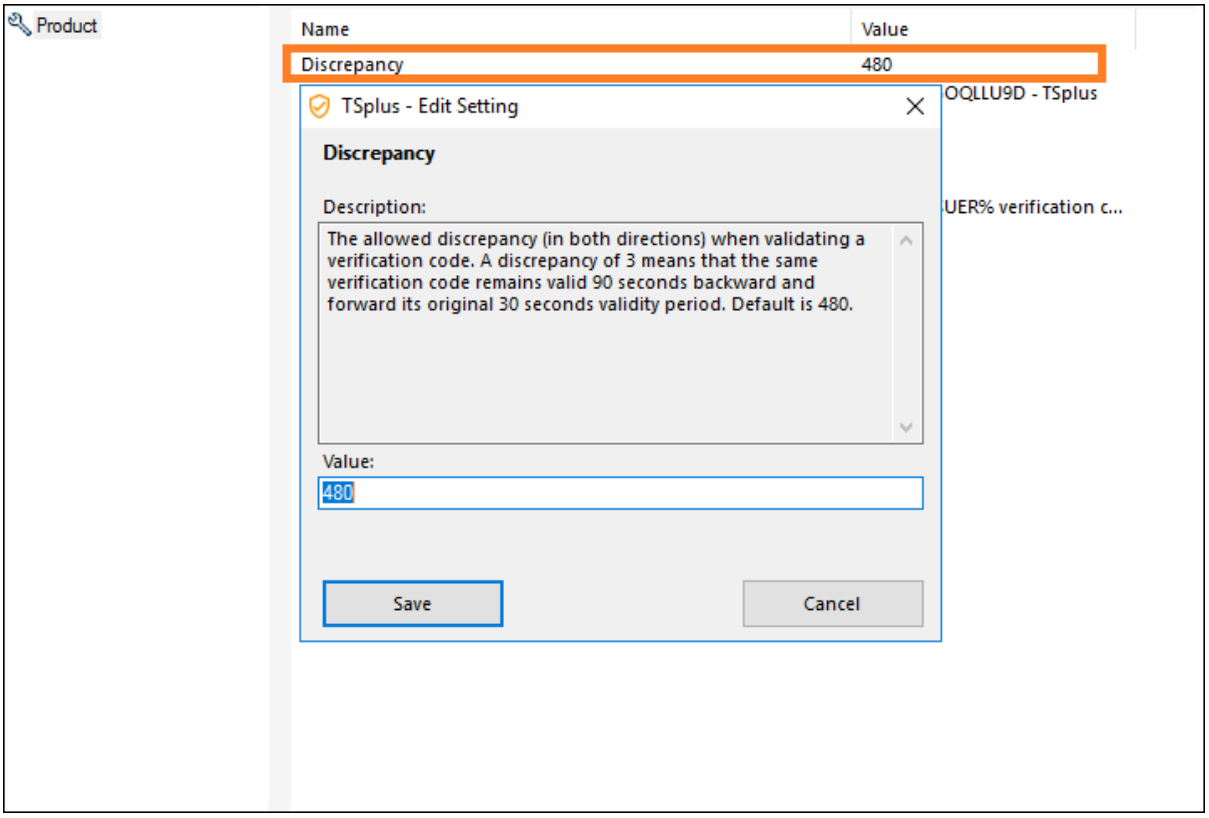


Discrepancia

Puedes modificar el valor de Discrepancia, que te permite establecer el tiempo de validación de

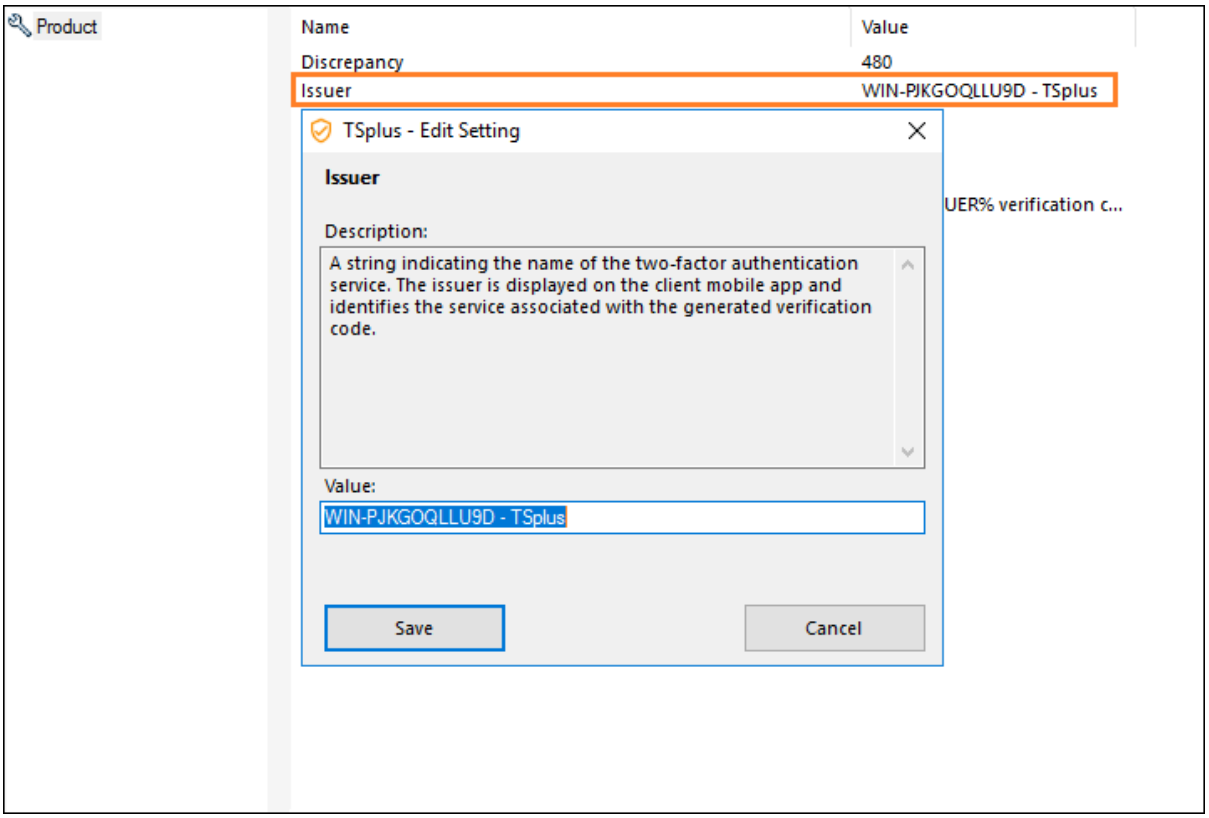
un código de verificación.

Una discrepancia de 3 significa que el mismo código de verificación sigue siendo válido 90 segundos hacia atrás y hacia adelante desde su período de validez original de 30 segundos. El valor predeterminado es 480, lo que significa 480 x 30 segundos = 4 horas.



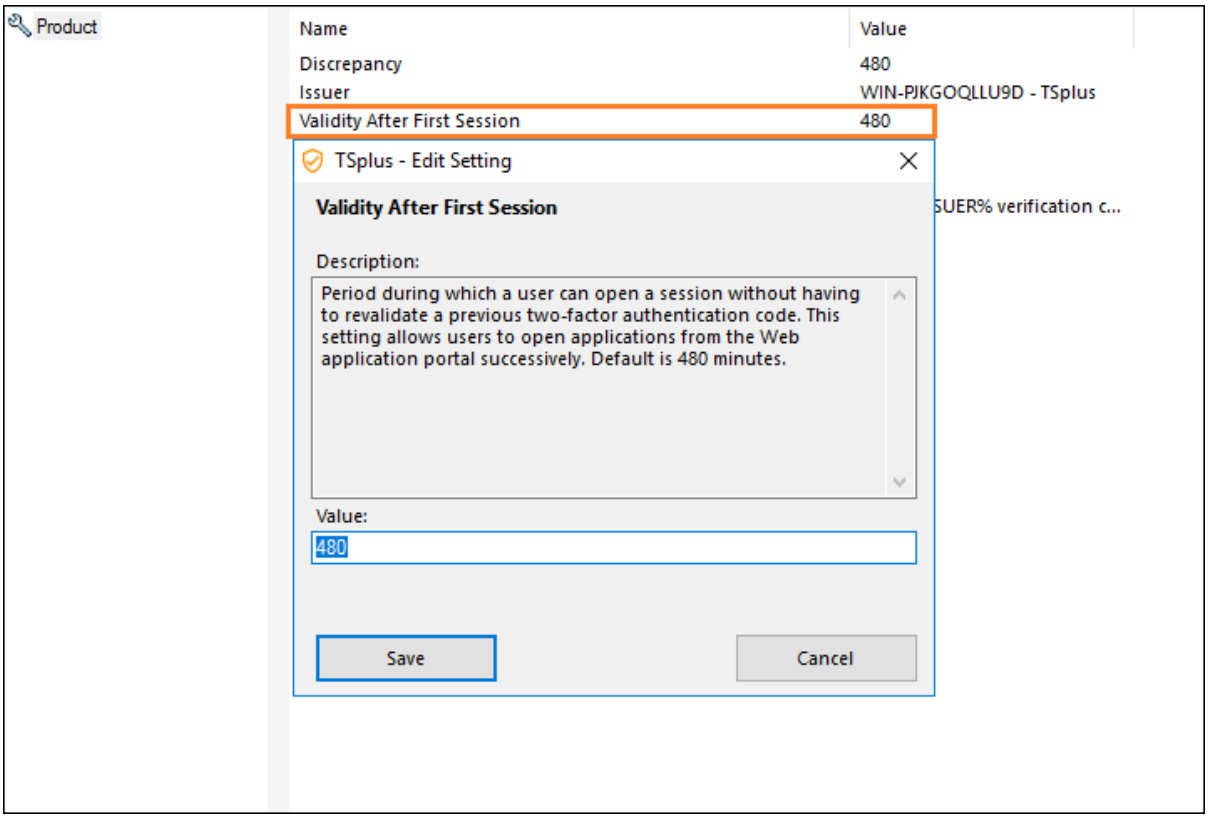
Emisor

Una cadena que indica el nombre del servicio de autenticación de dos factores. El emisor se muestra en la aplicación móvil del cliente e identifica el servicio asociado con el código de verificación generado. Por defecto, está compuesto por el nombre del servidor con TSplus.



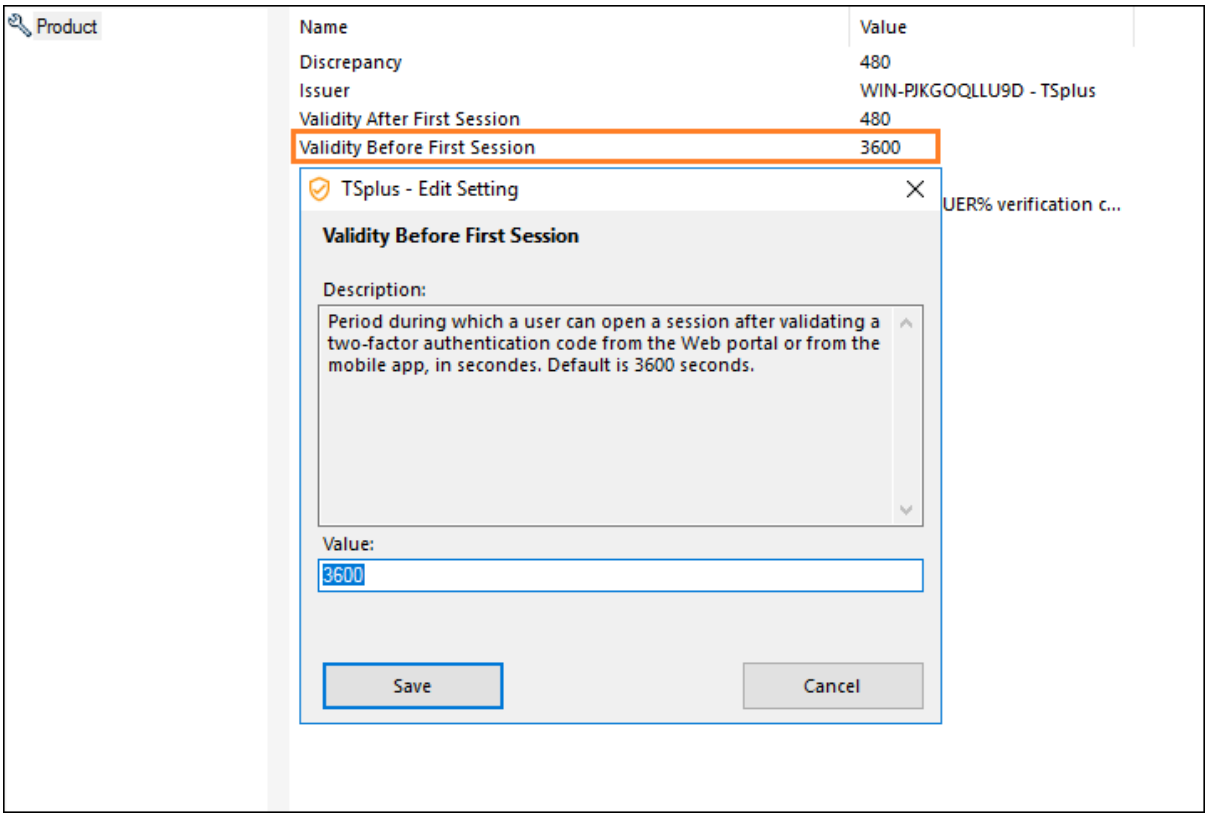
Validez después de la primera sesión

Período durante el cual un usuario puede abrir una sesión sin tener que volver a validar un código de autenticación de dos factores anterior. Esta configuración permite a los usuarios abrir aplicaciones desde el portal de la aplicación web de forma sucesiva. El valor predeterminado es de 480 minutos.



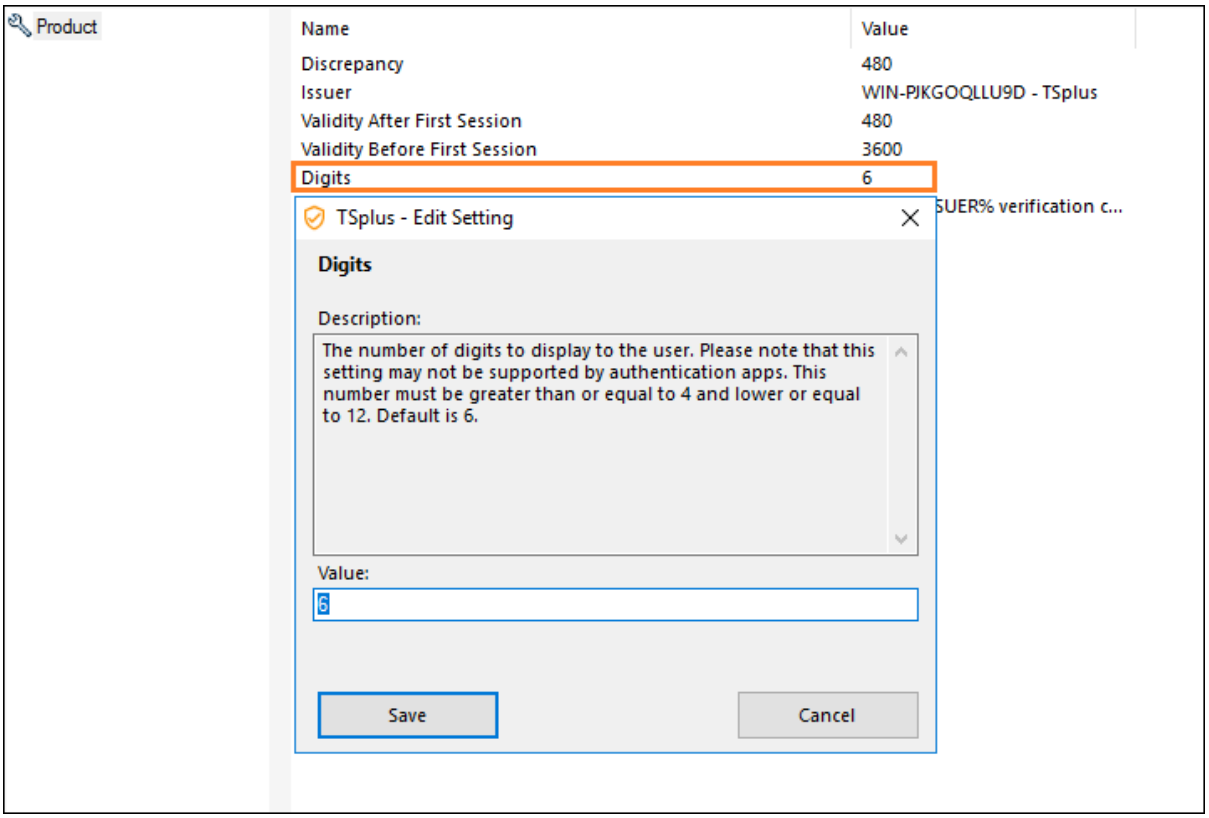
Validez antes de la primera sesión

Período durante el cual un usuario puede abrir una sesión después de validar un código de autenticación de dos factores desde el portal web o desde la aplicación móvil, en segundos. El valor predeterminado es 3600 segundos.



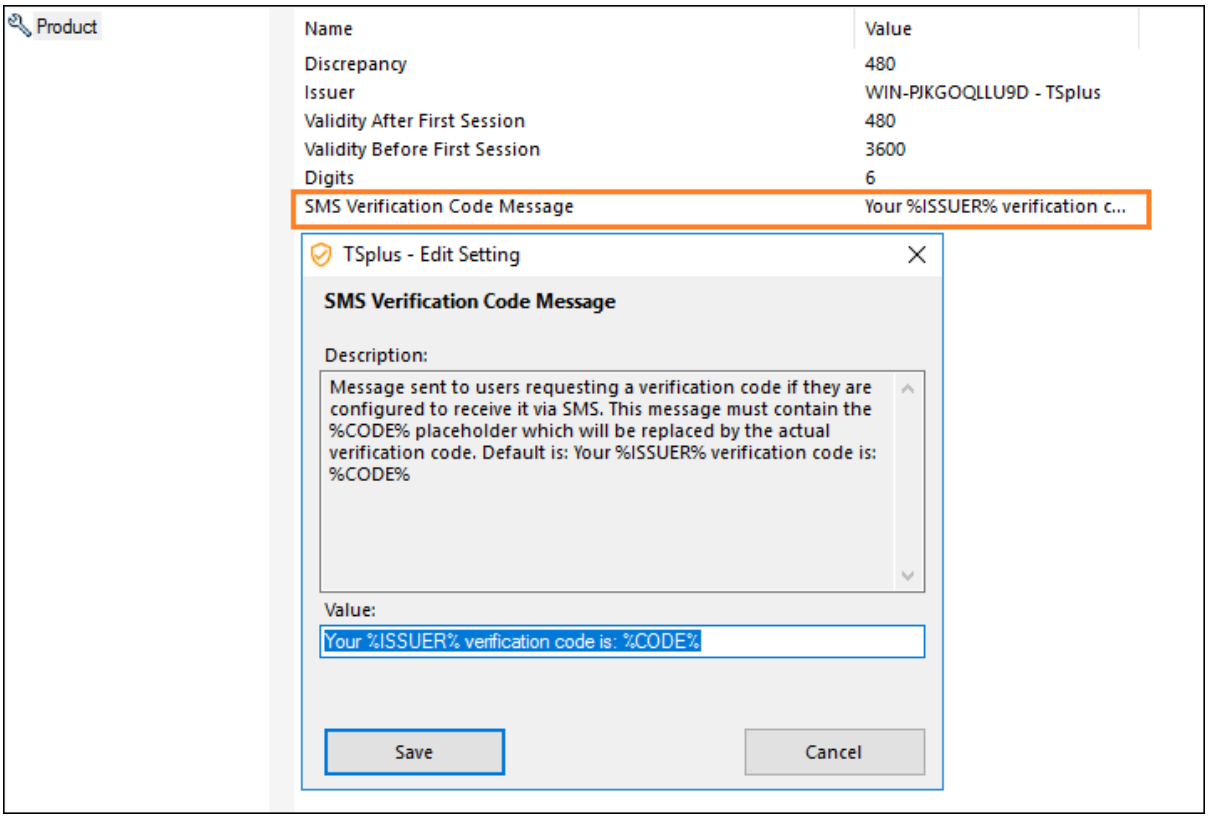
Dígitos

El número de dígitos a mostrar al usuario. Tenga en cuenta que esta configuración puede no ser compatible con las aplicaciones de autenticación. Este número debe ser mayor o igual a 4 y menor o igual a 12. El valor predeterminado es 6.



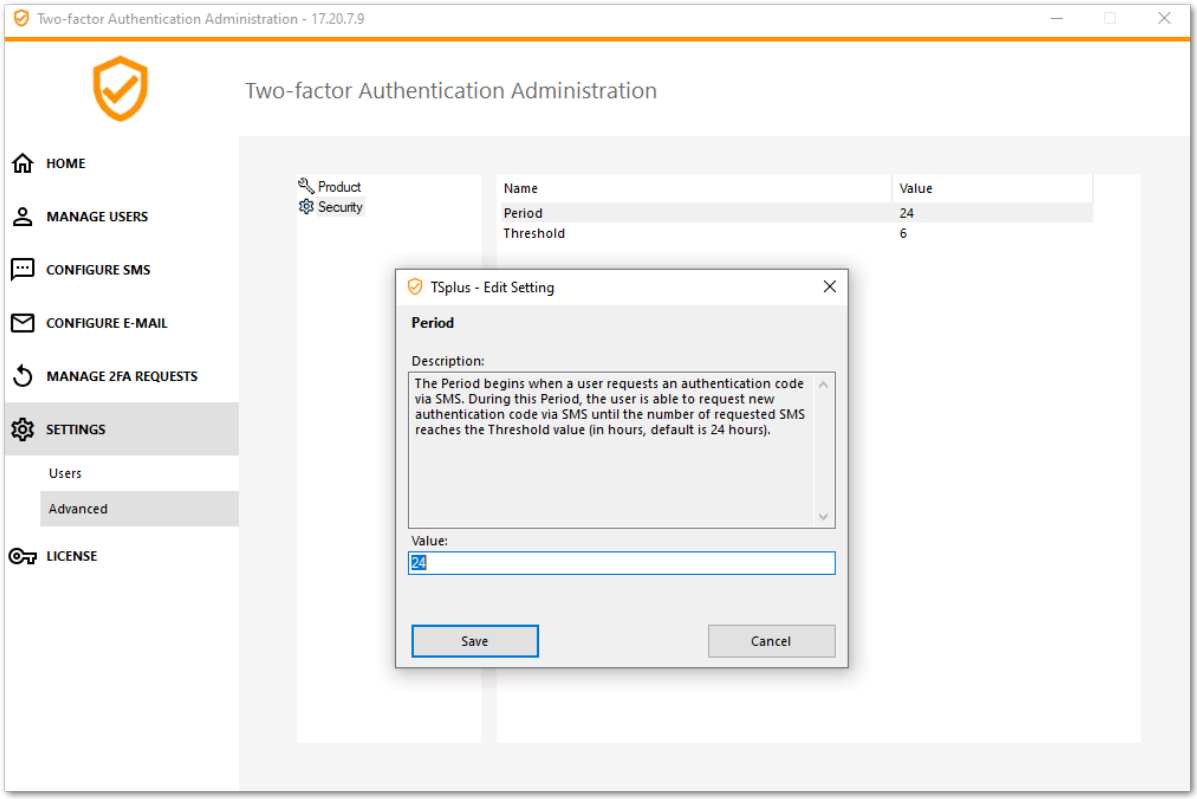
Mensaje del código de verificación por SMS

Mensaje enviado a los usuarios que solicitan un código de verificación si están configurados para recibirlo por SMS. Este mensaje debe contener el marcador de posición %CODE% que será reemplazado por el código de verificación real. El valor predeterminado es: Su código de verificación %ISSUER% es: %CODE%



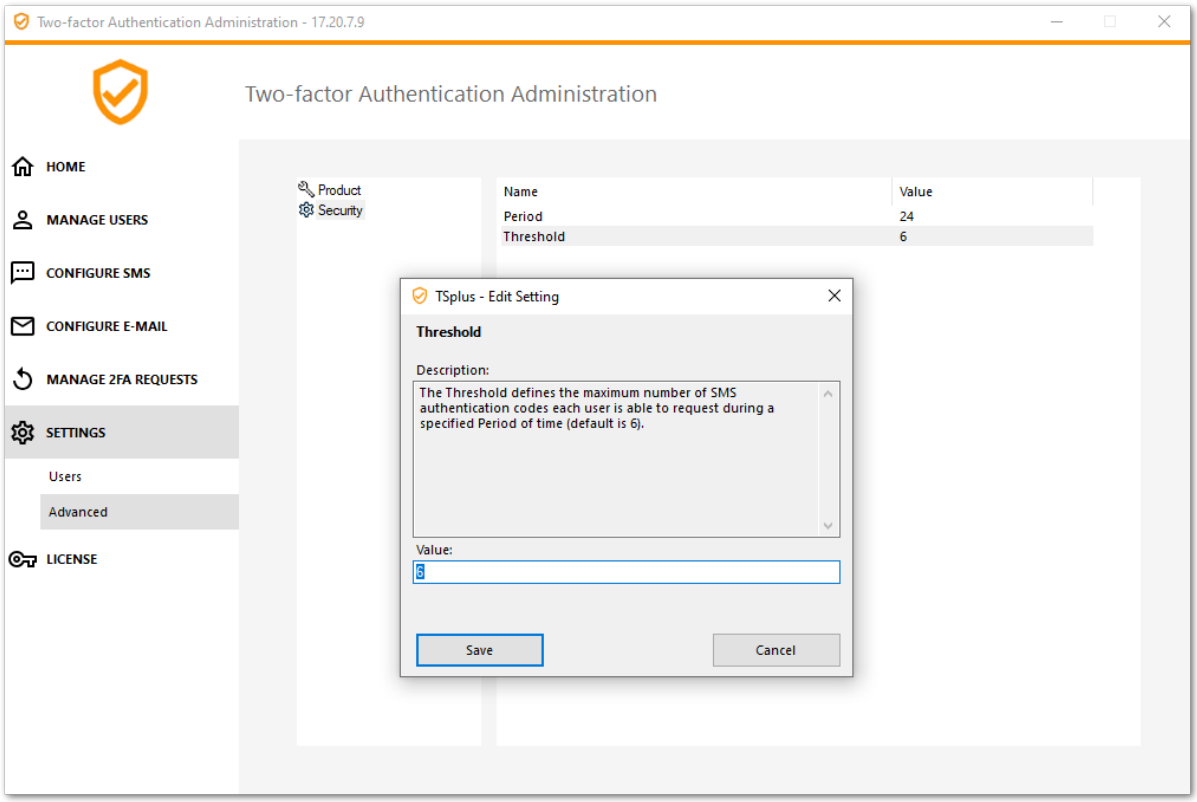
Período de Seguridad SMS

El período comienza cuando un usuario solicita un código de autenticación a través de SMS. Durante este período, el usuario puede solicitar un nuevo código de autenticación a través de SMS hasta que el número de SMS solicitados alcance el valor umbral (en horas, el valor predeterminado es de 24 horas).



Umbral de Seguridad SMS

El umbral define el número máximo de códigos de autenticación SMS que cada usuario puede solicitar durante un período de tiempo específico (el valor predeterminado es 6).



Impresora Universal (novaPDF)

El Impresora Universal de TSplus te permite previsualizar o imprimir documentos desde cualquier PC o dispositivo móvil compatible con TSplus Remote Access. La Impresora Universal es relevante desde una sesión HTML5 y cuando se está conectado utilizando un cliente generado. La Impresora Universal no es relevante al usar el cliente RDP estándar (mstsc.exe) porque las impresoras pueden ser compartidas entre el servidor y el cliente.

Iniciando la versión 17 de Remote Access, Universal Printer aprovecha novaPDF (https://www.novapdf.com/) para producir archivos PDF (Formato de Documento Portátil) que cumplen con el estándar de la industria al 100% desde el documento remoto. El documento PDF generado se envía a la impresora local deseada. La Impresora Universal (novaPDF) reemplaza a la Impresora Universal (CustPDF) y a la Impresora Universal (GhostScript), que han sido descontinuadas y ya no están disponibles para instalar en su servidor de Remote Access.

Dos impresoras están disponibles para la impresión remota: Impresora Universal e Impresora Virtual. Aunque la Impresora Virtual ofrece un mejor rendimiento de impresión, no es compatible con el cliente HTML5 y requiere la instalación de una aplicación cliente. Por lo tanto, la Impresora Universal se establece como la impresora predeterminada tras la configuración de Remote Access. Ver TSplus Virtual Printer .

Requisitos

NovaPDF11Service debe estar en la lista de exclusión de cualquier firewall o antivirus activo.

Configurar la Impresora Universal

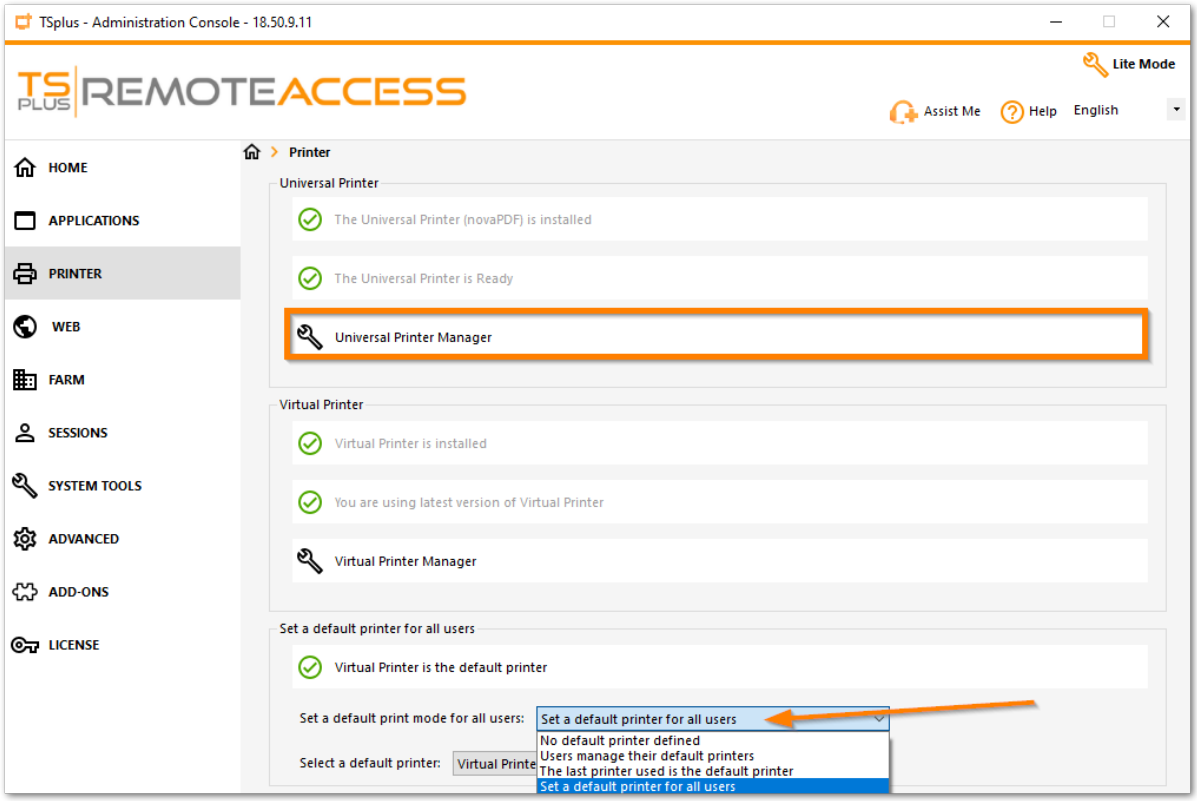
Para configurar su Impresora Universal, abra el AdminTool y haga clic en el Impresoras menú.

Para acceder al panel de control de Universal Printer, por favor navegue a través de AdminTool: Impresora > Administrador de Universal Printer.

Establecer una impresora predeterminada para todos los usuarios

- No se ha definido una impresora predeterminada: la configuración de la impresora predeterminada del usuario no se ve afectada.

- El usuario gestiona sus impresoras predeterminadas: la opción "Dejar que Windows gestione mi impresora predeterminada" está desactivada, por lo que depende del usuario seleccionar su impresora predeterminada.
- La última impresora utilizada es la impresora predeterminada: la opción "Dejar que Windows administre mi impresora predeterminada" está habilitada.
- Establecer una impresora predeterminada para todos los usuarios: el administrador obliga a la impresora predeterminada del usuario.



La sección de la Impresora Universal muestra cuatro mosaicos que permiten a los administradores:

- Verifique el estado de configuración de la Impresora Universal. Si la Impresora Universal no está instalada, al hacer clic en el mosaico se instalará la Impresora Universal.
- Verifique el estado de impresión de la Impresora Universal. Si la Impresora Universal no está lista para recibir trabajos de impresión, el mosaico puede mostrar información adicional relevante sobre el error.
- Verifique si la Impresora Universal está configurada como la impresora predeterminada. Si la Impresora Universal no está configurada como la impresora predeterminada, al hacer clic en el mosaico se configurará como la impresora predeterminada. Tenga en cuenta que este comportamiento puede ser anulado por sus usuarios si se les permite hacerlo.

- El azulejo llamado **Administrador de Impresoras Universal** lleva a una pantalla más detallada que proporciona acciones y propiedades adicionales, como eliminar la Impresora Universal.

Administrador de Impresoras Universal

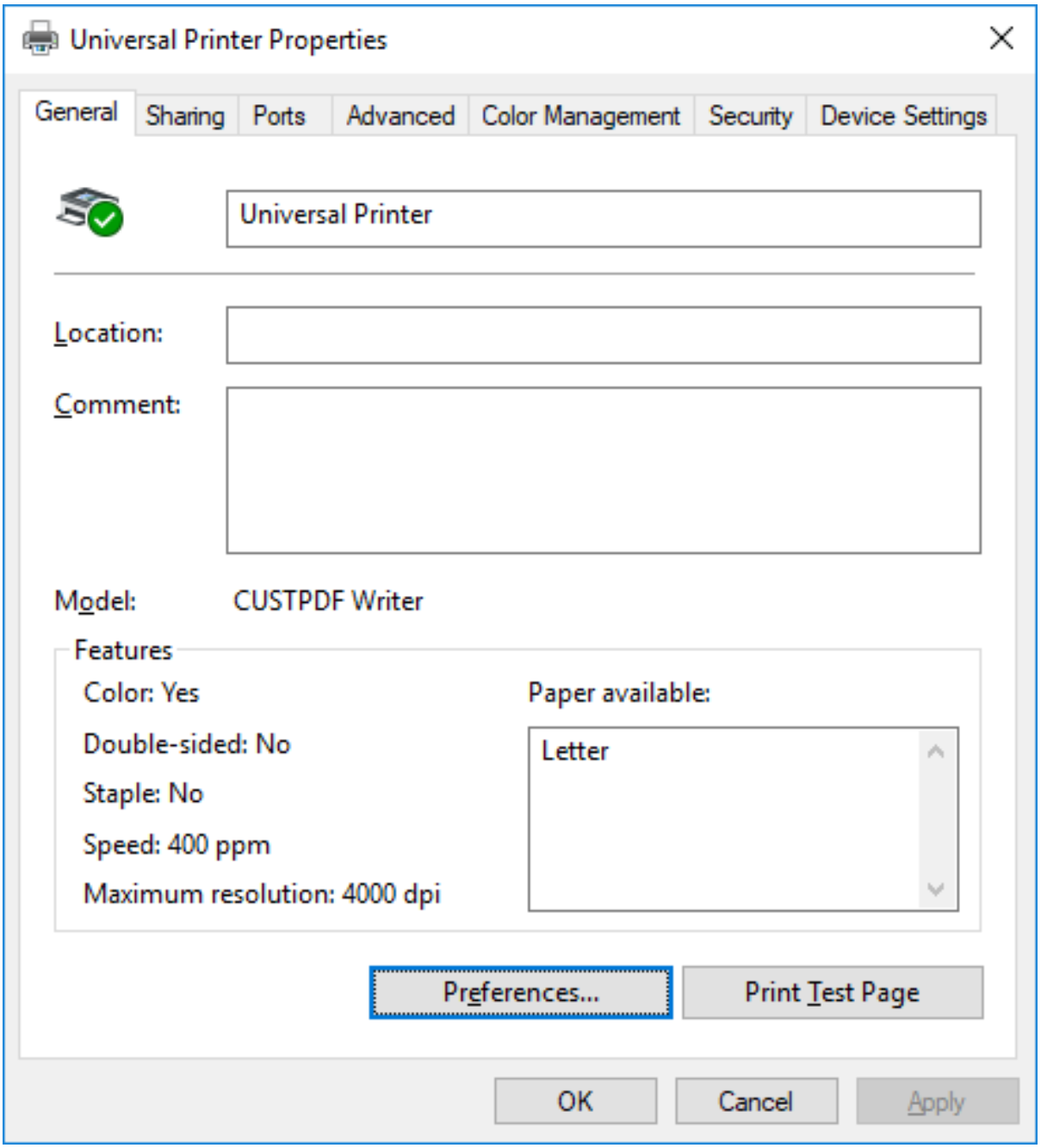
El Administrador de Impresoras Universales permite al administrador verificar el estado de la Impresora Universal, eliminar la Impresora Universal, acceder a la cola de impresión y a las propiedades de la impresora.

En particular, el botón ubicado en la parte inferior de la página permite a los administradores:

- **Eliminar la impresora universal** Desinstale la Impresora Universal. Se puede reinstalar más tarde desde esta pantalla.

- **Ver impresora** Abre una ventana donde puedes ver el estado de tus documentos de impresión, pausar, reanudar o cancelar el trabajo de impresión. También puedes establecer tus preferencias y propiedades de impresión.

- **Propiedades de la impresora universal** Abre esta ventana, donde puedes ver todas las propiedades de impresión. Después de la pestaña General, hay pestañas para compartir, puertos, avanzado, gestión del color, seguridad y configuración del dispositivo. En la parte inferior de la ventana emergente, la impresora **propiedades** permite a los administradores establecer el tamaño de página para imprimir desde A4 a cualquier tipo de formato de impresión. También puede elegir entre dos orientaciones de impresión: Vertical u Horizontal.

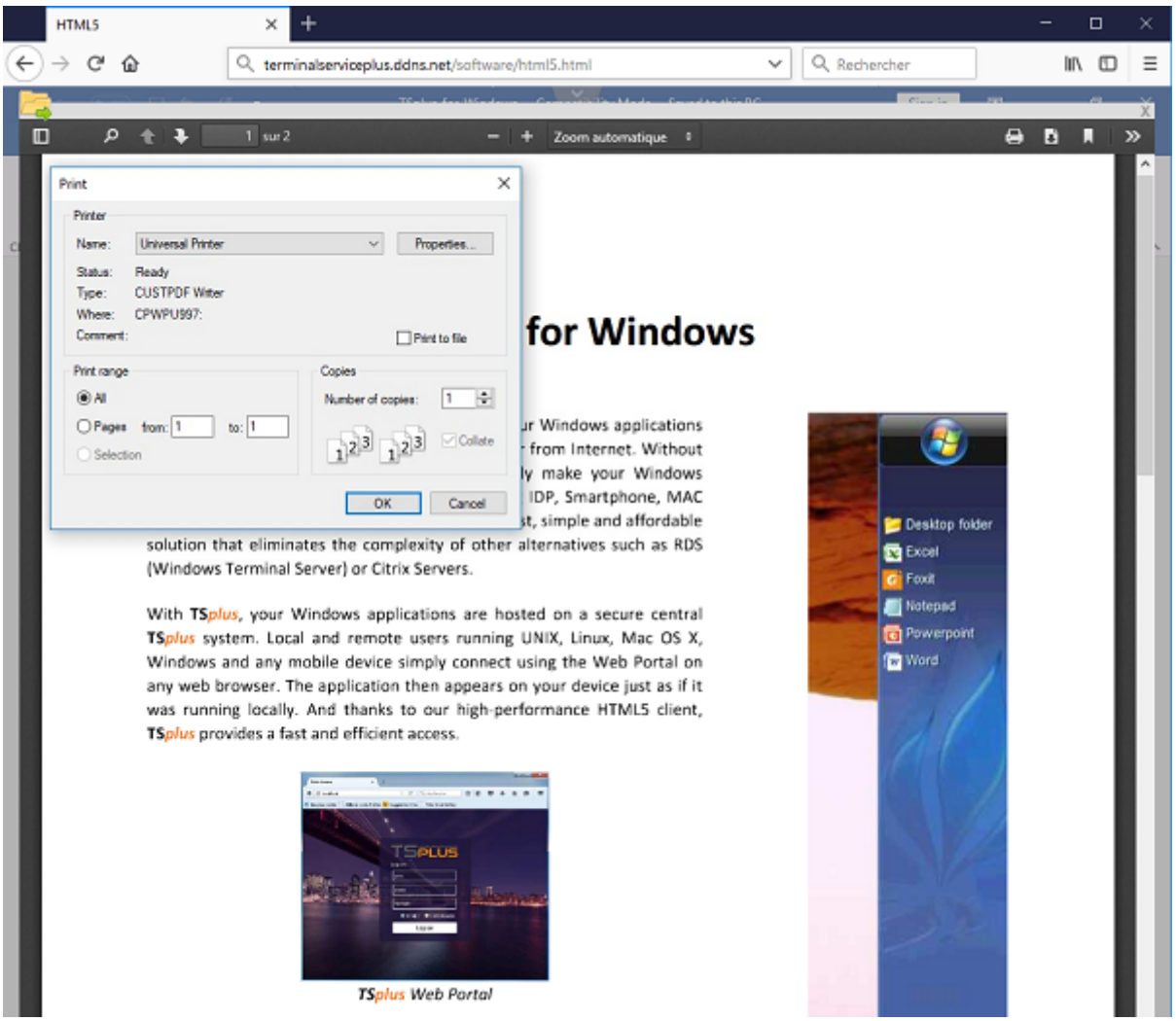


Nota: El Universal Printer aprovecha novaPDF, que permite a los administradores crear perfiles para definir fuentes, gráficos, marcas de agua, superposiciones y más a través del **Administrar perfiles** botón ubicado debajo de las secciones Tamaño de página y Orientación en la ventana emergente de propiedades de la impresora. Si se selecciona un perfil por defecto, entonces el **Mostrar el diálogo de Seleccionar Perfiles antes de imprimir** puede ser verificado para permitir al usuario seleccionar un perfil antes de imprimir. Por favor, consulte la documentación de novaPDF para más detalles sobre los perfiles: Administrador de perfiles .

Impresión con la Impresora Universal

Mientras se imprime utilizando esta impresora, el documento en la cola de impresión se convierte automáticamente en un archivo PDF por la impresora Universal Printer (novaPDF).

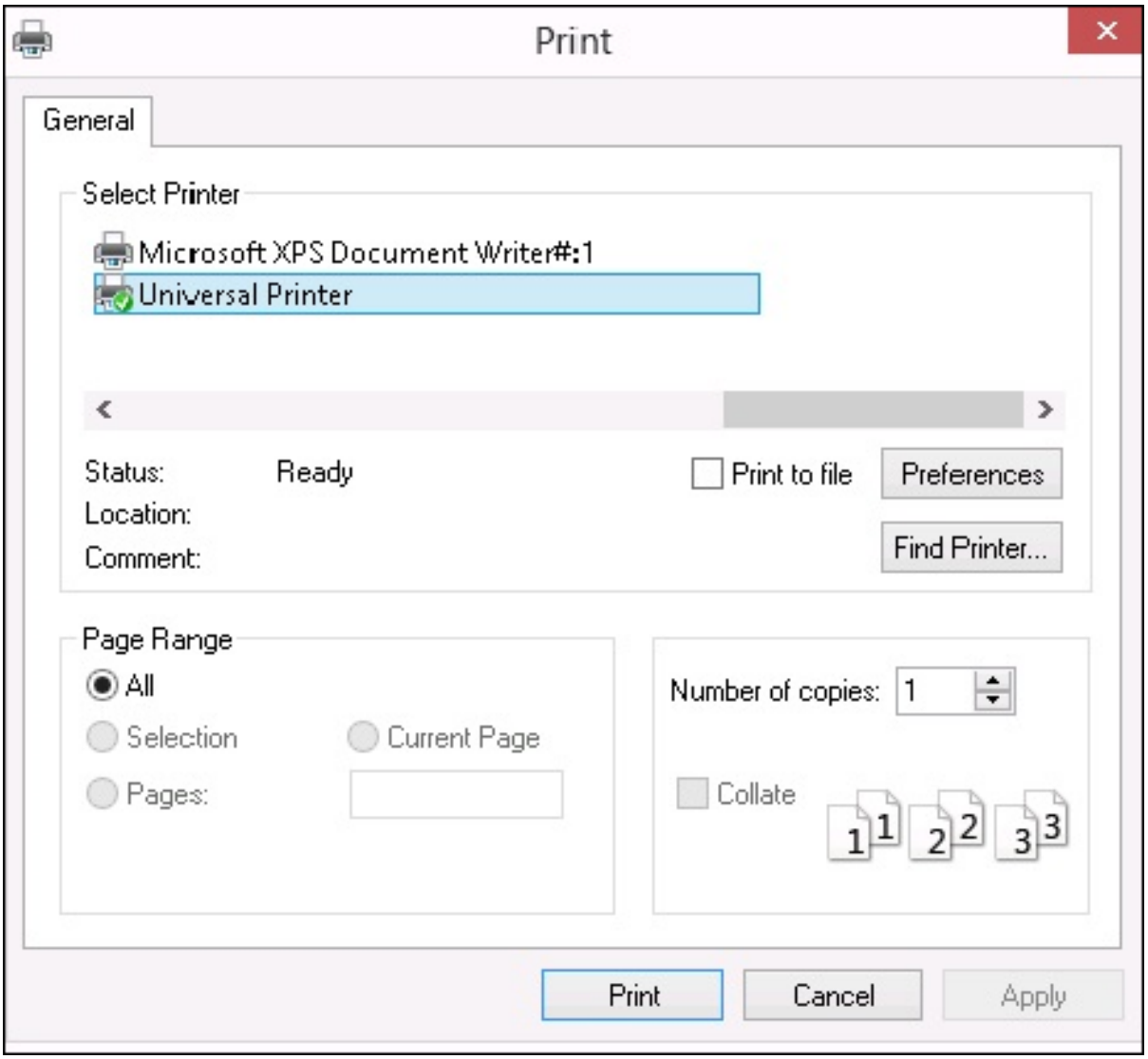




TSplus Web Portal

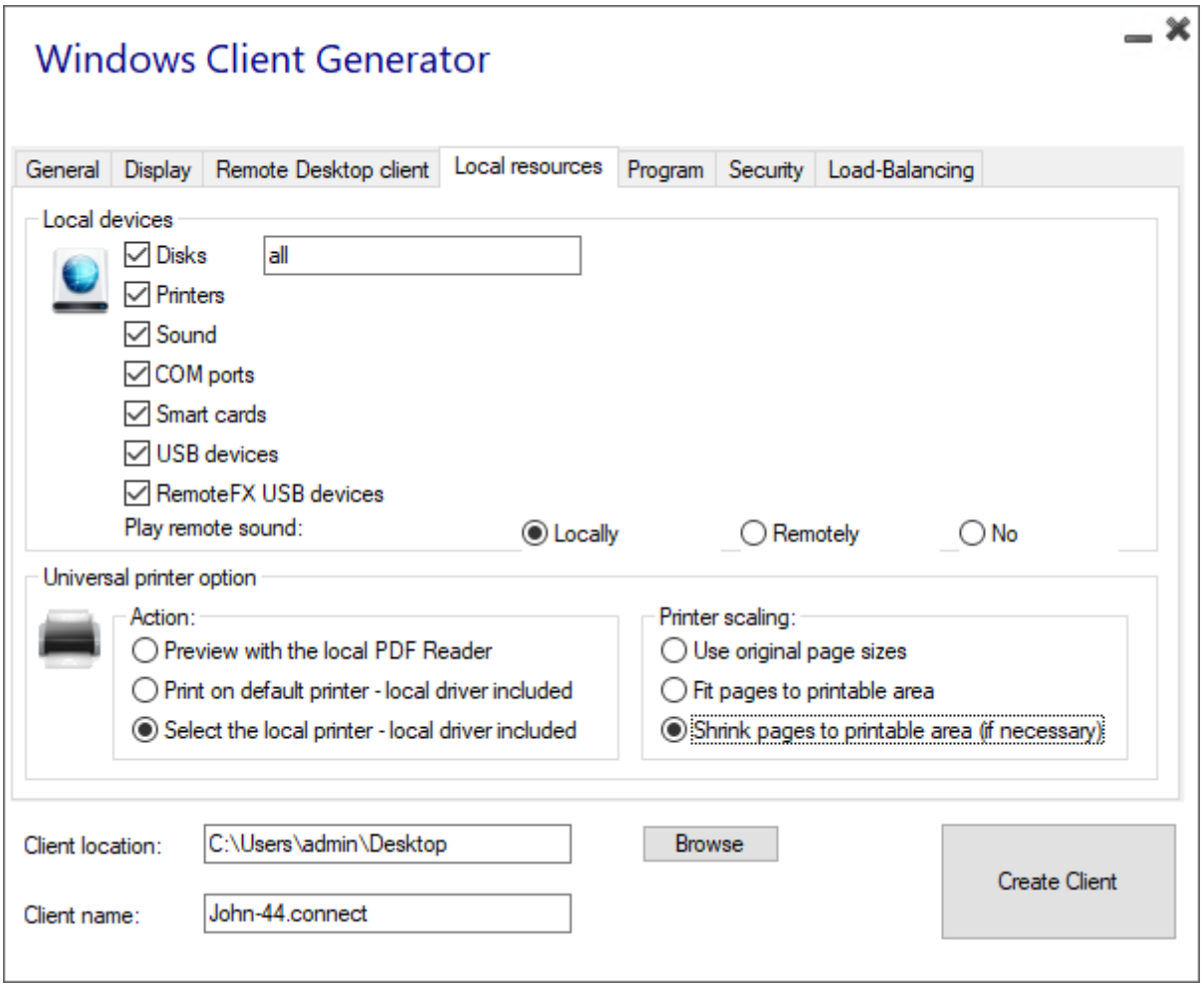
El archivo PDF generado se envía al lector de PDF local de la estación de trabajo del usuario.

Cada trabajo de impresión se abre tan pronto como está listo en el disco local del usuario. El proceso de impresión comienza una vez que el archivo PDF ha sido transferido al lado del cliente, lo que garantiza que el trabajo de impresión comience sin demora.



Configurando opciones de impresión con el Generador de Clientes

Puedes elegir entre 3 opciones de impresión en la pestaña de Recursos Locales del Generador de cliente portátil
Al utilizar el cliente de conexión de TSplus, necesitas mapear al menos el **C: unidad o todos los discos**



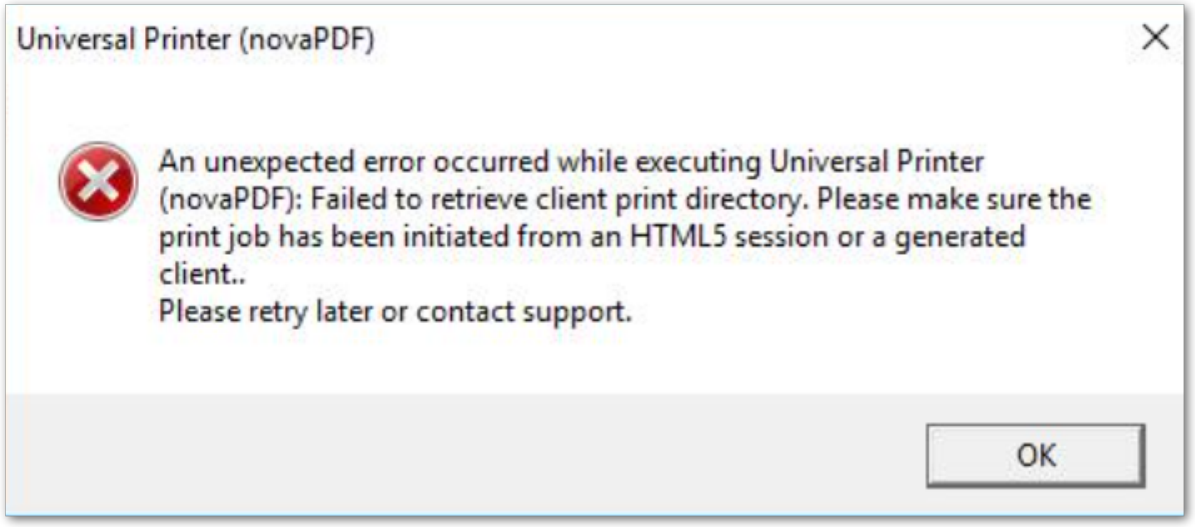
- **Vista previa del lector de PDF local** el documento se envía a la estación de trabajo del cliente y se abre el lector de PDF predeterminado local para mostrar el archivo PDF recibido. El usuario puede imprimirlo o guardar una copia en su disco duro local (este comportamiento se espera al imprimir desde una sesión HTML5).

- **Imprimir en la impresora predeterminada del usuario** el documento se imprime automáticamente con la impresora predeterminada del usuario (esta opción solo está disponible al usar el cliente de conexión de TSplus). Esta opción es preferida para los usuarios que tienen muchos trabajos de impresión para imprimir durante el día y utilizan la misma impresora para este propósito.

- **Seleccionar una impresora local** el usuario puede seleccionar una de sus impresoras locales (esta opción solo está disponible al usar el cliente de conexión TSplus).

Para leer archivos PDF, hoy en día muchas personas se las arreglan sin tener que usar una aplicación externa en absoluto. Tanto Firefox como Chromium, la versión de código abierto del navegador Chrome de Google, vienen empaquetados con lectores de PDF en el navegador, por lo que un complemento externo ya no es necesario para la mayoría de los usuarios.

PARA SU INFORMACIÓN
Si la unidad C: no está mapeada, el usuario recibirá este mensaje de error



Configurar la impresora novaPDF

Desde **Preferencias de impresora > Herramientas > Contraseña** , puedes:

- Editar la contraseña predeterminada
- Cambiar el idioma de la interfaz del Administrador de Perfiles
- Monitore el progreso de los trabajos de impresión en tiempo real
- Verifique el historial de la impresora

Abriendo trabajo de impresión en una nueva pestaña

Por defecto, los trabajos de impresión de una sesión HTML5 se muestran dentro de una ventana emergente como antes de la versión 17.10.

Es posible modificar este comportamiento y abrir trabajos de impresión en una nueva pestaña del navegador utilizando la siguiente configuración: **AdminTool > Avanzado > Sesión > Abrir trabajos de impresión en una nueva pestaña**

Perfiles

Profiles permite personalizar diseños, marcas de agua, nivel de compresión y mucho más. El Administrador de Perfiles te permite gestionar perfiles. Los perfiles consisten en configuraciones utilizadas al imprimir con la Impresora Universal. Por ejemplo, puedes establecer varios perfiles de impresión adaptados a requisitos de salida específicos, como distribuir PDFs, impresión de alta calidad, propósitos de revisión o marcar documentos como confidenciales.

Para abrir el Administrador de Perfiles, abre Dispositivos e Impresoras, haz clic derecho en Impresora Universal y selecciona Preferencias de impresión. Luego, haz clic en el **Administrar Perfiles** botón. La contraseña predeterminada es: pass@word1

Entendiendo los perfiles predeterminados

- **Perfil predeterminado** el perfil predeterminado está destinado a funcionar para imprimir un solo documento o múltiples documentos a la vez. Adecuado para la mayoría de los escenarios.
- **Perfil de Documentos Abiertos para Imprimir** Utilice este perfil para imprimir automáticamente un documento al abrirlo con un visor de PDF. Este perfil es útil para obtener un clic al imprimir desde una sesión HTML5.

Al abrir una sesión HTML5, el Perfil de Documentos Abiertos para Imprimir se selecciona automáticamente para el usuario actual. Sin embargo, la impresión automática en la sesión HTML5 se desactivará si otra sesión está actualmente abierta para el mismo usuario en modo RDP. En este caso, el Perfil Predeterminado se aplica por defecto.

Nota El perfil de documentos abiertos para impresión no se puede seleccionar automáticamente para aplicaciones UWP como Notepad en Windows 11 porque estas aplicaciones están diseñadas para ejecutarse en completa aislamiento con el sistema. Sin embargo, sigue siendo posible que el usuario seleccione manualmente el perfil a utilizar y lo elija por defecto para los próximos trabajos de impresión. No hay una solución alternativa en este momento. Sin embargo, el rediseño de la impresora novaPDF programado para la próxima versión importante de novaPDF prevista para el cuarto trimestre de 2024 levantará esta limitación.

¿Qué perfil puede elegir el usuario?

Por defecto, los usuarios pueden elegir qué perfil utilizar entre los dos perfiles predeterminados. Los usuarios pueden seleccionar un perfil como activo y no mostrar el cuadro de diálogo Seleccionar perfil para los próximos trabajos de impresión. Los administradores pueden definir uno o varios perfiles disponibles para todos los usuarios. Esta decisión anula cualquier elección de los usuarios. Ver https://www.novapdf.com/printer-manager-profiles-help.html .

Importante Se recomienda copiar los perfiles existentes para crear perfiles más personalizados, ya que los perfiles existentes incorporan varias características requeridas para la mayoría de las instalaciones, como fuentes incrustadas en el documento PDF generado.

Solución de problemas

Por favor, encuentre a continuación consejos de solución de problemas para resolver problemas de Universal Printer (novaPDF).

Manteniéndose actualizado

- Actualizar el Cliente de Conexión puede solucionar algunos problemas que ocurren en el lado del cliente.
- Revisa el registro de cambios para ver si una versión más reciente soluciona tu problema en https://dl-files.com/TSplus-changelog.html
- Recuerda que el equipo de desarrollo solo puede dar soporte a la última base de código.

Entendiendo qué parte del proceso de impresión falló

- ¿Se ha creado el trabajo de impresión en la cola de impresión? ¿Cuál es su estado?

Recopilando registros de errores de impresión

- **Registros de apertura de sesión** , especialmente útil para problemas como la recuperación fallida del directorio de impresión del cliente, ubicado en **C:\wsession\trace** .
- **Registros de la aplicación AdminTool** ubicado en **C:\Program Files (x86)\TSplus\UserDesktop\files** .
- **Registros de Universal Printer** enviando el trabajo de impresión al lado del cliente, ubicado en **C:\wsession\UniversalPrinter\logs** .
- **Registros de eventos de sesión** para el usuario de impresión, manejo de reconexiones, ubicado en **%appdata%\UniversalPrinter\logs** .

Recopilación de registros para problemas de instalación de impresoras

- **Registro de configuración** 2024-02-XX #XX.txt disponible en el **%temp%** directorio.
- **gestión de impresoras universales** XX022024.txt ubicado en **C:\Program Files (x86)\TSplus\UserDesktop\files** .
- Todos los archivos .txt ubicados en **C:\Program Files (x86)\TSplus\UserDesktop\files\UniversalPrinter** .

Recopilación de registros para errores de impresión del lado del cliente, al usar el Cliente de Conexión

- **version.dat** file. Por favor, siempre aconseje actualizar el Cliente de Conexión a la última versión.
- **Cliente de Conexión** y **Cliente de Impresora Universal** registros. Estos registros se pueden habilitar creando el siguiente valor de clave en el registro: **HKEY_LOCAL_MACHINE\Software\Digital River\ConnectionClient\Debug" = "true"** Los

registros resultantes se encuentran aquí: **C:\Usuarios \RDP6\logs** .

Actualizando TSplus Remote Access

Consulta nuestras correcciones y mejoras haciendo clic en Historial de cambios

Nuestro equipo de desarrollo está trabajando a diario para garantizar la estabilidad y compatibilidad de TSplus con las últimas versiones de los sistemas operativos de Microsoft y las últimas actualizaciones.

Estamos orgullosos de ofrecerte nuevas funciones y mejoras cada semana.

Esta es la razón por la que se recomienda mantener su servidor actualizado.

Cuando ocurre un problema de "2 sesiones por servidor", típicamente después de las actualizaciones de Windows el segundo martes del mes, por favor verifique su TSplus Remote Access (o TSplus LTS 18/17) versión.

Pronto se publicará una nueva versión para restaurar la compatibilidad con la última actualización de Windows.

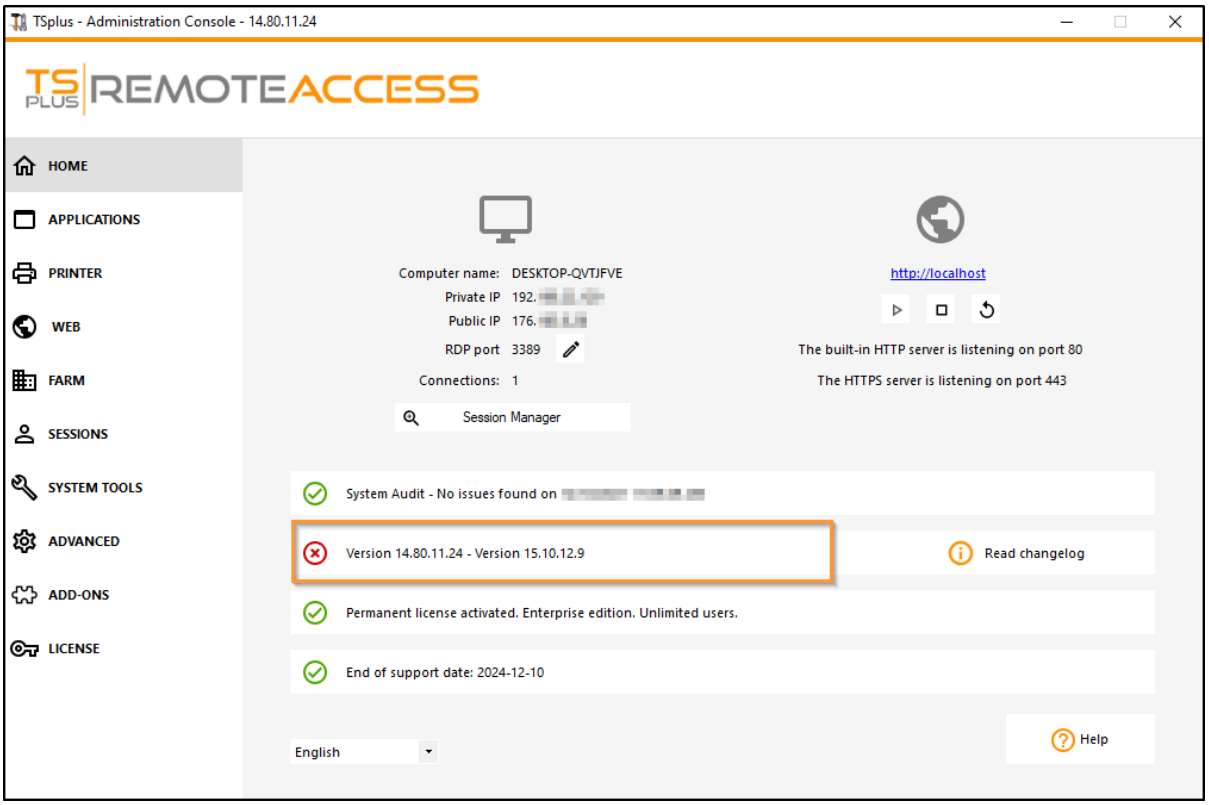
Como solución temporal, puede desinstalar la actualización de Windows del día y reiniciar.

Importante: Evite desinstalar TSplus Remote Access o restaurar una imagen del sistema anterior. Estas acciones pueden provocar conflictos de licencia que son mucho más complejos de resolver. En la mayoría de los casos, un simple reinicio es suficiente para aplicar automáticamente las correcciones de compatibilidad.

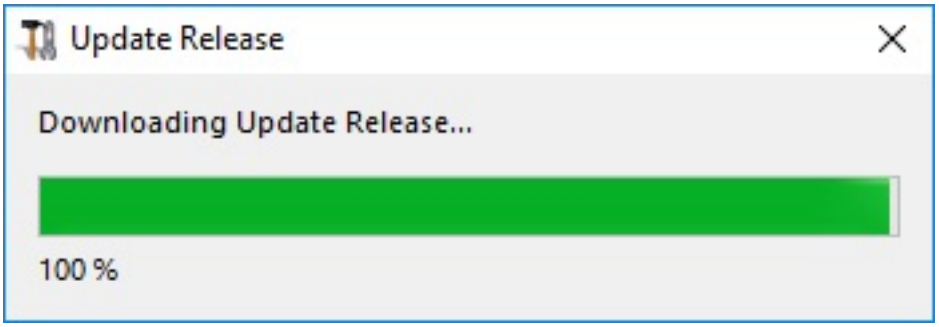
Al suscribirse a nuestros servicios anuales de Soporte y Actualizaciones, tendrá acceso a las últimas Actualizaciones y correcciones de errores.

Para ver qué versión de TSplus tienes y actualizarla:

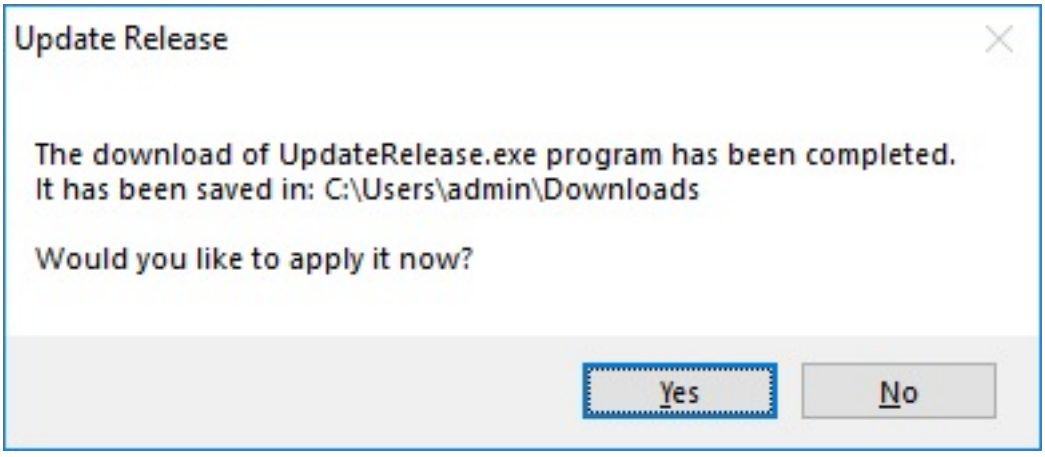
- Puedes verificar el estado de tu versión de TSplus en la pestaña Inicio de tu AdminTool:



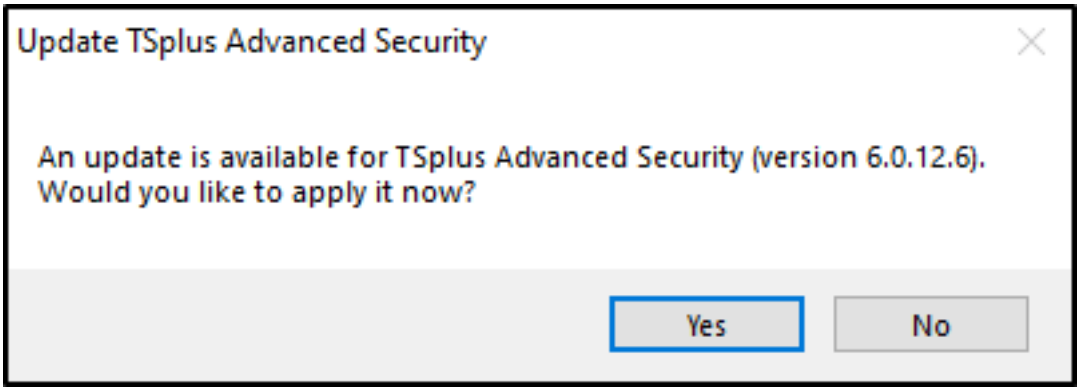
- Puedes hacer clic en él. Desde la versión 11.50 de TSplus, el AdminTool se descarga automáticamente…



…y aplica el programa de lanzamiento de actualizaciones cuando se solicita:



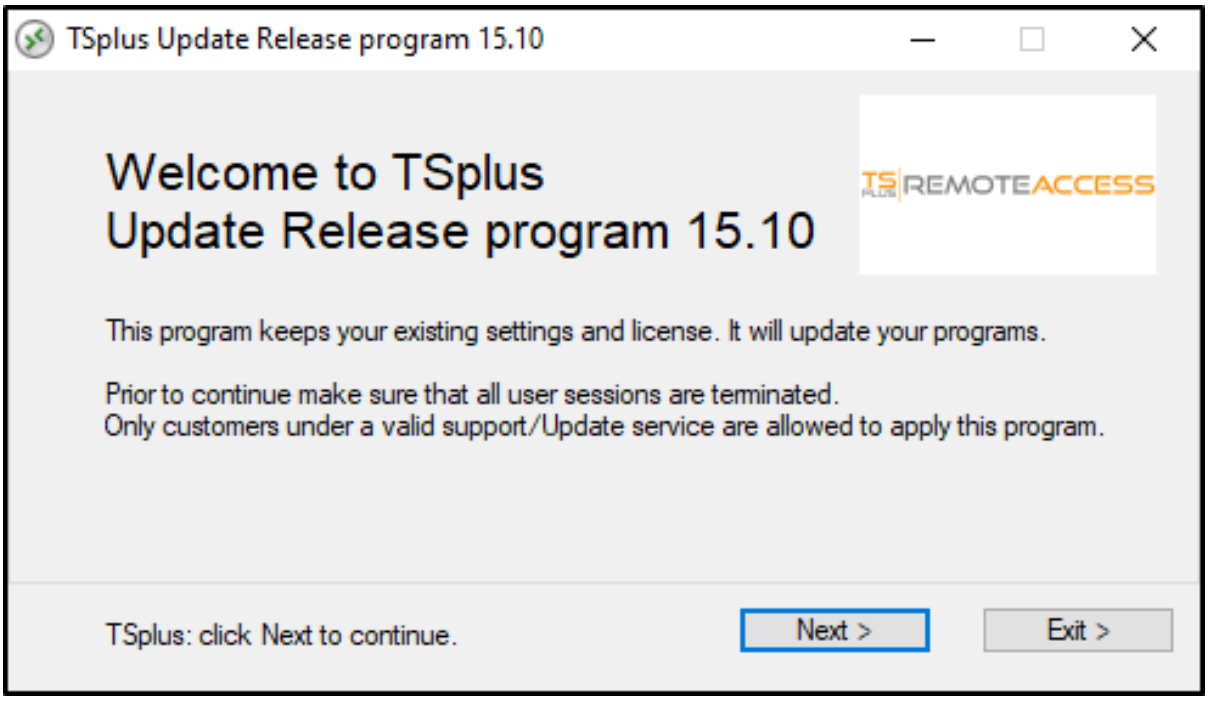
- Desde la versión 11.40 de TSplus, tendrás la opción de instalar TSplus Advanced Security nuestra poderosa Adición de Seguridad, en su versión de prueba Ultimate (todas las funciones de seguridad gratis para usar durante 2 semanas) a su sistema TSplus:

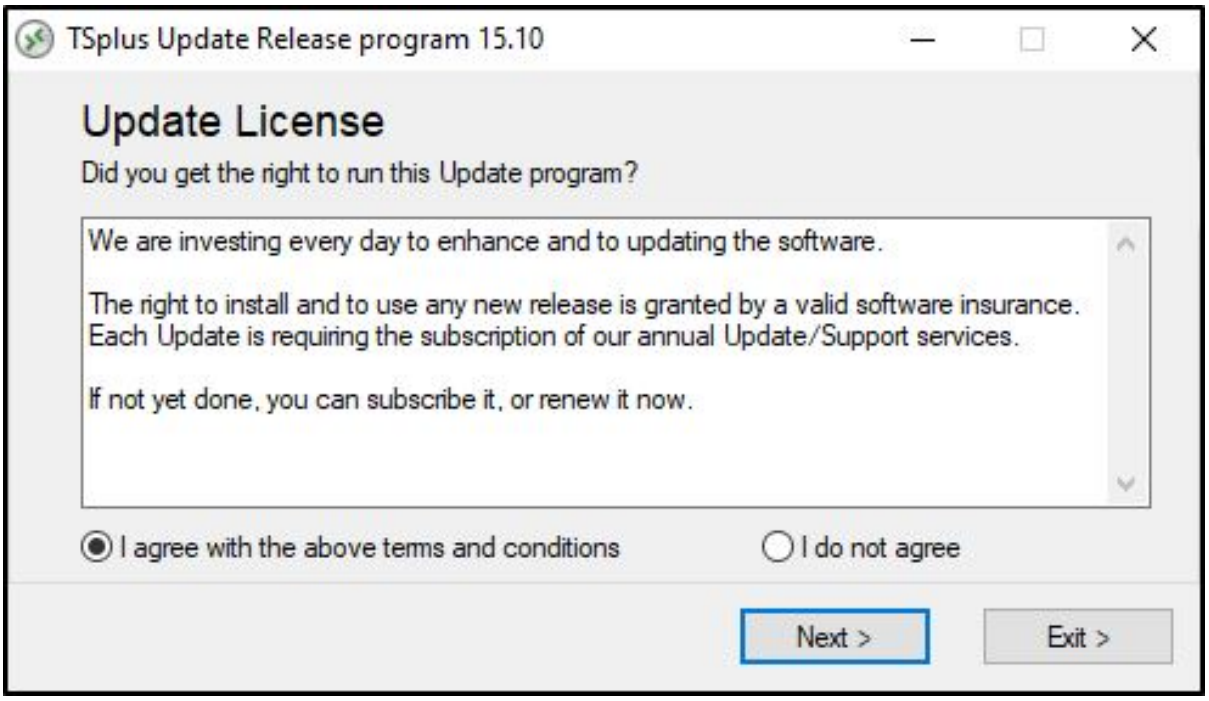


Aún puedes descargarlo a través de este enlace: Actualización de la versión y aplíquelo manualmente.

El programa de actualización está diseñado para mantener seguros sus ajustes actuales de TSplus.

Si aún no se ha suscrito a los servicios de actualización/soporte de TSplus, o si su suscripción ha expirado, no podrá ejecutar el programa de lanzamiento de actualizaciones:

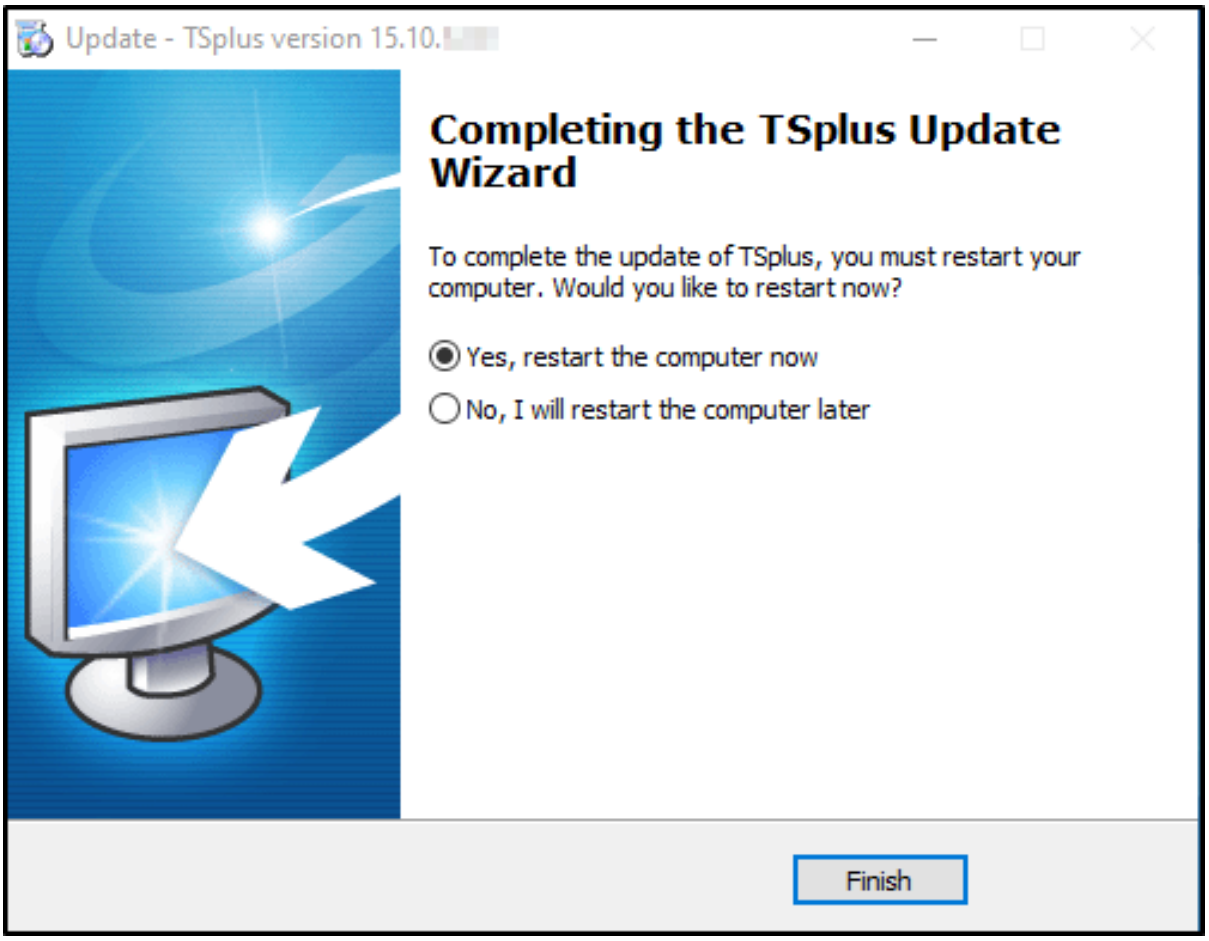




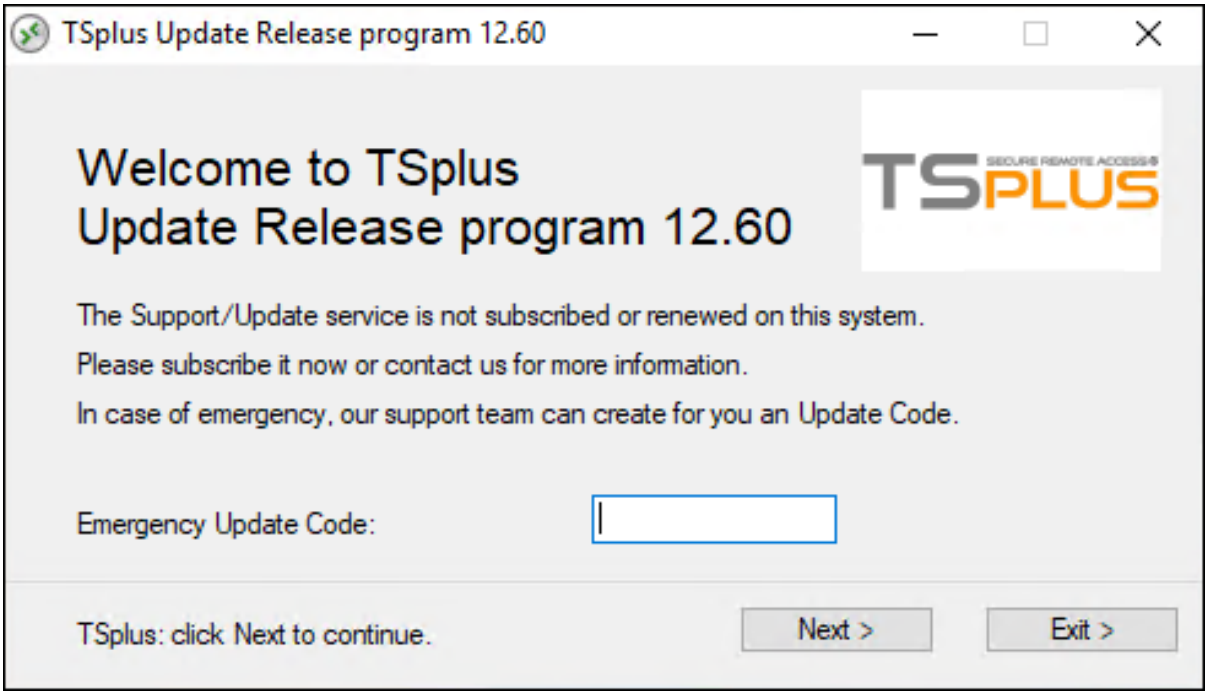
En tal caso, le recomendamos que realice su pedido en nuestra página de tienda.

Recibirá la información adecuada para descargar su archivo support.lic. Activar sus servicios de Actualización/Soporte es un proceso fácil descrito. aquí .

Cuando se complete la actualización, se requiere un reinicio:



Para versiones anteriores a la v14, solo para requisitos específicos, el equipo de soporte de TSplus puede entregar un código de actualización de emergencia que desbloqueará el programa de lanzamiento de actualizaciones.



Problema de actualización:

Verifique si falta el archivo

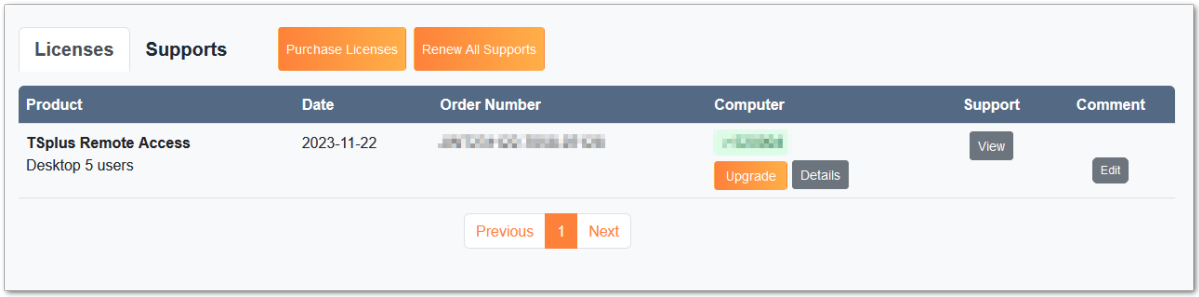
C:\Program Files (x86)\TSplus\reboot_required.dat

1. Si este archivo está presente, elimínalo.
2. Reinicie su servidor
3. Ejecuta la actualización nuevamente desde este enlace haciendo clic aquí : Actualización de la versión

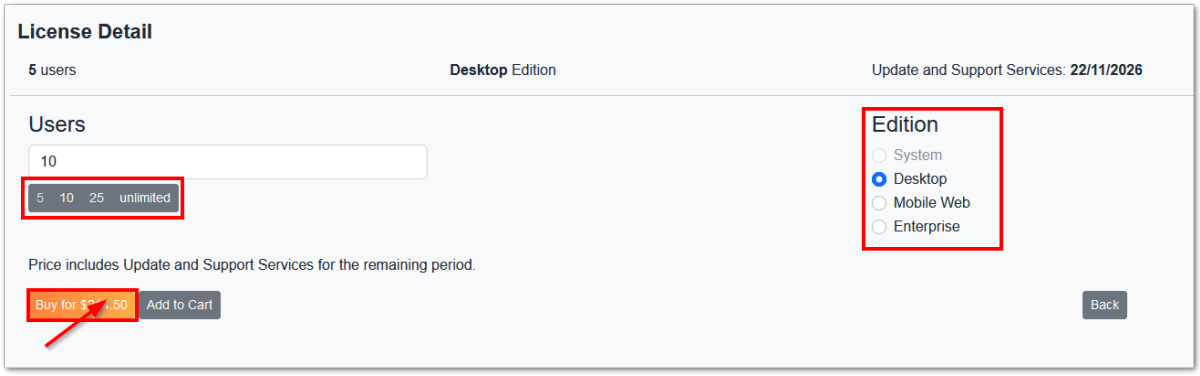
---

Actualizando su versión de TSplus

Si deseas actualizar tu versión actual de TSplus, para agregar más usuarios o más funciones, regístrate en tu portal de licencias.



Seleccione su opción de actualización (usuarios y versión) y haga clic en **Comprar por** para continuar en nuestra tienda.



Después de su compra, la actualización será instantánea y visible en su portal de licencias. También debes seguir el mismo procedimiento en tu dispositivo para que esté vinculado a tu licencia.

En su servidor, haga clic en el **Actualiza tu licencia** botón en la herramienta de administración > pestaña de licencia.

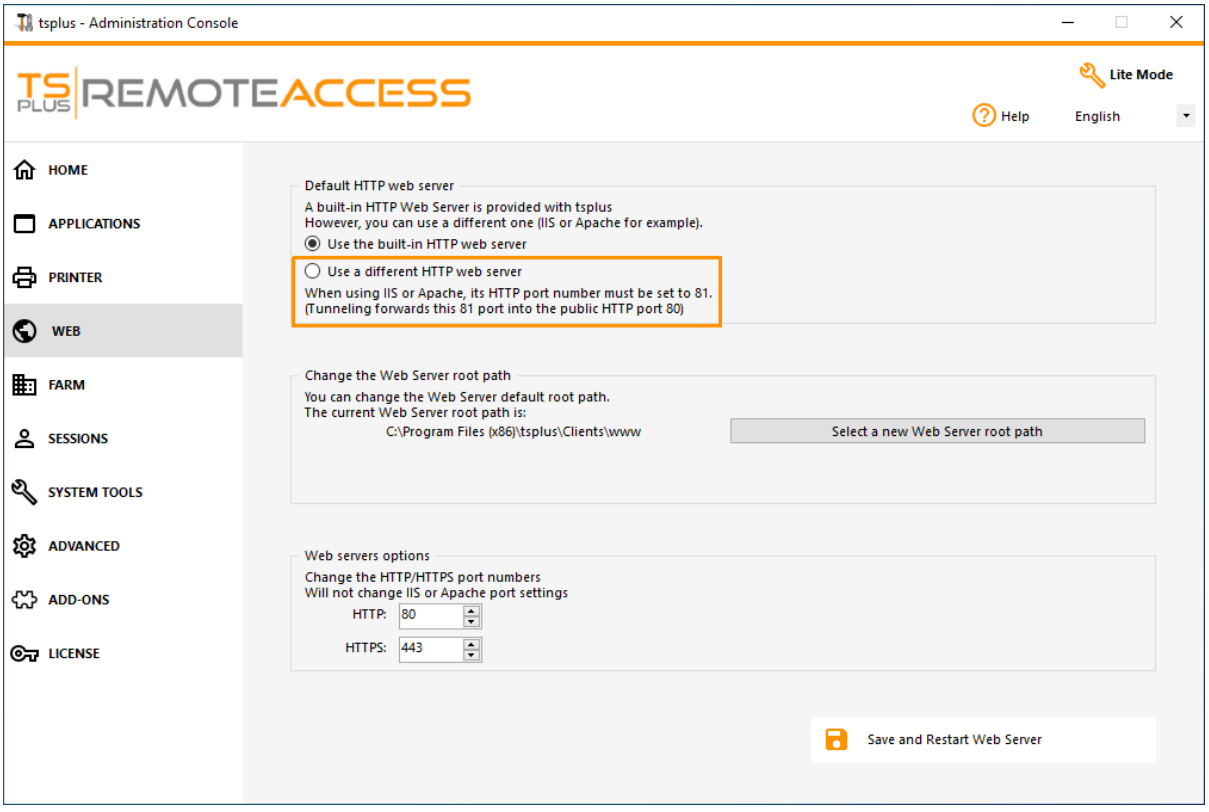
Cómo usar Apache en lugar del servidor web predeterminado de Terminal Service Plus

Requisitos previos

Puede ser una buena idea que Actualizar Terminal Service Plus para asegurarte de que obtienes los últimos programas de TSplus.

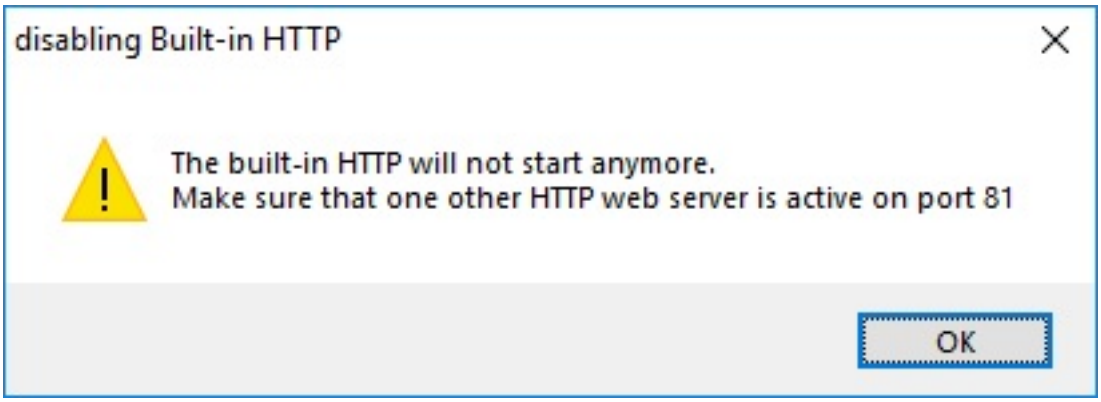
1. Inicie AdminTool y vaya a la pestaña del servidor web

Haga clic en el mosaico Administrar servidores web, verifique **Utilice un servidor web HTTP diferente** porque quieres usar Apache.



Luego, utiliza el botón **Seleccione una nueva ruta raíz del servidor web** para indicar a TSplus dónde estará la nueva raíz de la carpeta web.

TSplus copiará los archivos/carpetas solicitados en esta nueva carpeta raíz y, en este punto, la configuración de TSplus para Apache está casi completa. Un mensaje emergente te recomendará cambiar el puerto HTTP de Apache a 81.



Ahora es el momento de configurar Apache.

2. Configurando Apache

Cambia el HTTP de 80 a 81.

La forma específica de hacer esto depende de tu versión de Apache y de la configuración actual de Apache.

Le aconsejamos que haga una copia de seguridad de cualquier archivo de configuración de Apache antes de modificarlos, para que tenga una forma de restaurarlos si es necesario.

Normalmente, puedes cambiar el puerto de escucha de Apache editando el archivo httpd.conf que se encuentra en el directorio “Apache\conf”:

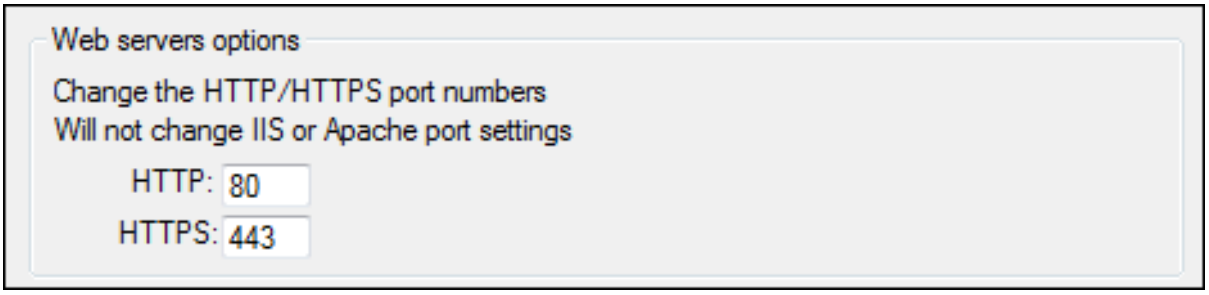
Escuchar 81

Una vez que se haya hecho, reinicie el servicio de Apache.

3. Volviendo a la herramienta de gestión de servidores web de TSplus

Puedes configurar los puertos HTTP y HTTPS en la herramienta de gestión web de TSplus. Recomendamos usar puertos estándar, pero esta función puede ser útil al intentar evitar un

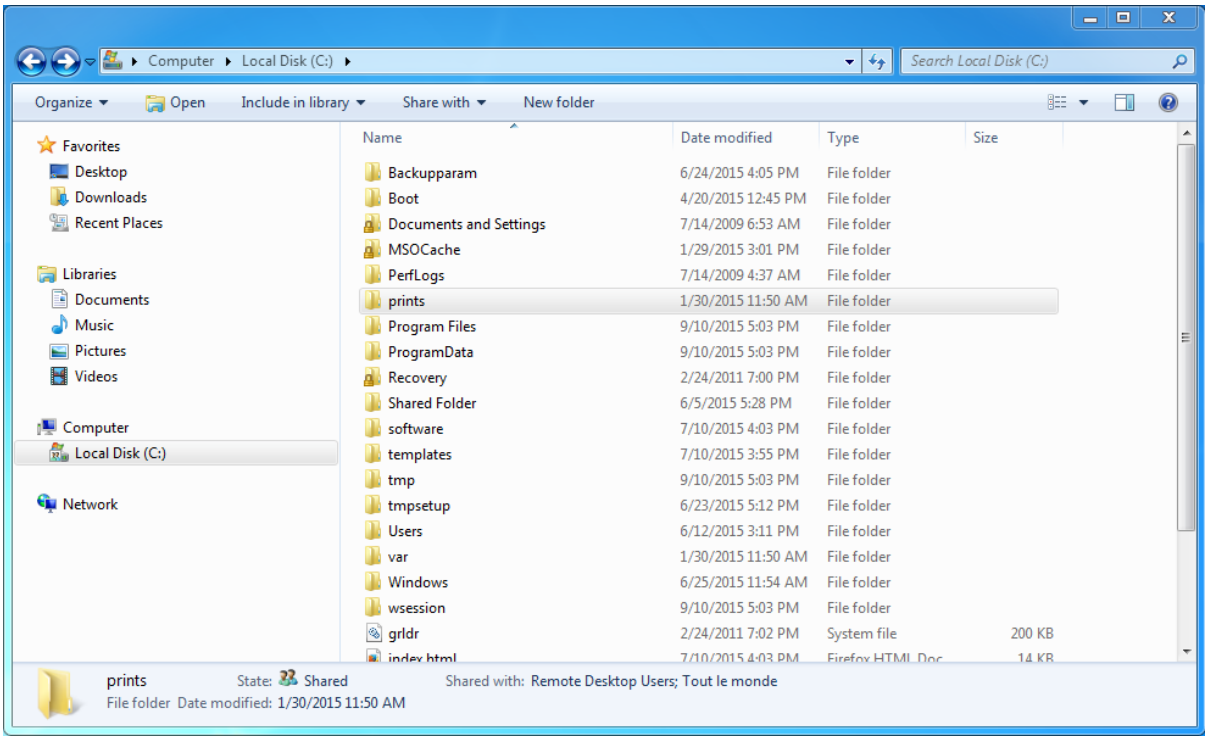
conflicto con otro proceso.

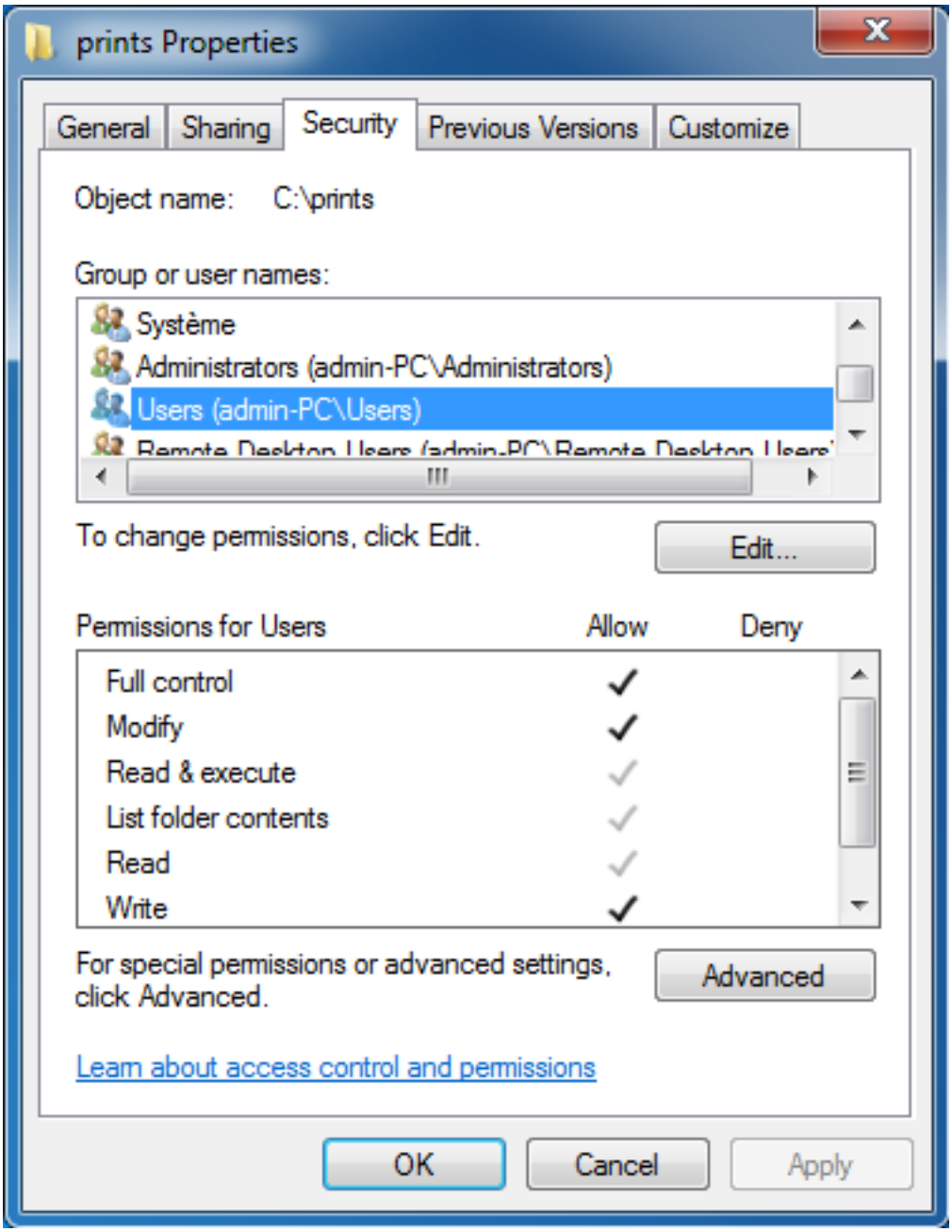


4. Últimos pasos

Para la Impresora Universal, necesitamos poder escribir en la carpeta PRINTS.

Así que verifica que Todos/Usuarios… tengan plenos derechos en la carpeta …/prints.





Luego selecciona el archivo .html que deseas usar como página de Acceso Web en:

C:\Program Files (x86)\TSplus\Clients\www

y cópialo como index.html en la carpeta raíz de tu web, típicamente este es el directorio “Apache\htdocs”.

5. Configuración específica para TSplus Gateway Portal, balanceo de carga y/o transferencia de archivos HTML5

Si desea utilizar este sistema basado en Apache como un TSplus Gateway Portal y/o utilizar la

función de balanceo de carga de TSplus Gateway Portal y/o utilizar la función de transferencia de archivos HTML5, deberá permitir la ejecución de scripts GCI de TSplus por Apache.

Primero, debes tener habilitado el módulo CGI en Apache.

Edita el archivo httpd.conf que se encuentra en el directorio “Apache\conf” y busca una línea que se parezca a:

;LoadModule cgi_module modules/mod_cgi.so

Remove the ”;” para habilitar el módulo CGI:

LoadModule cgi_module modules/mod_cgi.so

Luego, encuentra una línea que comience con:

Agregar controlador cgi-script

Y agregue la extensión .exe para autorizar que los archivos .exe sean tratados como programas CGI por Apache:

AddHandler cgi-script .exe

Finalmente, debes decirle a Apache que la carpeta “cgi-bin” de TSplus contiene programas CGI. Para hacerlo, debes agregar la siguiente línea en el archivo httpd.conf que se encuentra en el directorio “Apache\conf”:

ScriptAlias /cgi-bin/ “C:/Program Files (x86)/TSplus/Clients/www/cgi-bin/”

Una vez que se haya hecho, reinicie el servicio de Apache.

Si tiene algún problema al configurar CGI en su servidor Apache, consulte la Documentación oficial de Apache

Verificando su configuración: Para validar su configuración, abra un navegador web en su servidor y vaya a http://localhost/cgi-bin/hb.exe Si recibe una página de error de Apache, tiene un problema en su configuración de Apache. Si recibe una línea de texto/números, todo está bien.

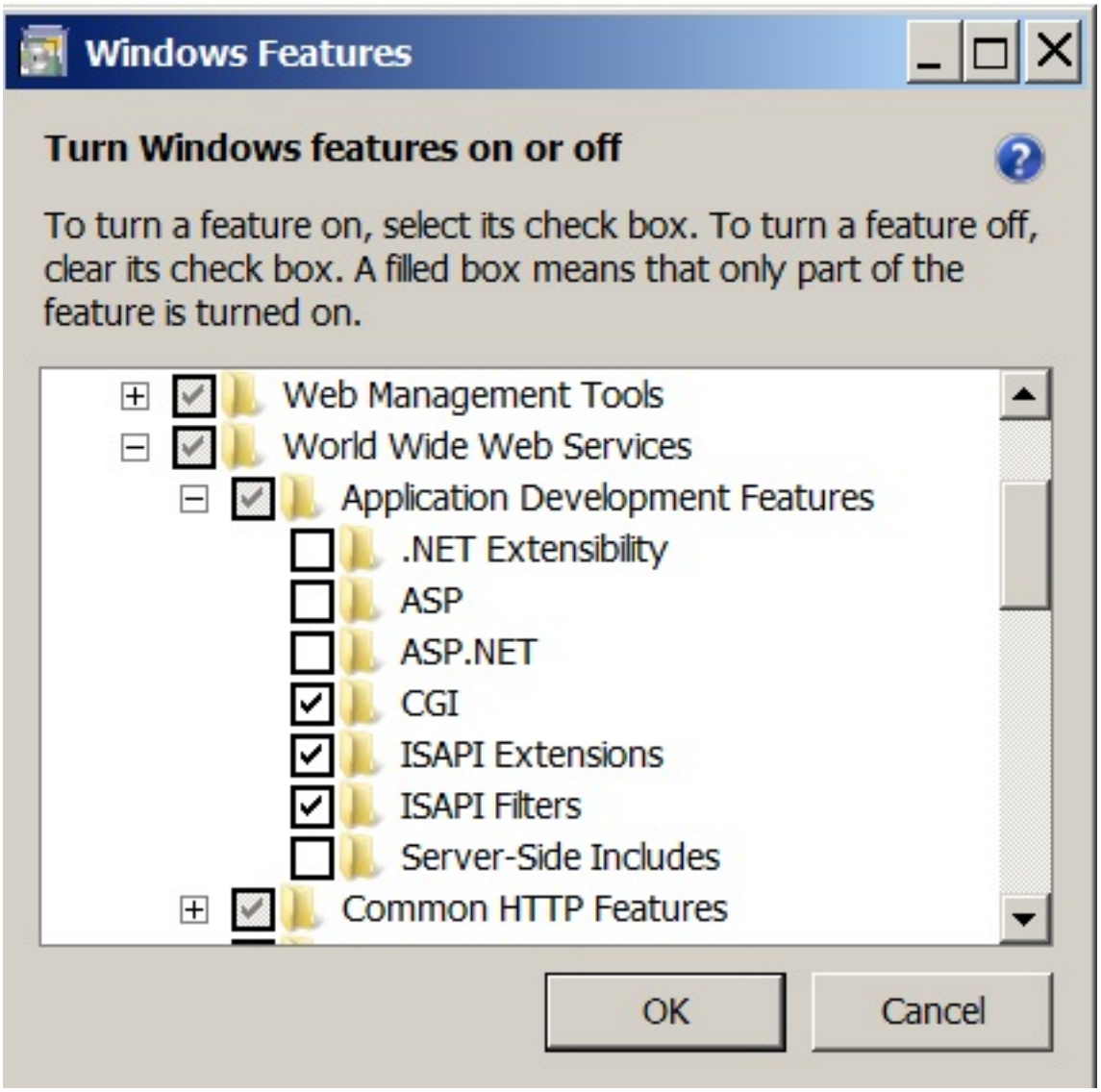
Cómo usar IIS en lugar de los servidores web predeterminados de Terminal Service Plus

Requisitos previos

Puede ser una buena idea que Actualizar Terminal Service Plus para asegurarte de que obtienes los últimos programas de TSplus.

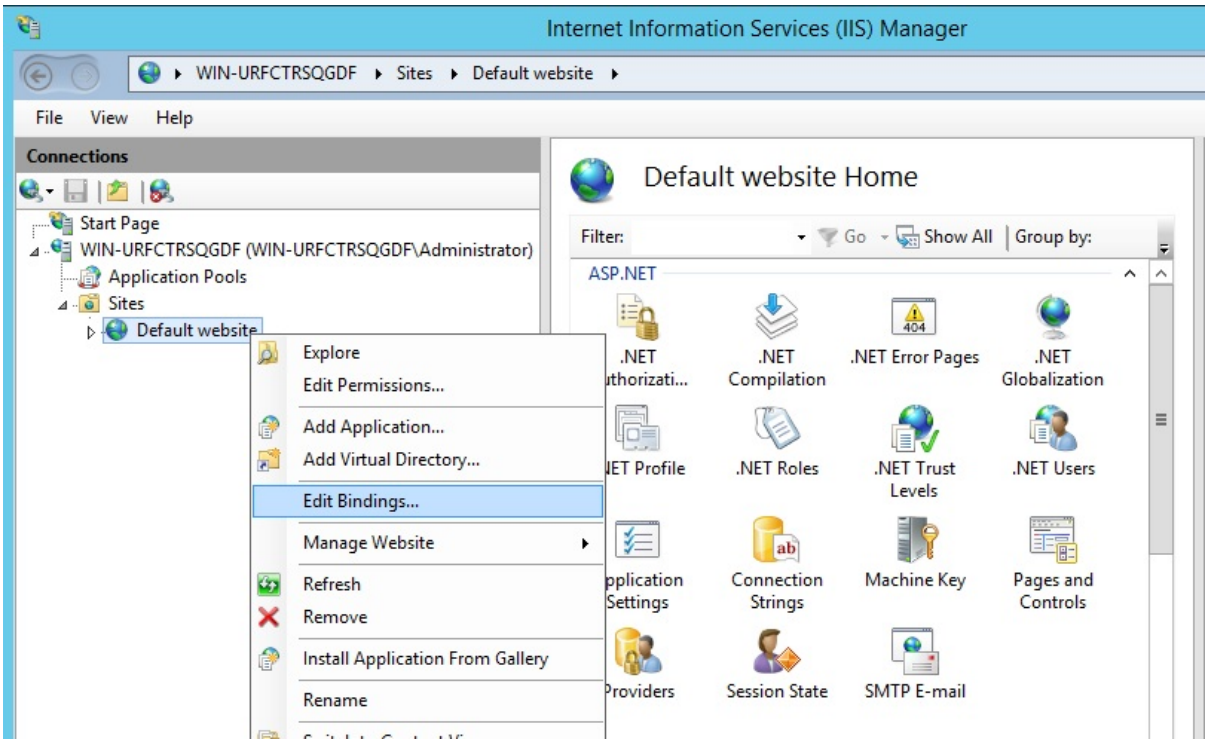
1. Configuración de IIS

- Instalar IIS con los siguientes módulos: CGI, extensiones ISAPI y filtros ISAPI.

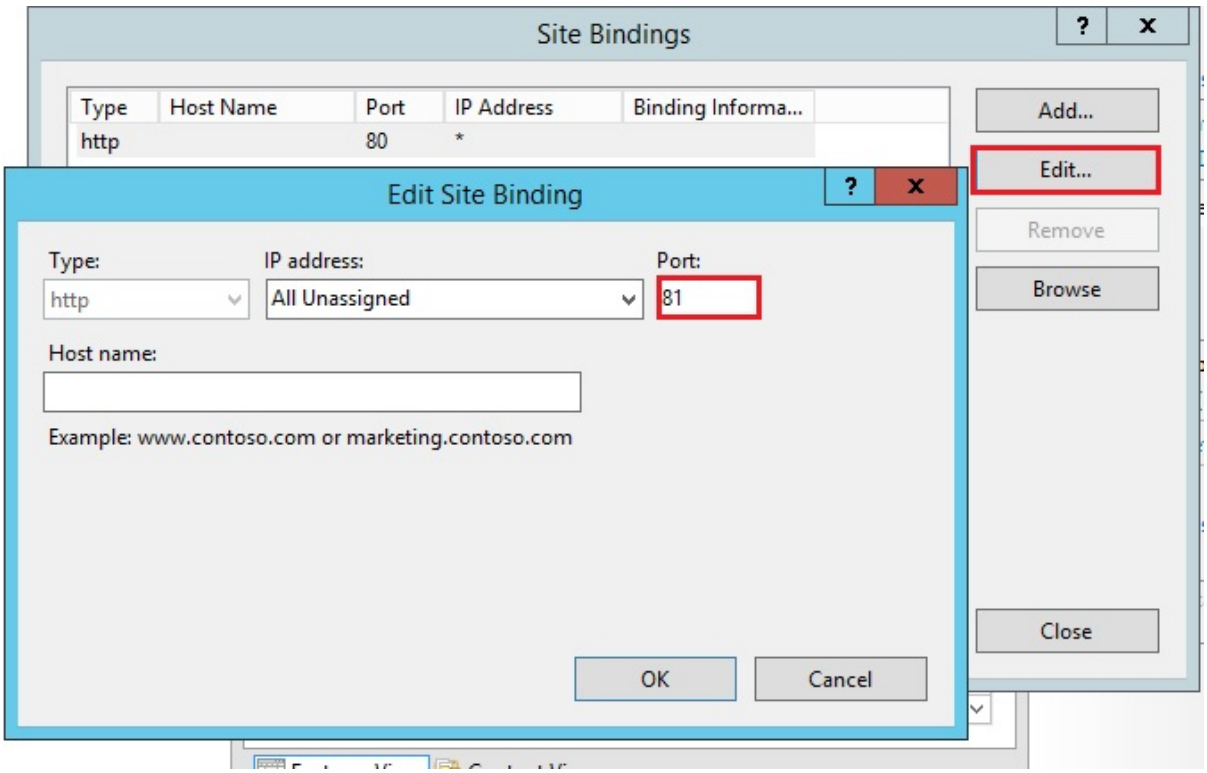


- Configurando el puerto de IIS:

Acceda a la consola de administración de IIS, expanda la lista debajo del nombre de su servidor, luego expanda el menú "Sitios" y haga clic derecho en "Sitio Web Predeterminado" y haga clic en "Editar enlaces".



Haz clic en “http” y “Editar”. Cambia el puerto a 81 y haz clic en Aceptar, y luego haz clic en Cerrar:



Desactive el puerto 443 o cambie este puerto por otro puerto libre.

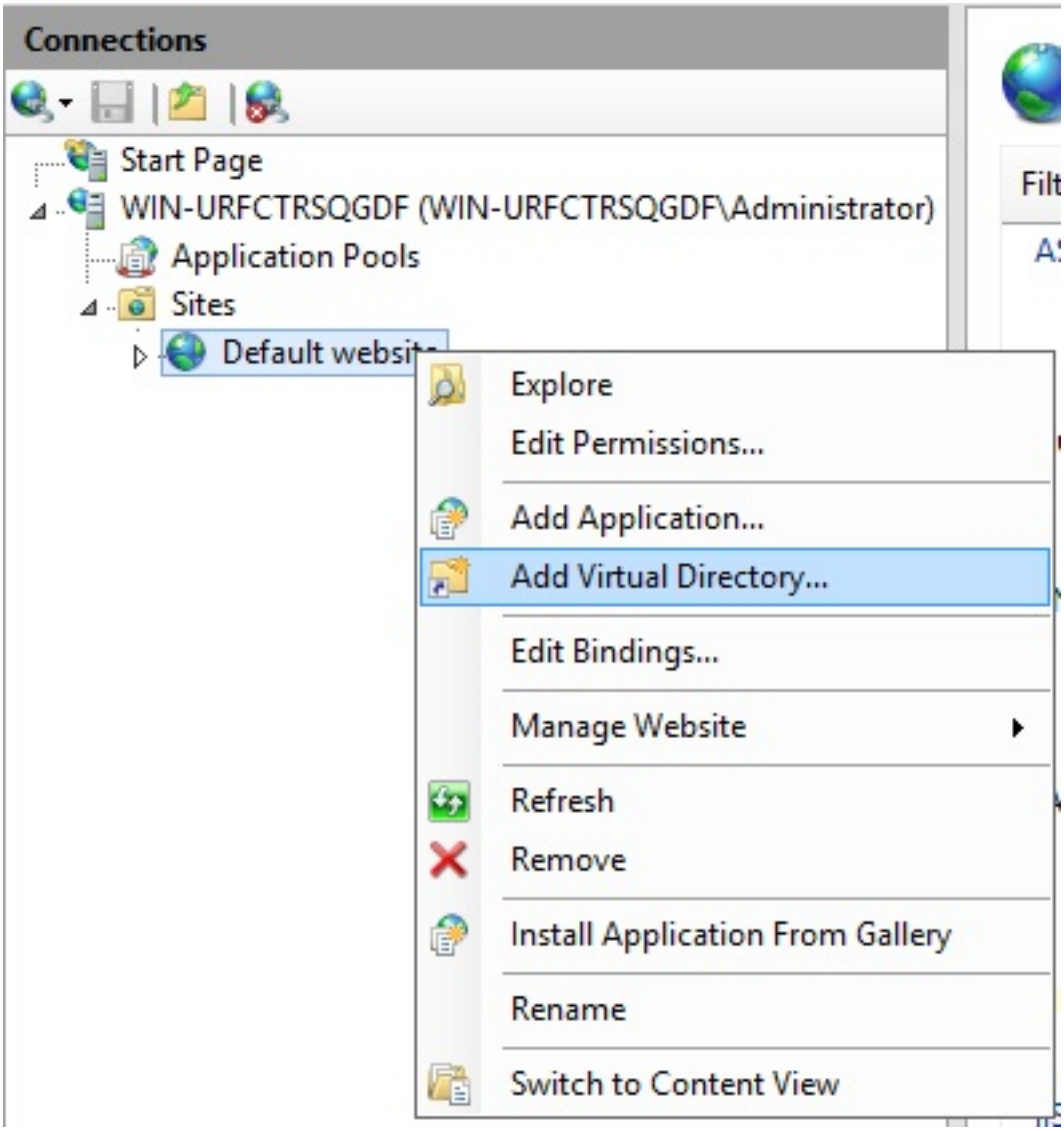
Luego, reinicie el Administrador de IIS.

2. Crear directorio virtual para CGI

NB: Todos los archivos de la raíz web predeterminada (C:\Program Files (x86)\TSplus\Clients\www) no se copian cuando se modifica el directorio de la raíz web.

Deberá verificarlos y copiarlos manualmente al migrar al servidor web IIS.

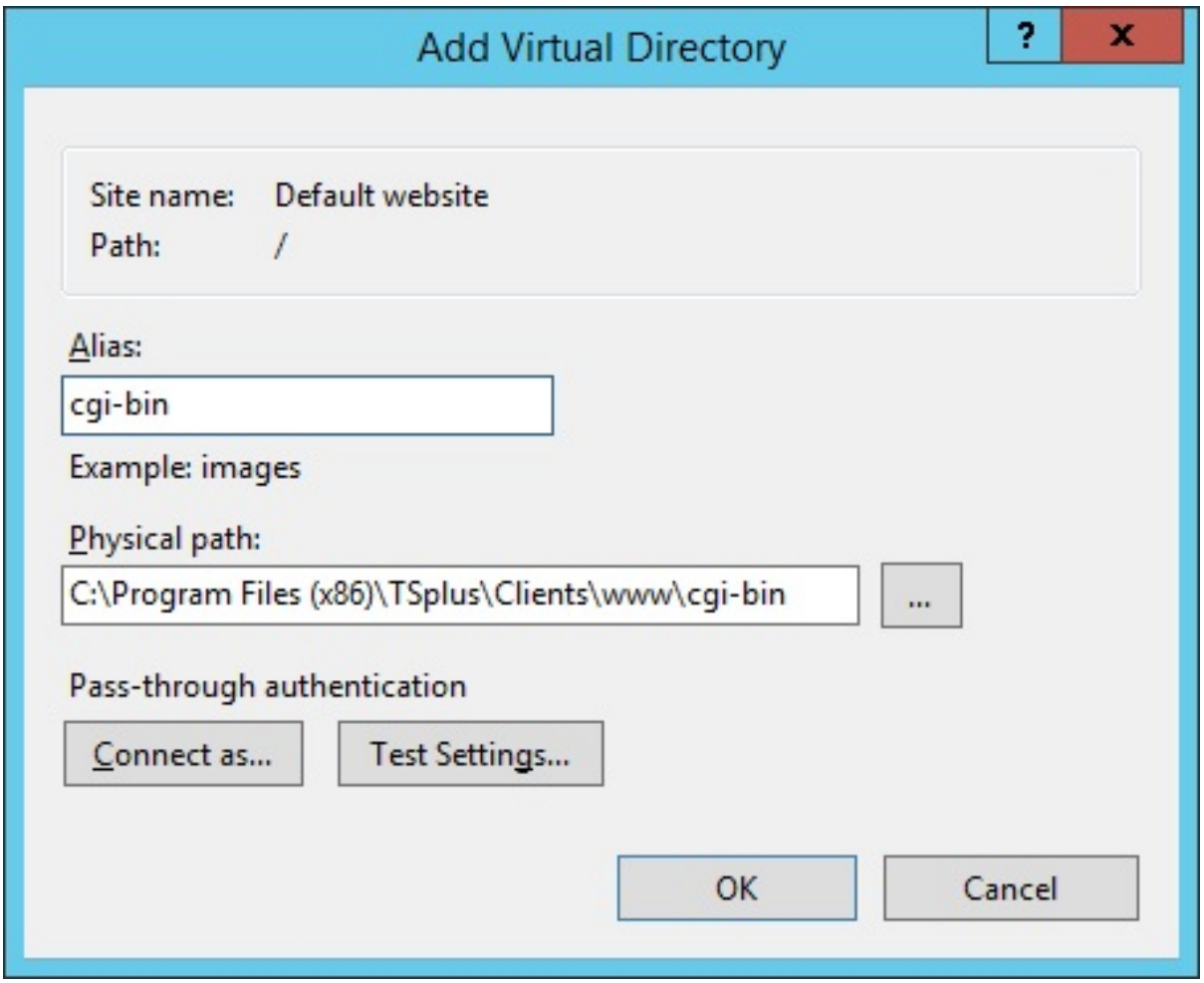
En el menú del panel izquierdo, expanda el menú bajo su servidor, luego "Sitios", y haga clic derecho en su sitio para agregar un nuevo "directorio virtual", como se muestra en la imagen a continuación:



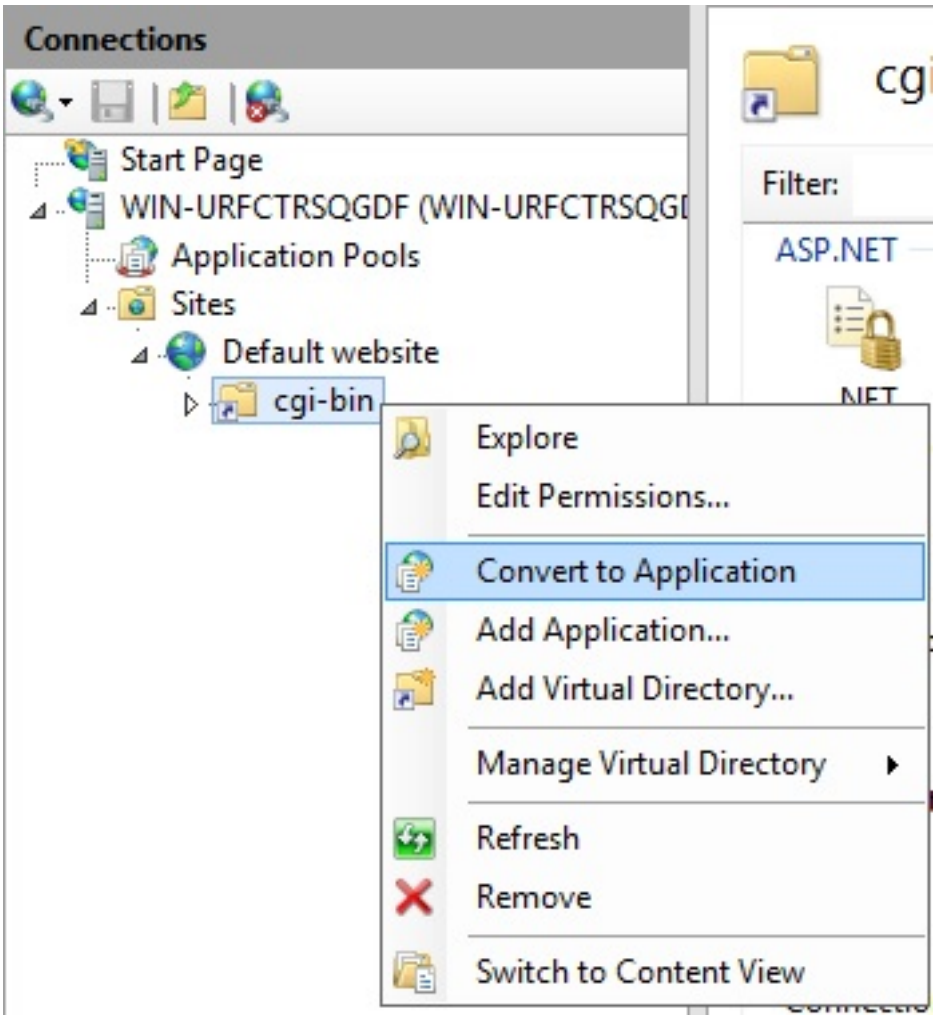
En la ventana que se abrirá, complete de la siguiente manera:

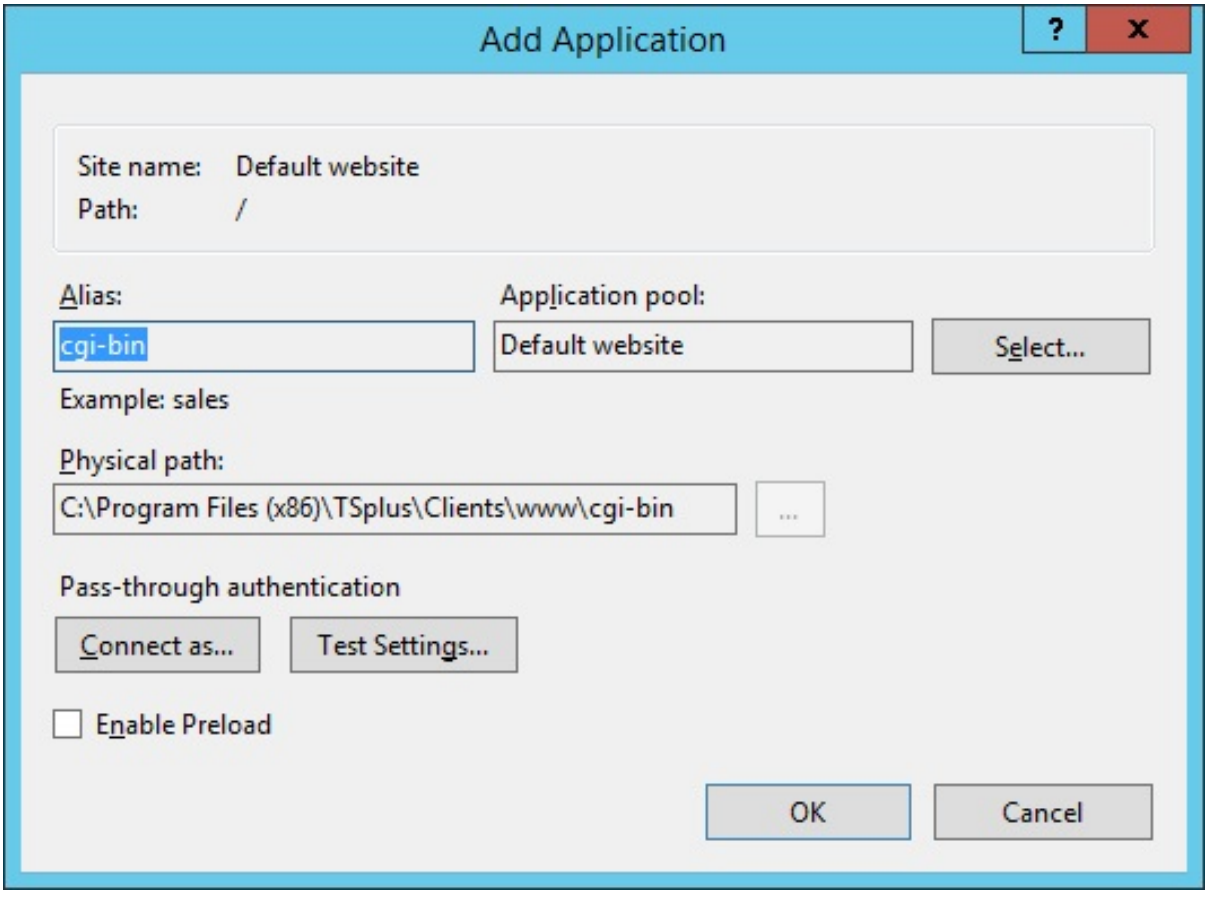
Alias: cgi-bin

Ruta física: C:\Program Files(x86)\TSplus\Clients\www\cgi-bin

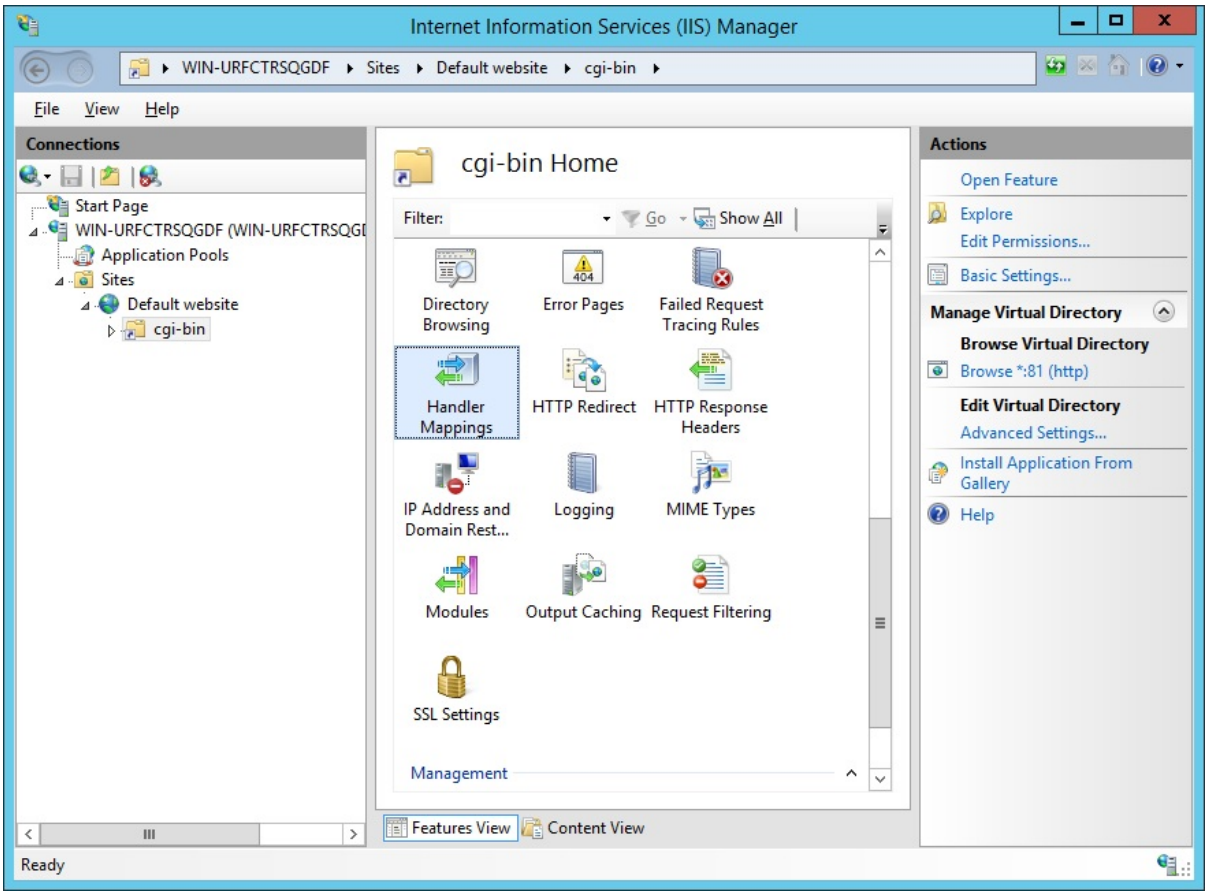


Luego haga clic en "Aceptar" y verá que el directorio virtual "cgi-bin" se ha agregado a su sitio web de IIS. Ahora, haga clic derecho en este directorio virtual "cgi-bin" y haga clic en "Convertir a aplicación". Haga clic en "Aceptar" y acepte la configuración predeterminada.


Connections
Start Page
WIN-URFCTRSQGDF (WIN-URFCTRSQGD
Application Pools
Sites
Default website
cgi-bin
Filter:
ASP.NET
Explore
Edit Permissions...
Convert to Application
Add Application...
Add Virtual Directory...
Manage Virtual Directory
Refresh
Remove
Switch to Content View

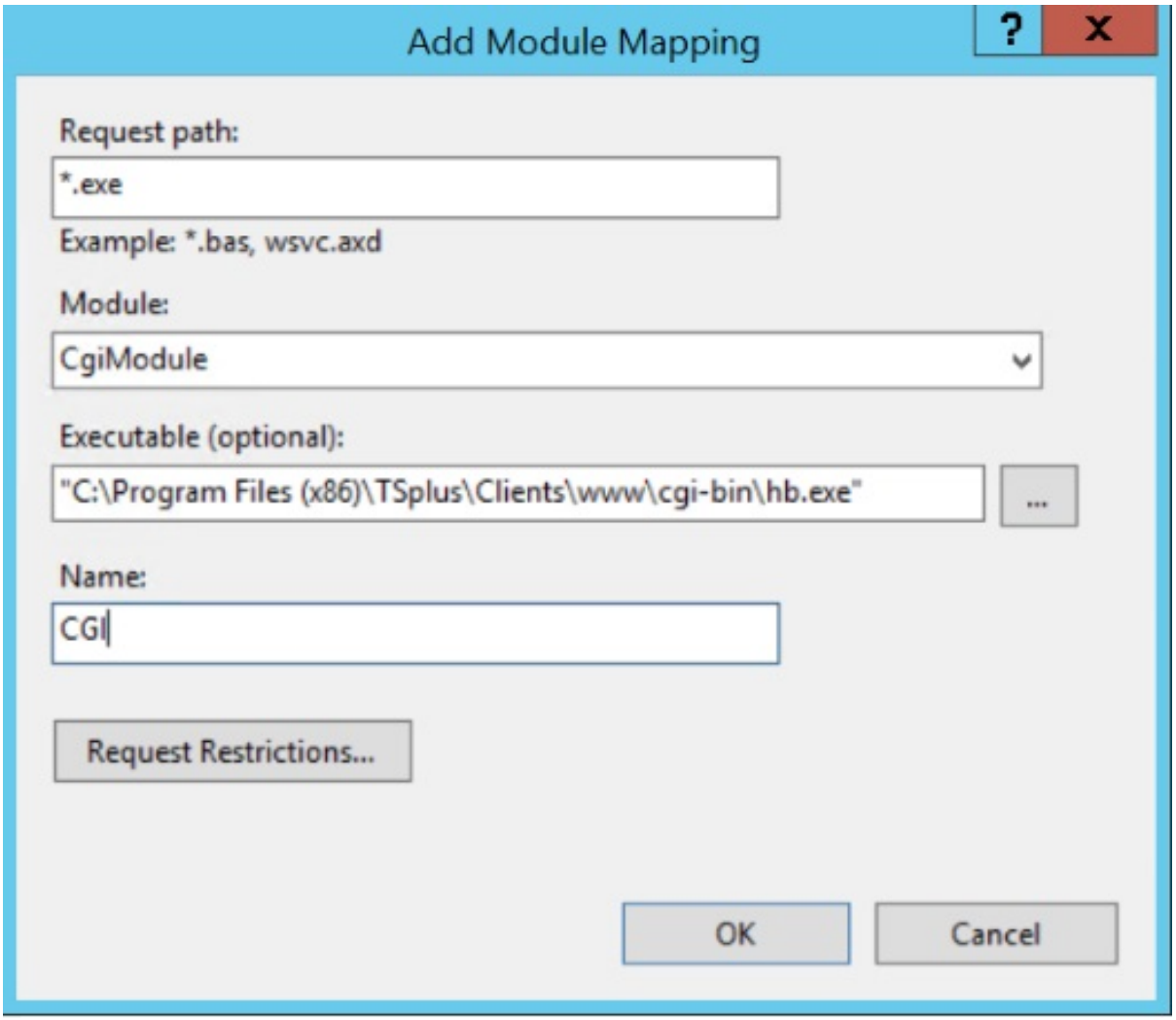

Add Application
Site name: Default website
Path: /
Alias:
cgi-bin
Example: sales
Application pool:
Default website
Select...
Physical path:
C:\Program Files (x86)\TSplus\Clients\www\cgi-bin
...
Pass-through authentication
Connect as...
Test Settings...
Enable Preload
OK
Cancel

Luego selecciona el icono "Asignaciones de controladores" para esta carpeta en el lado derecho de la ventana del Administrador:

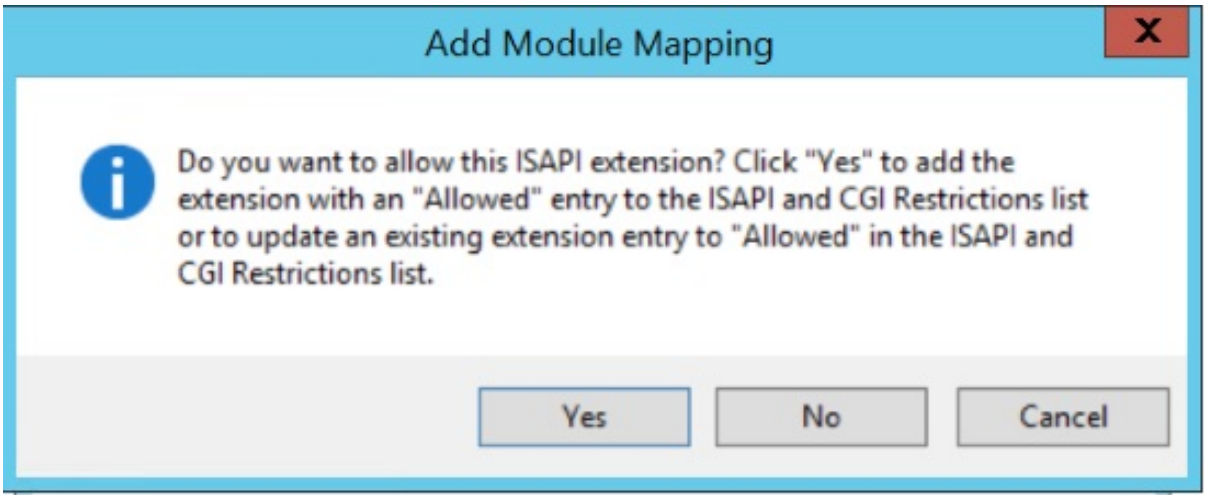


Desde la lista de Mapeos de Controladores, haz doble clic en “CGI-exe”.

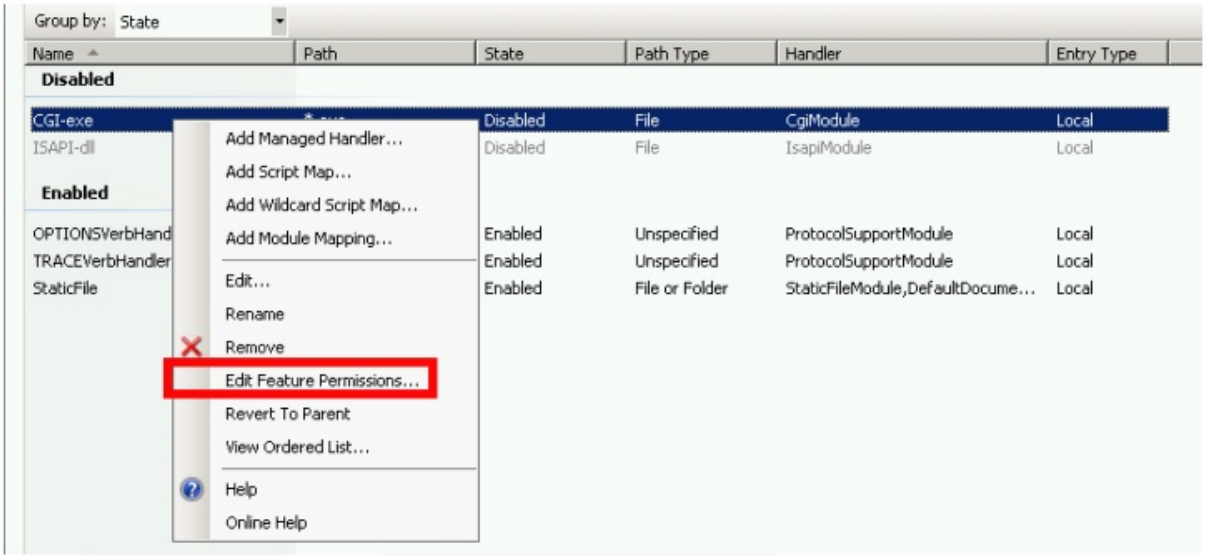
Luego, busca el ejecutable hb.exe en el cuadro de propiedades Ejecutable y haz clic en Aceptar.



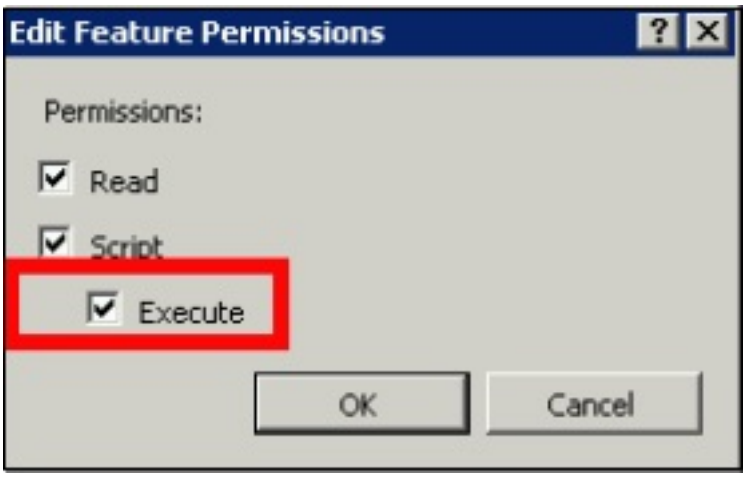
Aparece un aviso de confirmación. Haga clic en "Aceptar" para permitir esta extensión ISAPI.



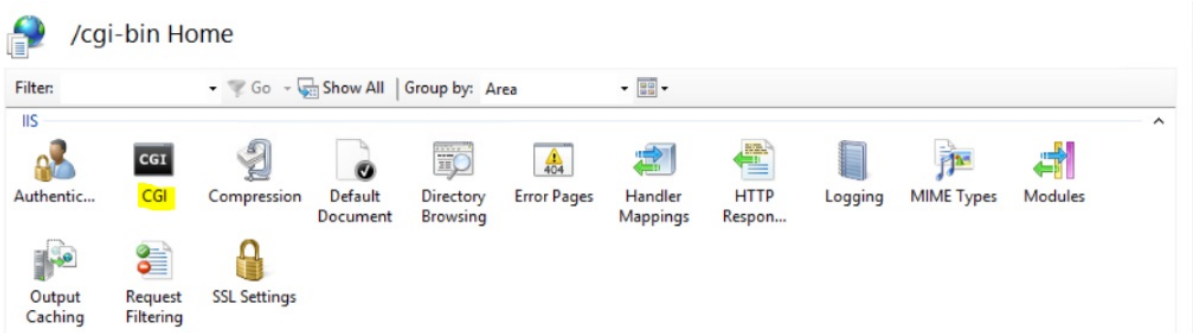
Ahora haga clic en "Editar permisos de características":



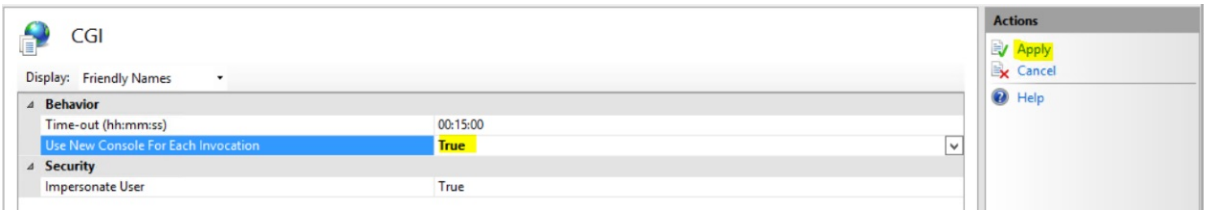
Marque la casilla "Ejecutar" y haga clic en Aceptar:



Volver a la página de inicio de “CGI-bin”, haga clic en “CGI” para abrir las propiedades de CGI:



Cambia el valor de "Usar nueva consola para cada invocación" a "Verdadero". Luego, haz clic en "Aplicar" para guardar los cambios.

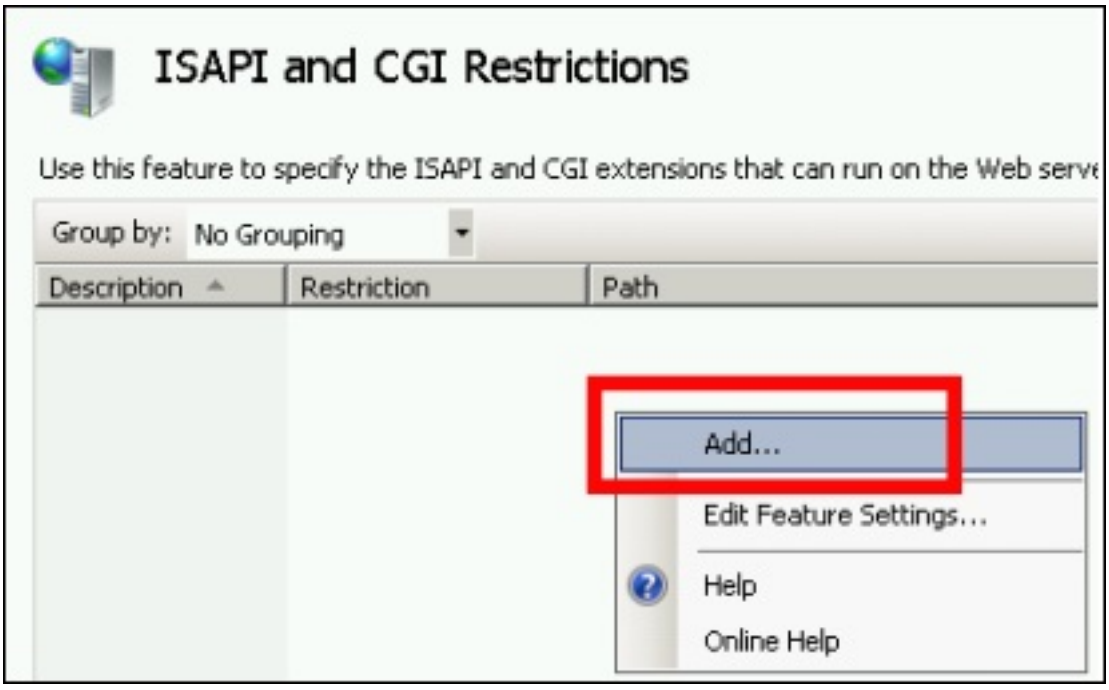


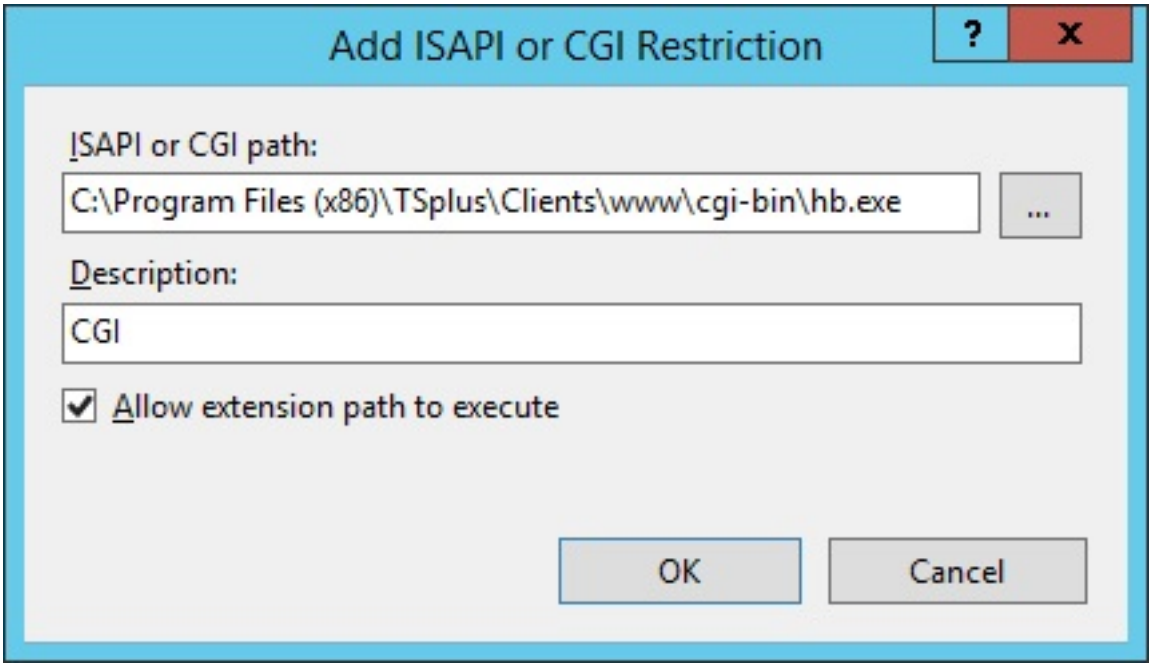
3. Configurar permiso de extensión CGI

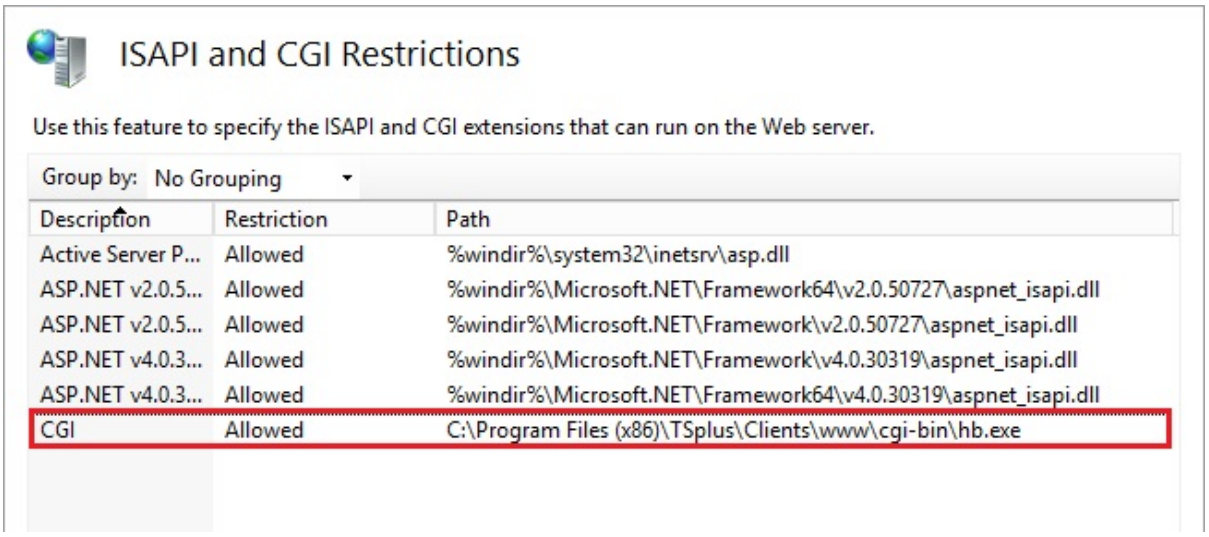
Ahora, el último paso es permitir que la extensión CGI se ejecute en el servidor. Haga clic en el icono de "Restricciones de ISAPI y CGI". Esto se puede encontrar haciendo clic en el nombre de la máquina en el menú del lado izquierdo de la ventana.



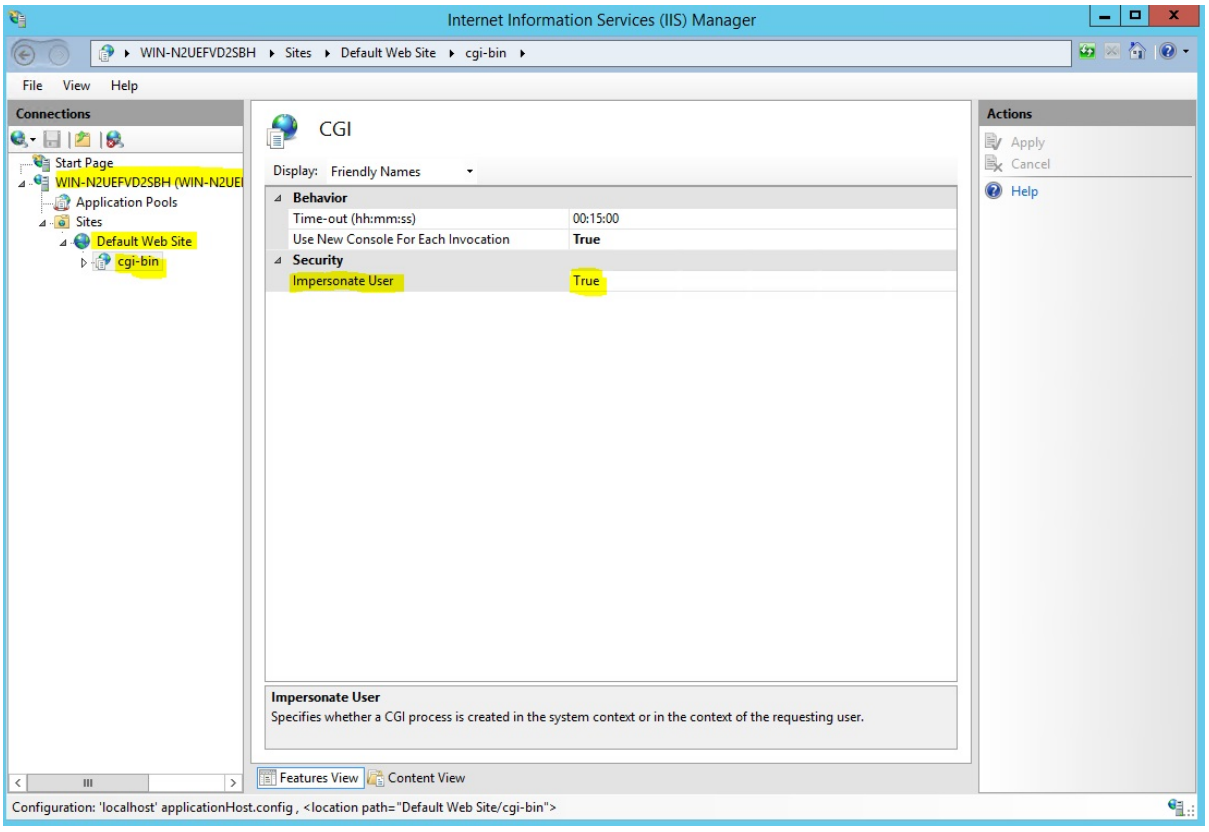
En la página de "Restricciones de ISAPI y CGI", haga clic en "Agregar ..." en el lado derecho de la ventana. Ahora especifique la ruta completa al archivo "hb.exe" alojado en la carpeta de TSplus. Asegúrese de marcar la opción "Permitir que la ruta de la extensión se ejecute", ya que Ilustre las siguientes imágenes:


ISAPI and CGI Restrictions
Use this feature to specify the ISAPI and CGI extensions that can run on the Web serve
Group by: No Grouping
Description
Restriction
Path
Add...
Edit Feature Settings...
Help
Online Help


Add ISAPI or CGI Restriction
?
X
ISAPI or CGI path:
C:\Program Files (x86)\TSplus\Clients\www\cgi-bin\hb.exe
...
Description:
CGI
Allow extension path to execute
OK
Cancel



Asegúrese de que en la sección CGI de su servidor, "Default Web Site" y "cgi-bin", la configuración "Impersonate User" esté establecida en "True".



- Otorgar permisos completos al usuario "IUSR" en el directorio C:\Program Files (x86)\TSplus\Clients\www\cgi-bin

- Por favor, asegúrese de habilitar la herencia de permisos cuando el usuario IUSR esté configurado para tener control total sobre el directorio. C:\Program Files (x86)\TSplus\Clients\www\cgi-bin

- Otorgar permisos completos al usuario "IUSR" en el directorio C:\Program Files (x86)\TSplus\Clients\webserver\twofa

4. Agregar tipos de Mime en IIS

Abre un símbolo del sistema como administrador y ejecuta los siguientes comandos:

Ventana de terminal

```
%SystemRoot%\system32\inetsrv\appcmd set config /section:staticContent
/+[fileExtension='.dat',mimeType='text/plain']
```

Ventana de terminal

```
%SystemRoot%\system32\inetsrv\appcmd set config /section:staticContent
/+[fileExtension='.',mimeType='text/plain']
```

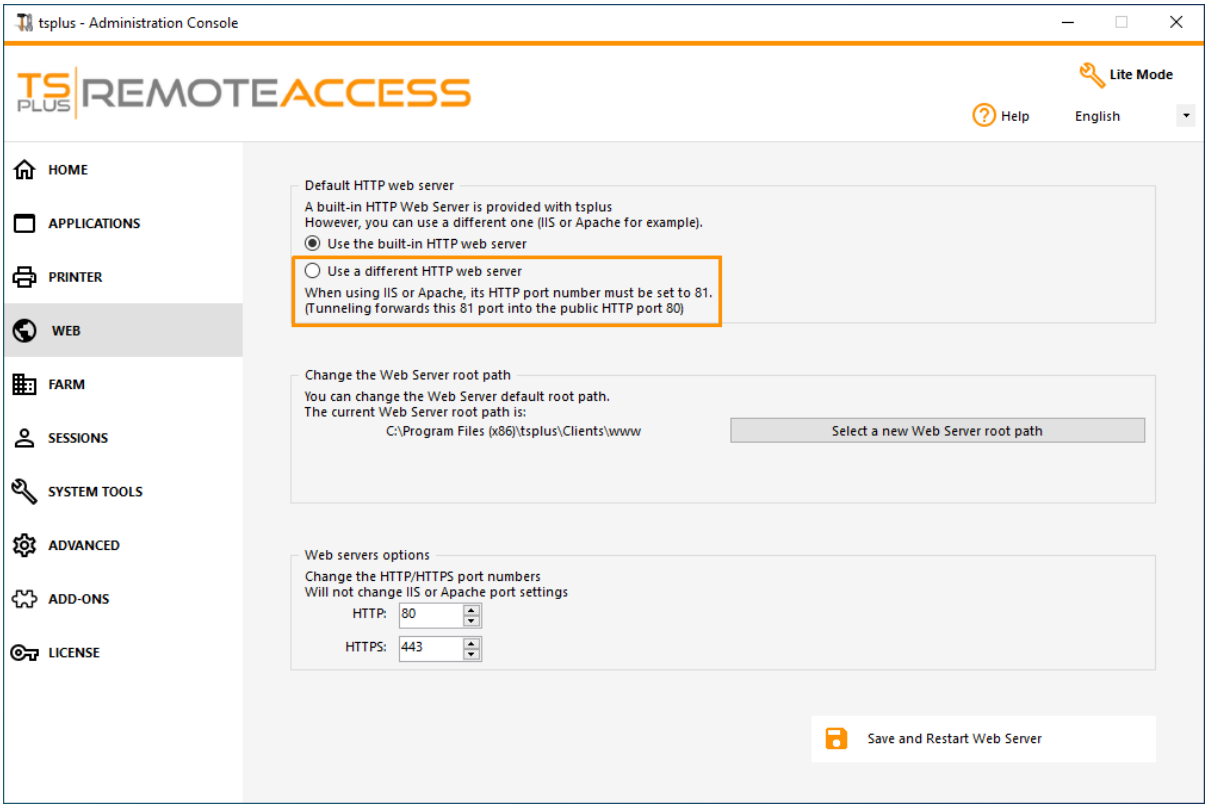
Reiniciar IIS.

5. Configurar permisos de directorio de IIS

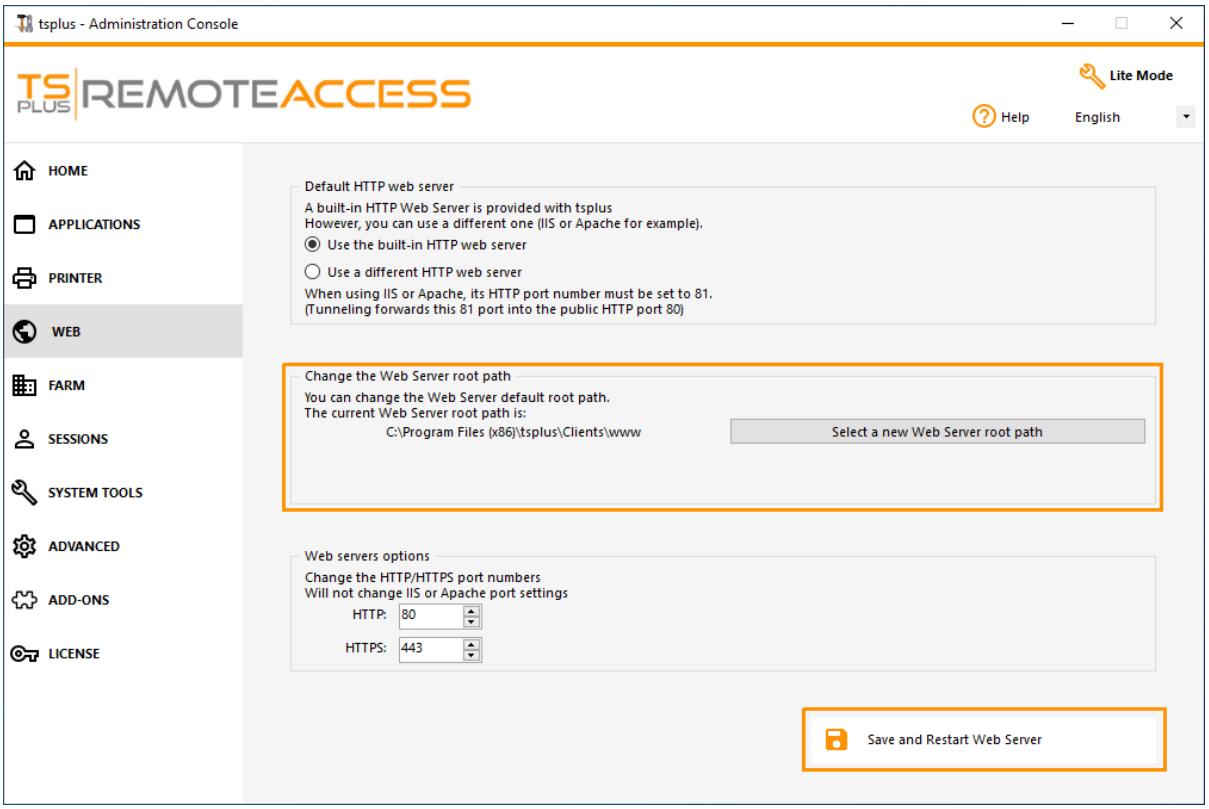
Otorgar permisos completos al grupo "Everyone" en el directorio "C:\inetpub\wwwroot"

6. Configurar TSplus

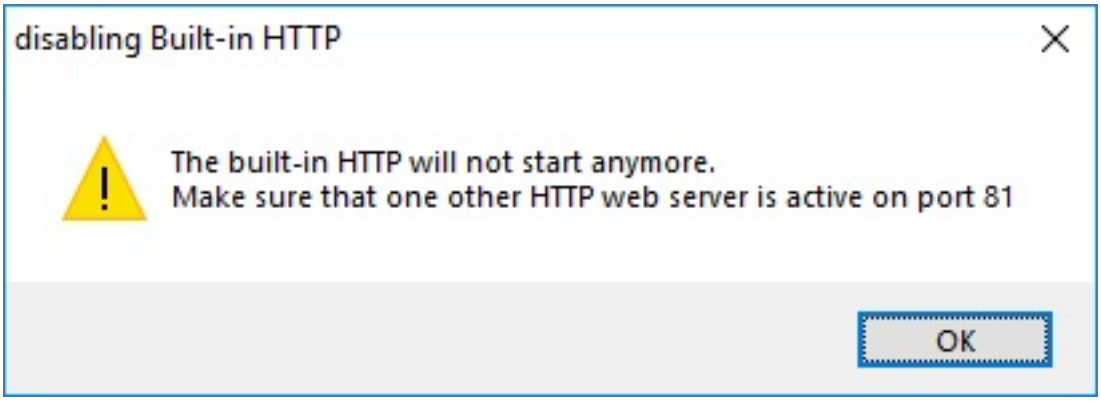
Ve a la pestaña del Servidor Web de AdminTool, luego elige la opción “Usar un servidor HTTP diferente”:

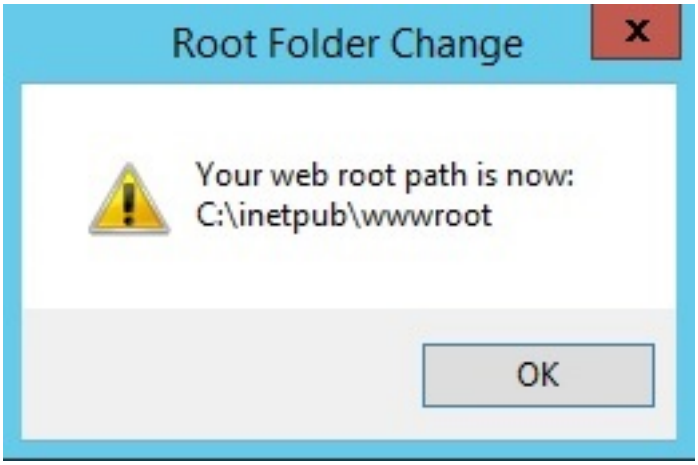


Luego, en la misma ventana, haz clic en “Seleccionar una nueva ruta raíz del servidor web” y coloca la ruta del directorio de IIS, que debería ser algo como: “C: \ inetpub \ wwwroot”. Ahora haz clic en “Guardar y reiniciar el AdminTool”.



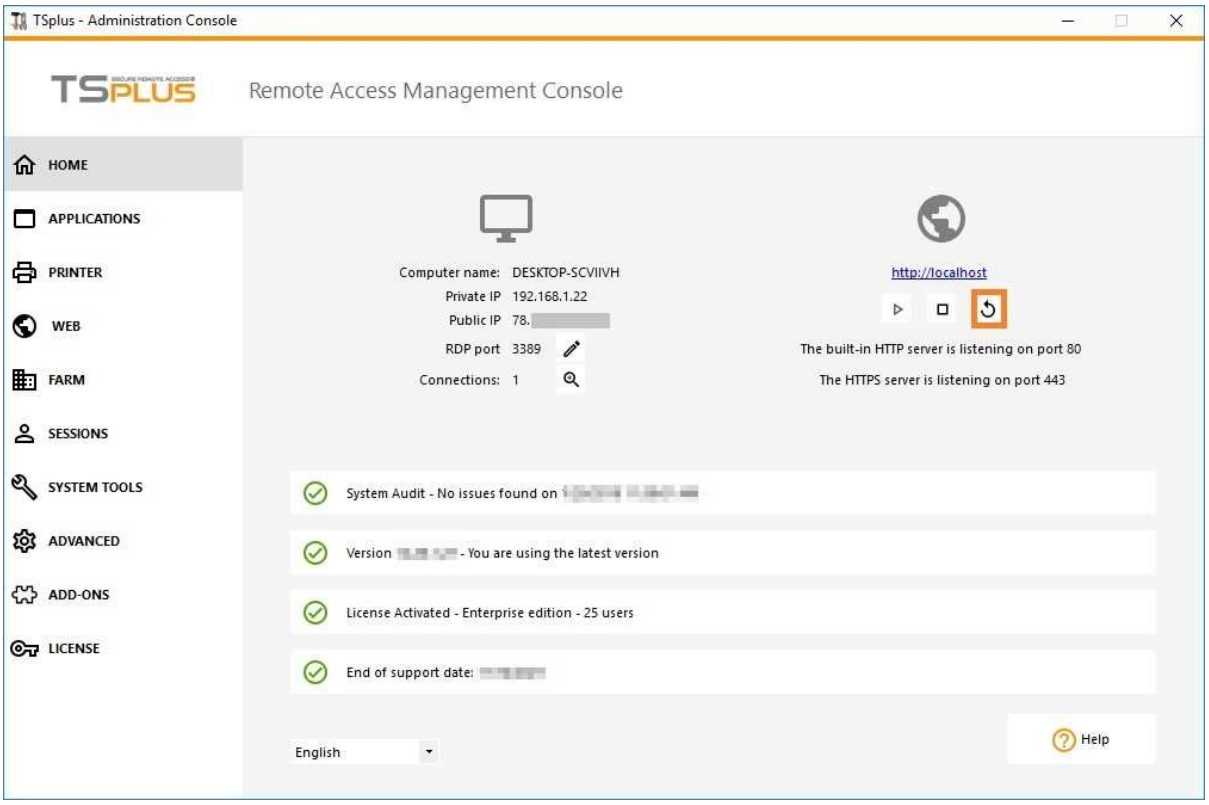
Los siguientes mensajes aparecerán:





Espera. La herramienta de administración se cerrará automáticamente. Luego abre la herramienta de administración nuevamente y haz clic en el mosaico de la web.

Finalmente, reinicie los servidores web:



7. Prueba con el host local

Advertencia Utilice una cuenta de usuario diferente.

Si intentas con tu cuenta de usuario actual desde tu propia sesión RDP al servidor, serás desconectado y no podrás reconectarte.



Acciones adicionales:

Configurar RemoteApp

La carpeta “remoteapp” en la raíz web de IIS (c:\inetpub\www\cgi-bin\remoteapp) también debe tener permisos completos para el usuario IUSR, de lo contrario, aparecerá un error 704 al intentar usar RemoteApp.

Configurar 2FA

En una instalación nueva donde 2FA nunca ha sido habilitado, no hay ninguna carpeta llamada C:\Program Files (x86)\TSplus\Clients\webserver\twofa, o el archivo twofactorauth.ini.

Es necesario:

- activa 2FA en AdminTool para crear esta carpeta y este archivo .ini
- entonces desactive 2FA
- entonces aplique los permisos de usuario IUSR a la nueva carpeta twofa.

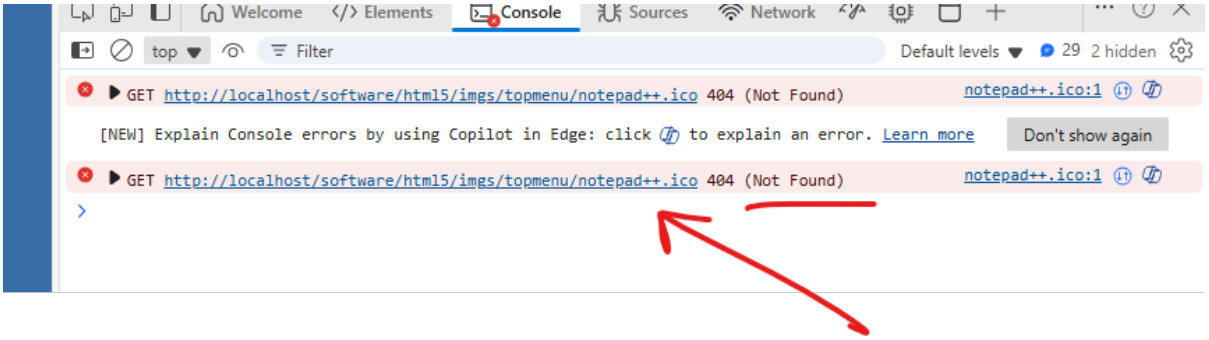
El no completar este paso (incluso si no tienes la intención de usar 2FA) impedirá que los usuarios inicien sesión con un mensaje de error que indica que las credenciales son inválidas.

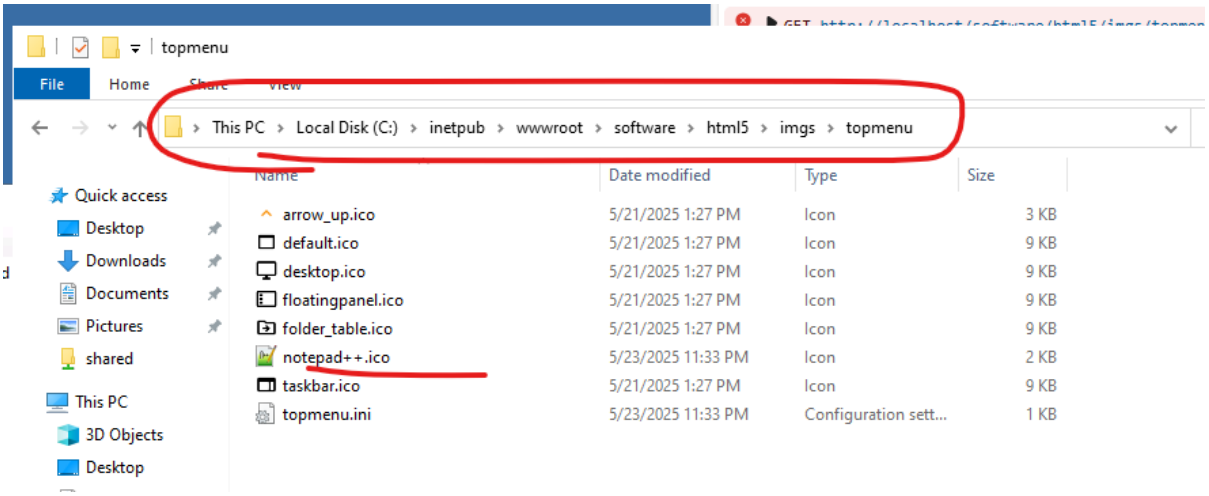
8. Permitir doble escape

Para permitir descargas, necesita habilitar "Permitir doble escape" en el filtrado de solicitudes dentro de IIS. Este cambio permitirá que IIS maneje correctamente caracteres especiales como "+" en los nombres de archivo. Aquí le mostramos cómo habilitar "Permitir doble escape" en IIS:

1. Abrir el Administrador de IIS: Inicie el Administrador de Servicios de Información de Internet (IIS).

2. Navegue a Filtrado de Solicitudes: En el Administrador de IIS, seleccione la carpeta o el sitio web que contiene el archivo con el carácter “+”. Luego, haga doble clic en “Filtrado de Solicitudes” en la Vista de Características.

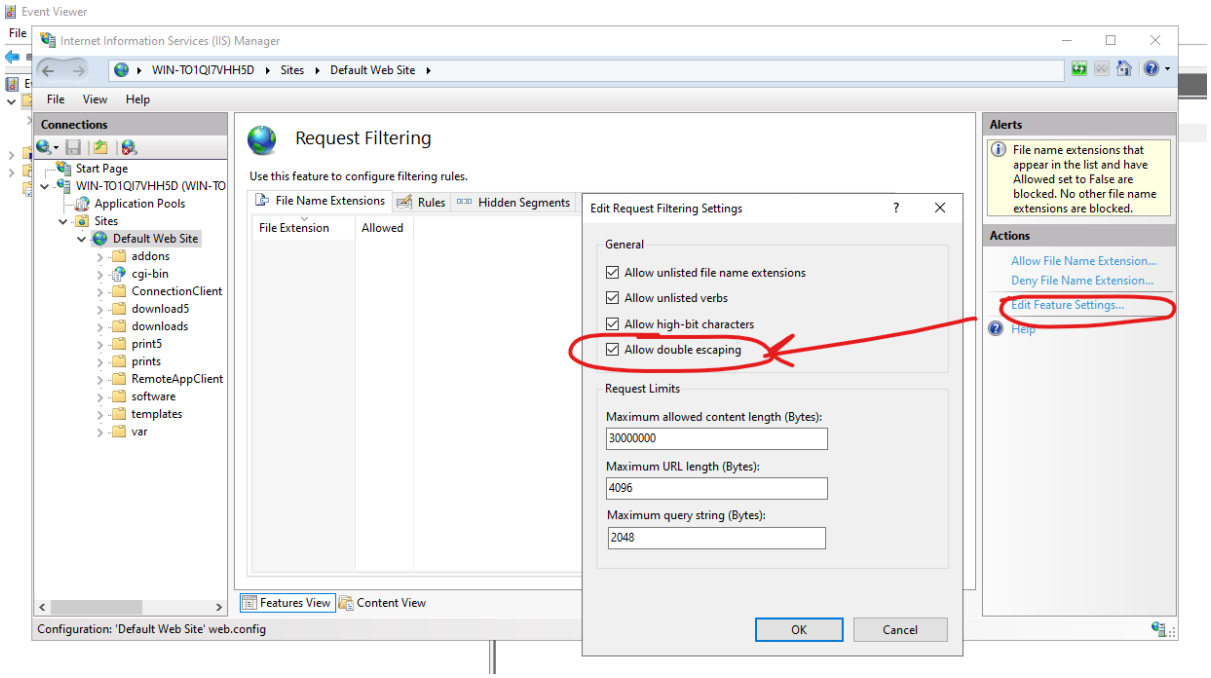




3. Editar la configuración de funciones: En el panel de acciones, haga clic en "Editar configuración de funciones".

4.

Habilitar permitir doble escape: En el cuadro de diálogo Editar configuración de filtrado de solicitudes, marque la casilla "Permitir doble escape".



5. Reiniciar IIS (opcional): Reiniciar IIS puede ayudar a asegurar que los cambios surtan efecto.

Usando servidores detrás de un Proxy Inverso

Es posible utilizar servidores detrás de proxies inversos a través de xhr-polling, con algunas limitaciones.

Como se describe Websockets no son parte del protocolo HTTP, aunque la primera solicitud http se parezca a una solicitud http, en realidad no lo es, por lo tanto, la mayoría de los proxies inversos conocidos no son compatibles con Websockets y descartan muchas áreas importantes de la primera solicitud Websocket.

Si sabe que el servidor está detrás de un proxy inverso, desactive Websockets configurando esta opción en Clients\www\software\html5\settings.js :

disablewebsocket = true;

Eso hará cumplir el uso de XHR-polling y evitar retrasos al conectarse.

Si no tiene un archivo llamado “settings.js” en la carpeta “C:\Program Files (x86)\TSplus\Clients\www\software\html5”, entonces su versión de TSplus es más antigua y esta documentación no se aplica. Por favor, actualice su sistema primero o contacte con el soporte.

Tenga en cuenta que el uso de XHR-polling no es tan estable como Websockets debido a la naturaleza de su conexión.

La otra limitación al usar la sondeo Xhr a través de un proxy inverso es el pobre soporte en la carga de archivos. Mientras se trabaja con XHR en conexión directa, realizado por ejemplo a través de un proxy inverso de Apache, Apache puede interrumpir accidentalmente la carga del archivo.

TSplus Virtual Printer v2

¡Una nueva versión de Virtual Printer ya está disponible!
Esta versión incluye una actualización importante para el componente de Virtual Printer (v1.x -> v2.x).

¿Por qué? la impresora virtual v2 es el último buque insignia de Fabulatech, que trae muchas mejoras y soluciona problemas reportados por los clientes.

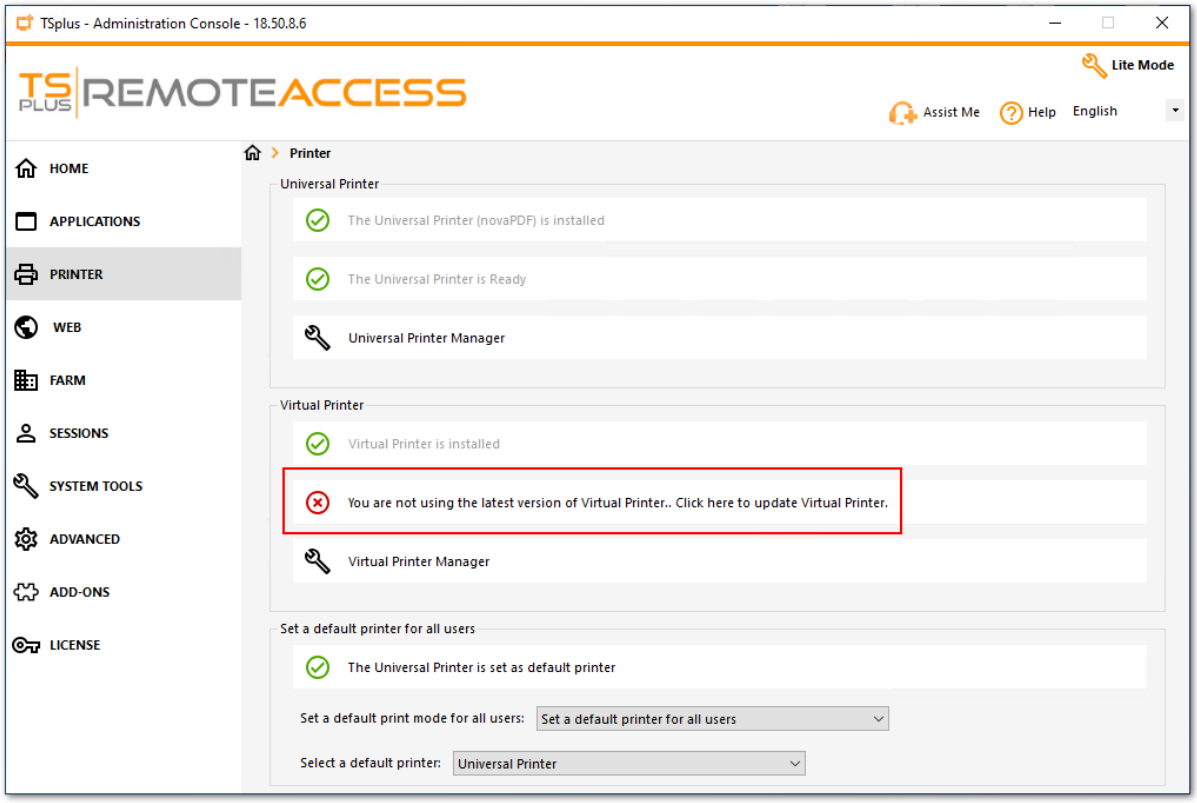
Atención: Virtual Printer v1.x y v2.x no son compatibles, necesitas la misma versión principal en ambos lados, cliente y servidor, para funcionar correctamente.

No te preocupes: la actualización solo trae los nuevos programas de configuración de la impresora virtual (cliente y servidor).
Están ubicados en C:\Program Files (x86)\TSplus\UserDesktop\files\addons .
Depende de usted activar manualmente la actualización real de la impresora virtual desde AdminTools.

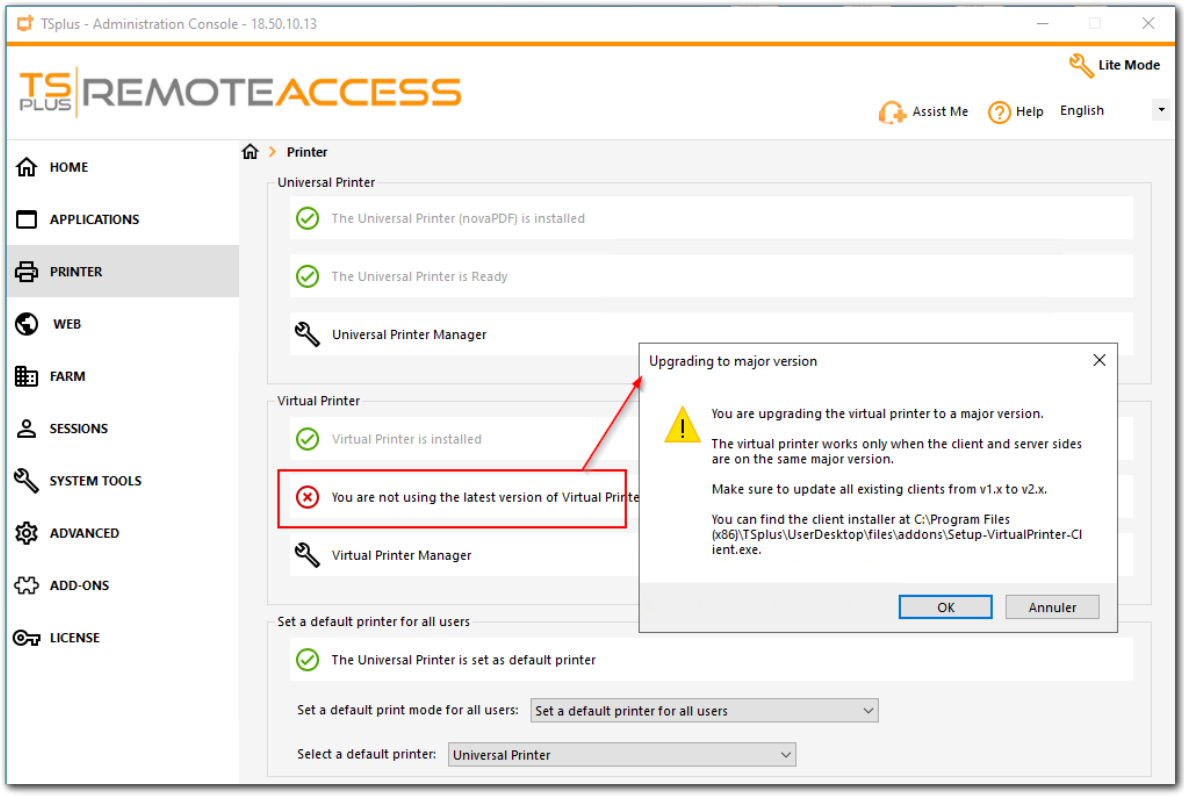
Enlaces : TSplus Configuración Completa TSplus Actualización de Lanzamiento Actualización de Rebranding

¿Cómo actualizar?

Después de instalar la UpdateRelease, AdminTools detectará que hay una nueva versión de la impresora virtual disponible.
Hasta que haga clic en el botón de "actualización de aviso", la versión de la impresora virtual que tiene instalada actualmente permanecerá sin cambios y todo seguirá funcionando como antes.

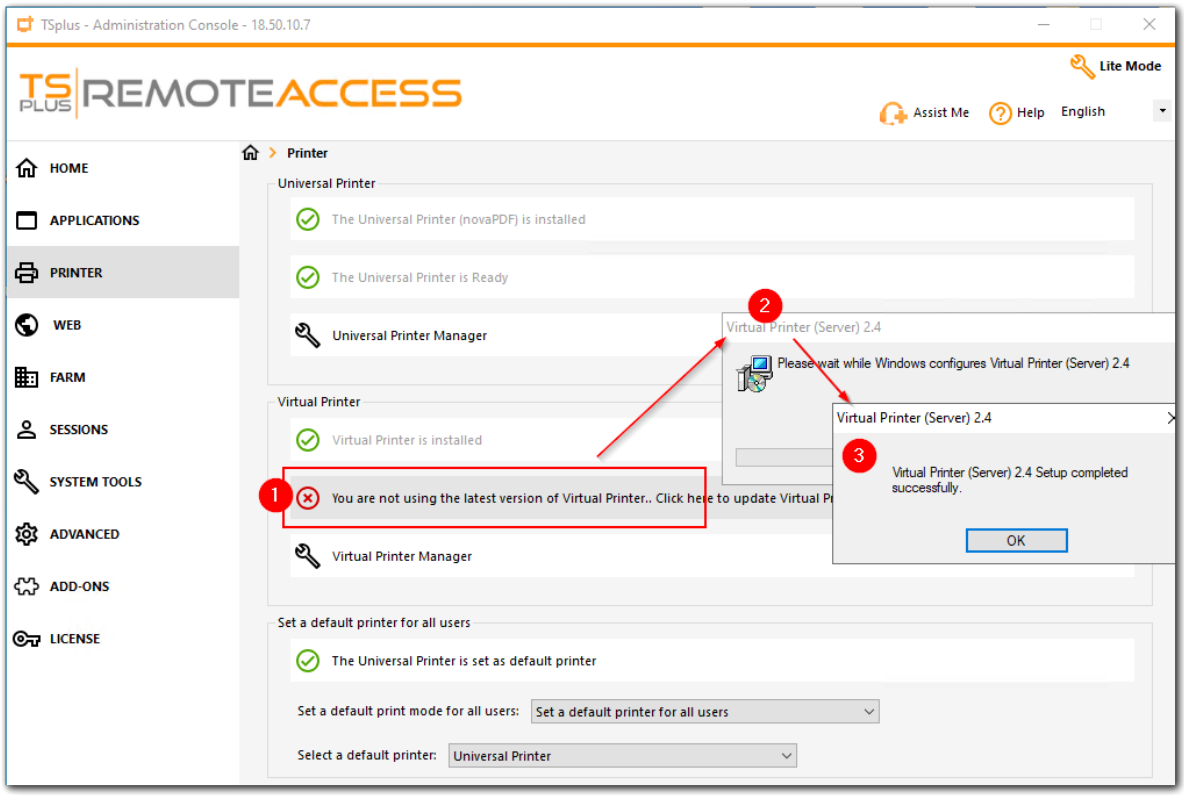


Está bien, pero estamos aquí para instalar la nueva versión de VP, así que hagamos clic en el botón de "notificar actualización".

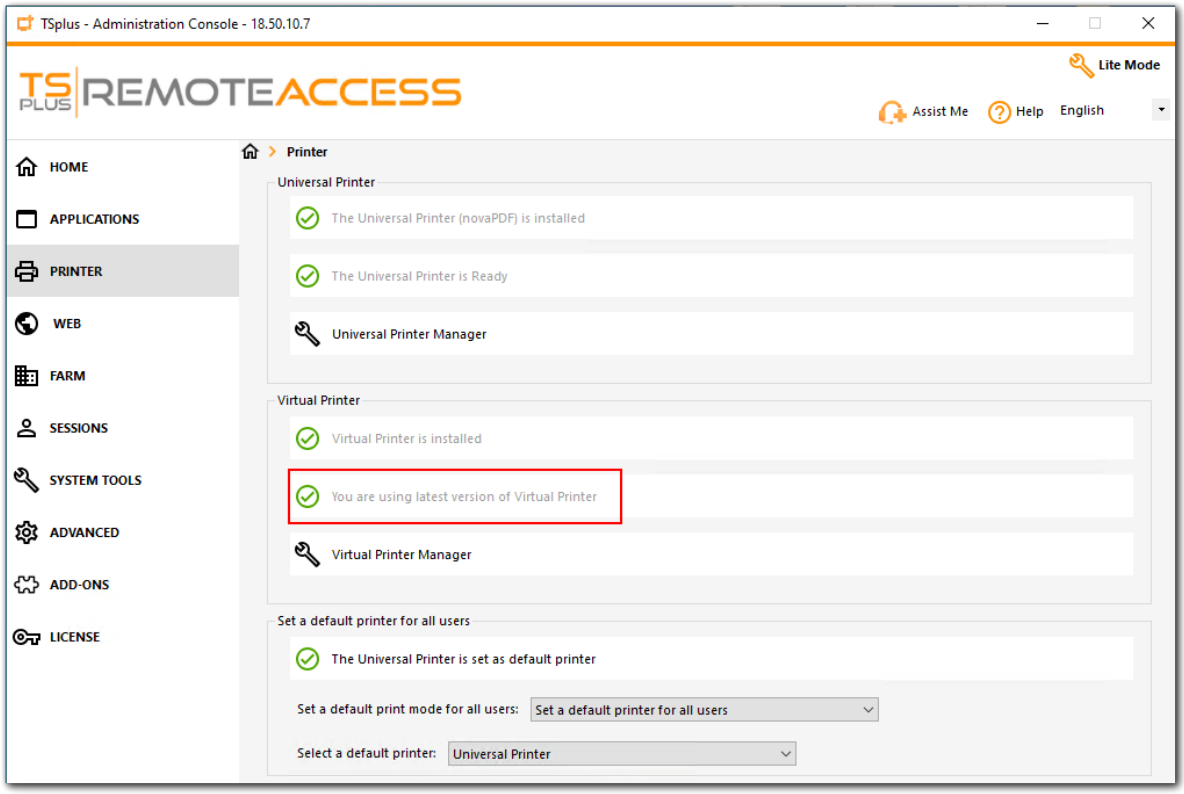


Un cuadro de diálogo de confirmación pregunta si realmente desea actualizar la impresora

virtual a la siguiente versión importante. Haga clic en "Aceptar".



Una vez instalado, el AdminTools detecta que estás actualizado.



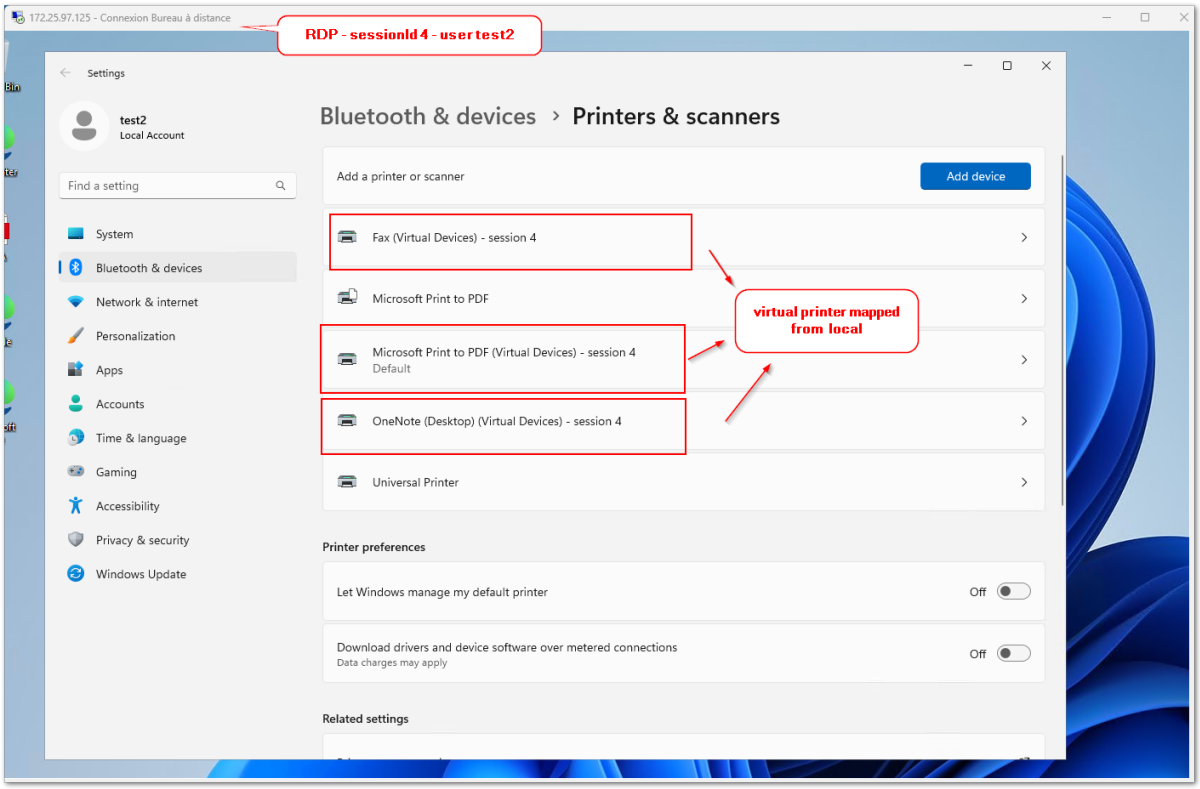
Atención: en este paso, solo los clientes que ejecutan la misma versión principal (v2.x) pueden imprimir a través de la impresora virtual en este servidor. Asegúrese de coordinar la actualización tanto del servidor como de los clientes. El instalador del cliente se encuentra en “C:\Program Files (x86)\TSplus\UserDesktop\files\addons\Setup-VirtualPrinter-Client.exe”

¡Cambio drástico!

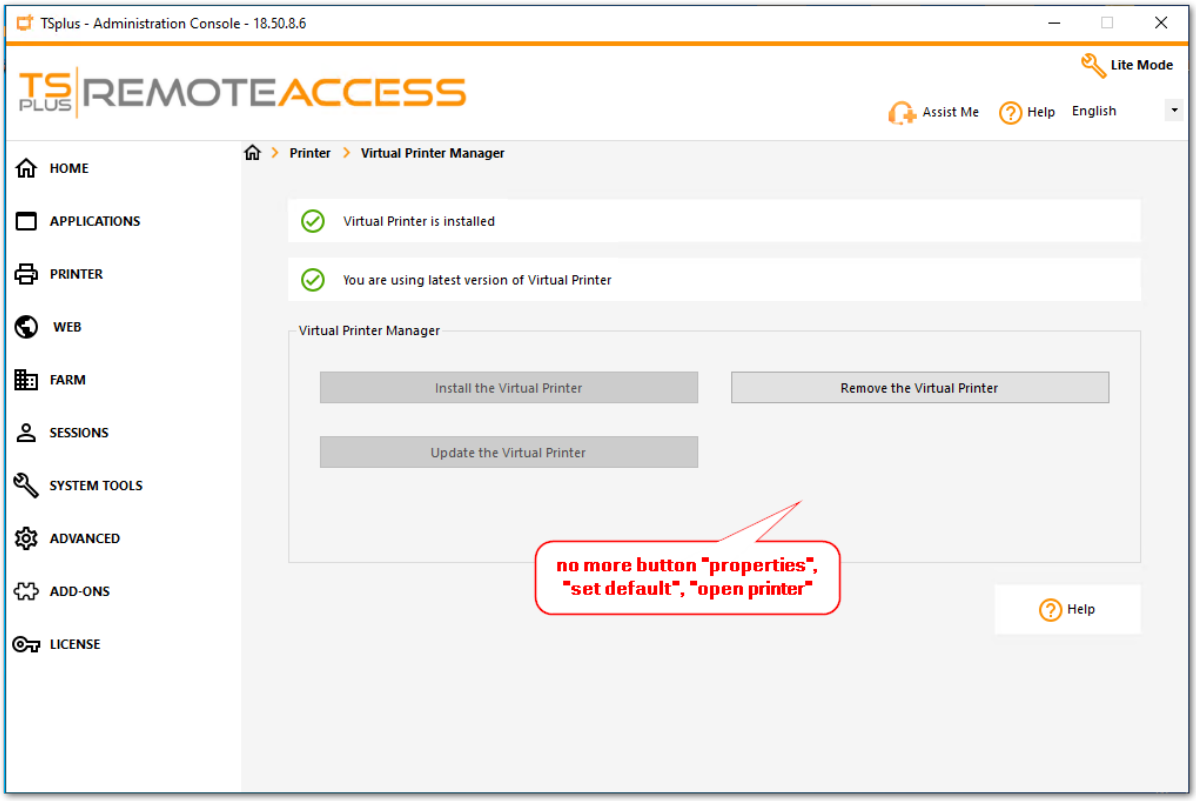
Ya no hay un único dispositivo de "Virtual Printer" en la lista de impresoras. En su lugar, cada impresora local ahora está mapeada a una impresora virtual correspondiente en la sesión RDP.

En la captura de pantalla a continuación, el usuario “test2” está conectado a la sesión RDP #4. Al abrir el panel de impresoras,
él puede ver y usar sus impresoras locales. Cada nombre de impresora sigue este formato : $printerName (Dispositivos Virtuales) - sesión $sessionId .

El hecho de que el usuario ahora vea cada una de sus impresoras locales de forma individual es una gran mejora en la experiencia del usuario, y por eso Fabulatech está impulsando esta nueva versión.

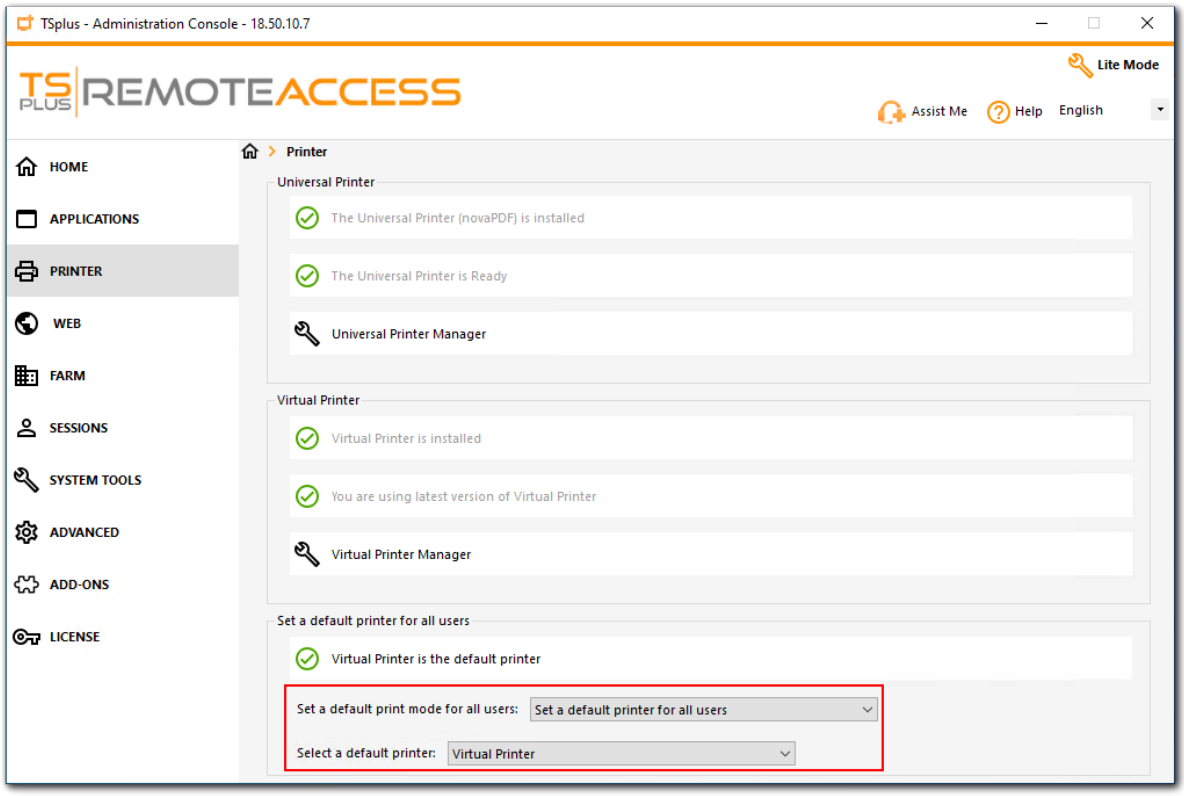


Debido a esto, hemos ajustado algunas partes en la interfaz de AdminTools, como el Administrador de Impresoras Virtuales: se han eliminado algunos botones.

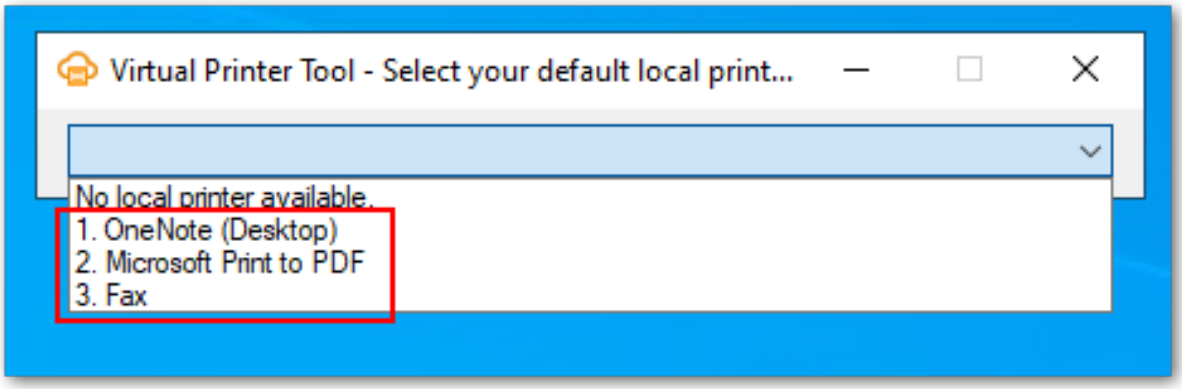


¿Cómo configurar?

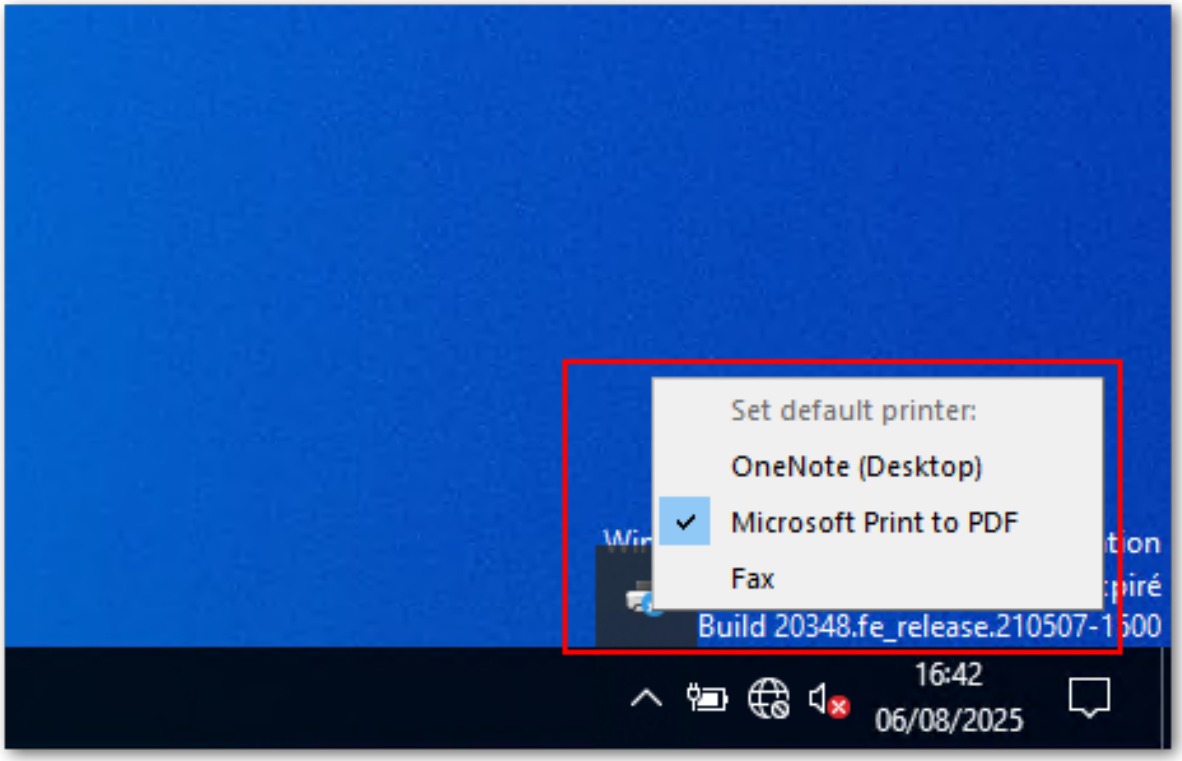
La configuración sigue siendo la misma en AdminTools y debería funcionar como antes.



Si utilizas las herramientas de Virtual Printer, nada cambia y funciona como antes.



Si utilizas el selector en la barra de herramientas, nada cambia y funciona como antes.



¿Cómo personalizar el nombre de los dispositivos mapeados de la impresora virtual?

En el servidor, ejecute el “customize-virtual-printer-name.reg” adjunto. Descargar

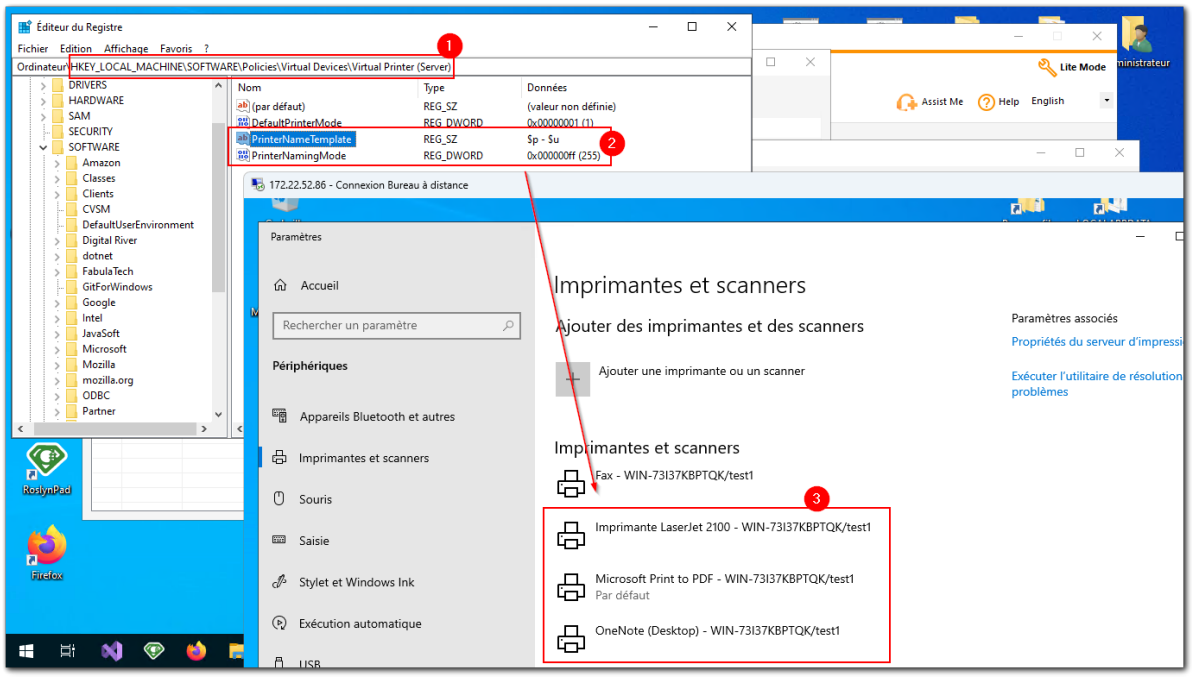
Agregará 2 claves en su registro HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Dispositivos Virtuales\Impresora Virtual (Servidor)

El PrinterNameTemplate es la cadena de plantilla, y hay 3 variables disponibles:

- $p - nombre de la impresora
- $u - nombre de usuario completo (dominio/usuario, o nombre de equipo/usuario)
- $s - número de sesión

Dadas algunas limitaciones de Fabuletch: **Es obligatorio especificar $p y $u, o $p y $s.** Es necesario ya que los nombres de las impresoras deben ser únicos en el servidor para diferentes usuarios.

Ejemplo: PrinterNameTemplate = “$p $u”, puedes ver el resultado en la captura de pantalla de la sesión RDP a continuación.



Configuración avanzada

La configuración avanzada para Virtual Printer v2 se puede gestionar del lado del servidor a través de la Política de Grupo o el Objeto de Política Local en Configuración del Equipo > Plantillas Administrativas > Dispositivos Virtuales > Virtual Printer (Servidor).

Las siguientes configuraciones son relevantes para la integración de Remote Access:

- Modo de selección de impresora predeterminada: Define cómo se asigna la impresora predeterminada cada vez que un usuario inicia sesión en una sesión remota.
- Nombre de la plantilla de impresora: Especifica el formato de nombrado para impresoras virtuales de sesiones de usuario.
- Limitar la calidad para impresiones grandes: Reduce la calidad de impresión para páginas que superan un tamaño especificado para acelerar la impresión en gran formato mientras se

preserva la máxima calidad para páginas más pequeñas.

Para obtener detalles completos de configuración, consulte la documentación de GPO de Virtual Printer en https://www.fabulatech.com/printer-for-remote-desktop-server-help/gpo.html

TSplus Virtual Printer

La impresora virtual de TSplus es una nueva alternativa a las soluciones clásicas de impresión de escritorio remoto, que pueden ser poco fiables, dependientes del hardware y difíciles de gestionar. El algoritmo de compresión único de la impresora virtual mejora la velocidad de tránsito de los trabajos de impresión remota al minimizar la transferencia de datos mientras mantiene la calidad de imagen.

Nota El cliente HTML5 de TSplus no es compatible y requiere el TSplus Universal Printer .

Beneficios

- Soporte para entornos de usuario único y multiusuario.
- No se requiere configuración.
- Funciona con cualquier máquina virtual.
- Entorno mixto de 32 y 64 bits.

Requisitos previos

Lista de compatibilidad del sistema operativo de la impresora virtual TSplus:

- Windows **7**
- Windows **8/8.1**
- Windows **10**
- Windows **11**
- Windows **Server 2008 R2**
- Windows **Server 2012 R2**
- Windows **Server 2016**
- Windows **Servidor 2019**

- Windows **Server 2022**
- Windows **Servidor 2025**

El TSplus Virtual Printer es compatible con:

- El cliente generado por TSplus
- El cliente TSplus RemoteApp
- El complemento TSplus RemoteApp al usar el Portal Web
- El cliente de Escritorio Remoto de Microsoft

No es compatible con:

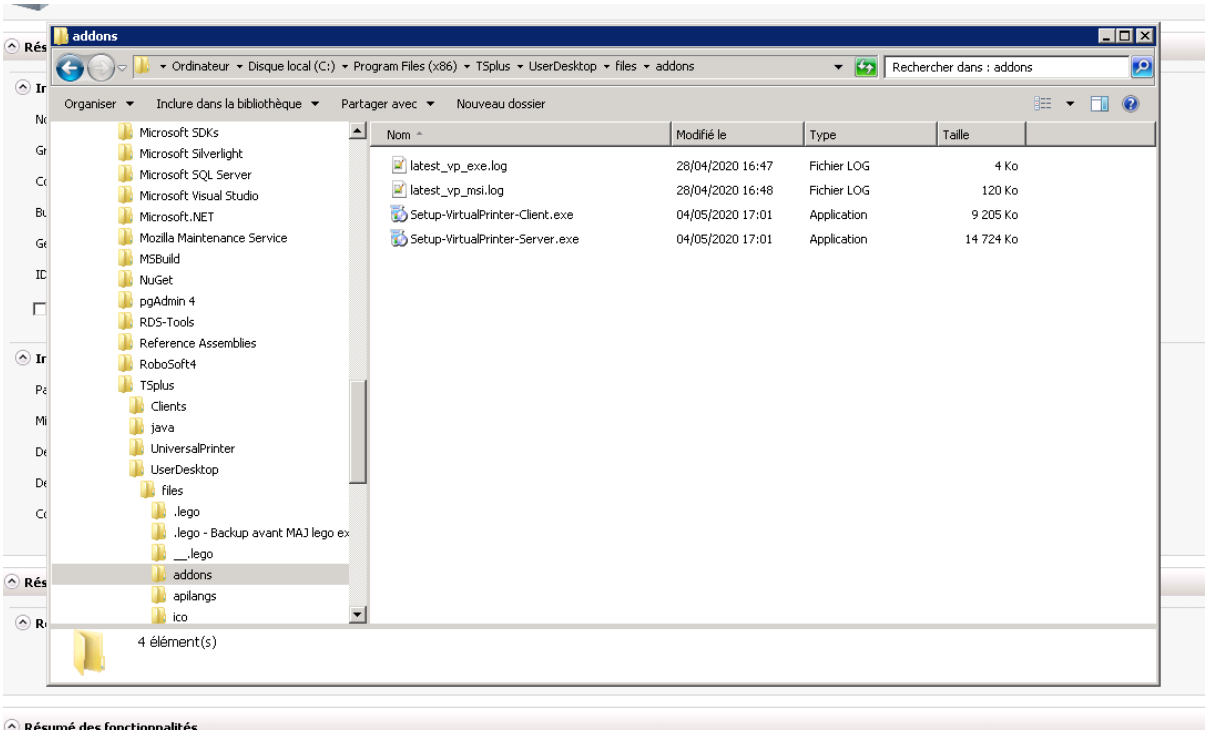
- El cliente HTML5 de TSplus
- Dispositivos de cliente delgado codificados de forma rígida donde no se puede instalar la configuración del lado del cliente.

Dos partes

El TSplus Virtual Printer se compone de dos componentes:

- Un componente del lado del servidor que se instala en TSplus Remote Access.
- Un componente de escritorio que se instala en la estación de trabajo de Windows del usuario final.

Ambas configuraciones están disponibles directamente en el lado del servidor en la carpeta “C:\Program Files (x86)\TSplus\UserDesktop\files\addons” y se llaman “Setup-VirtualPrinter-Server.exe” y “Setup-VirtualPrinter-Client.exe”:



La configuración del cliente también está disponible desde su servidor web TSplus, utilizando el enlace a continuación:

“tuipdeservidorsplusopúblico”/addons/Setup-VirtualPrinter-Client.exe

También puede realizar una instalación silenciosa del Cliente a través de una línea de comandos, ejecutando la configuración con los siguientes parámetros:

/SUPPRESSMSGBOXES /VERYSILENT /SILENT /no_ui

Comenzando

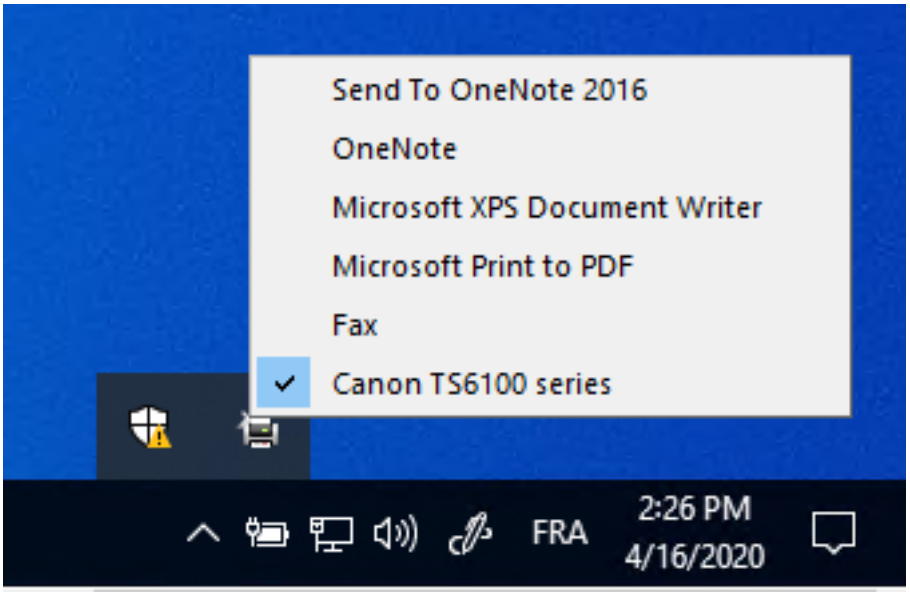
TSplus Virtual Printer se instala automáticamente durante la primera instalación de TSplus y está disponible directamente durante el período de prueba.

Una vez que TSplus esté instalado, necesitarás instalar el “Cliente de Impresora Virtual” en la computadora del usuario.

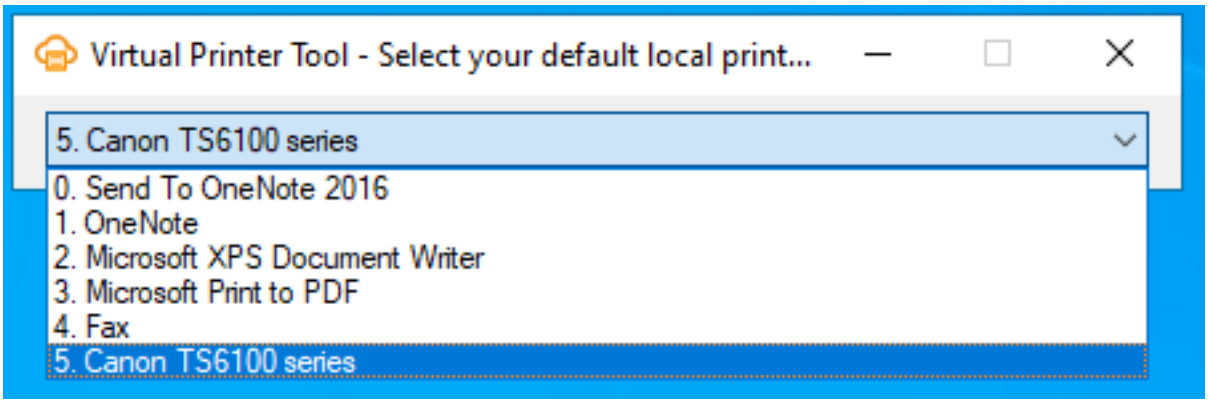
Cuando te conectas de forma remota a tu servidor TSPlus utilizando cualquiera de **cliente RDP de Microsoft** mstsc **Cliente generado por TSplus** o **Complemento RemoteApp del Portal Web** podrá imprimir desde su sesión remota a su impresora local utilizando la impresora “Virtual Printer”. Por defecto, la impresora local seleccionada es la impresora predeterminada local.

Tienes 2 formas de cambiar la impresora local asignada a la impresora “Virtual Printer” según tu situación:

1. Si está utilizando el escritorio completo, entonces puede seleccionar qué impresora local utilizar mediante el icono de la impresora virtual en la bandeja del sistema:



2. Si no tienes acceso al escritorio completo, necesitarás usar la "Herramienta de Impresora Virtual" llamada "VirtualPrinterTool.exe" ubicada en "C:\Program Files (x86)\TSplus\UserDesktop\files". Nota: puedes asignar la aplicación al usuario o hacer que se ejecute automáticamente al iniciar sesión a través de la configuración avanzada de la Impresora Virtual.

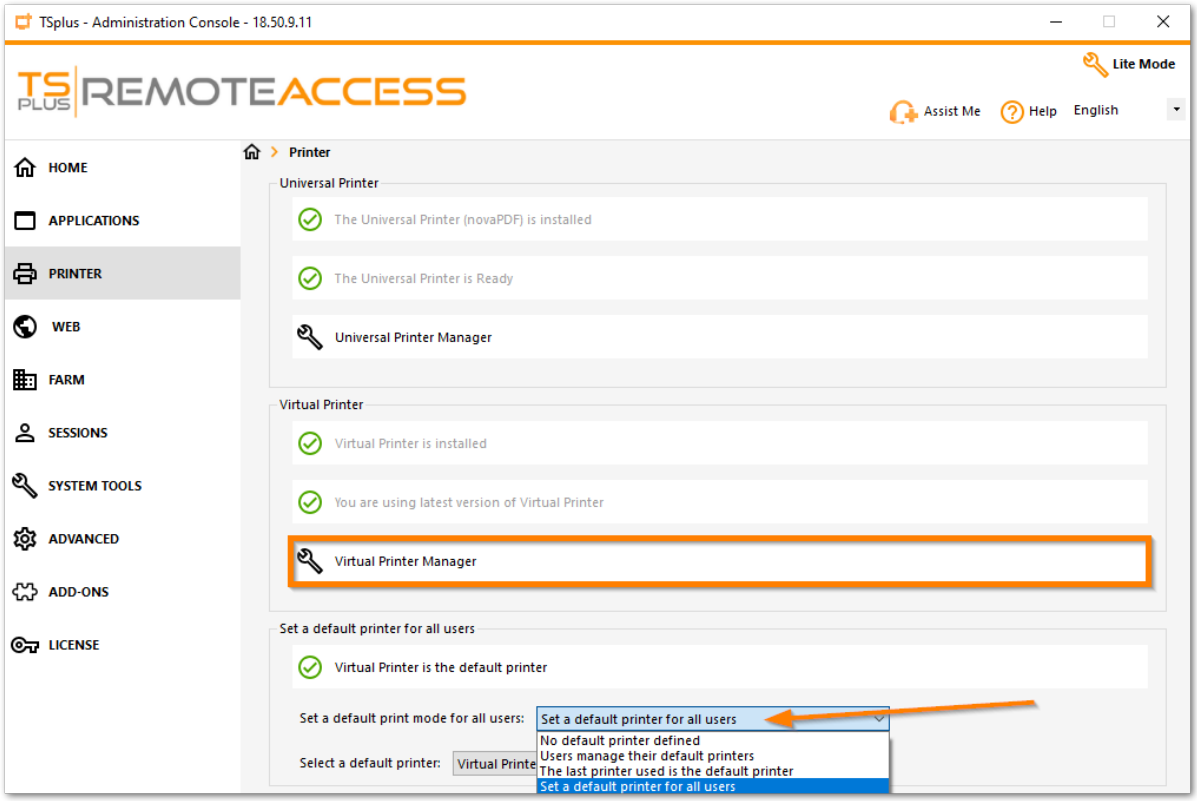


Configuración

Para acceder al panel de control de la TSplus Virtual Printer, por favor navegue a través del AdminTool: Impresora > Administrador de Impresoras Virtuales.

Establecer una impresora predeterminada para todos los usuarios

- No se ha definido una impresora predeterminada: la configuración de la impresora predeterminada del usuario no se ve afectada.
- El usuario gestiona sus impresoras predeterminadas: la opción "Dejar que Windows gestione mi impresora predeterminada" está desactivada, por lo que depende del usuario seleccionar su impresora predeterminada.
- La última impresora utilizada es la impresora predeterminada: la opción "Dejar que Windows administre mi impresora predeterminada" está habilitada.
- Establecer una impresora predeterminada para todos los usuarios: el administrador obliga a la impresora predeterminada del usuario.



Solución de problemas de la impresora virtual

Si la Impresora Virtual no está funcionando, la causa más común es que el software del lado del cliente "Aplicación de Impresión" no se esté ejecutando en el Administrador de Tareas del ordenador local del usuario, o que el software de la Impresora Virtual (servidor) se haya instalado en el ordenador local del usuario, en lugar de la versión de la Impresora Virtual (estación de trabajo) (Setup-VirtualPrinter-Client.exe). A continuación se detallan los pasos de solución de problemas tanto para el lado del cliente como para el del servidor.

Tenga en cuenta que la Impresora Virtual no es compatible con nuestro cliente HTML5. Si está utilizando el cliente HTML5, utilice la Impresora Universal en su lugar.

Guía de solución de problemas

¿Cómo activar una licencia por volumen desde el servidor después de la configuración?

Si ha instalado su producto sin ninguna línea de comandos, entonces se ha instalado como una versión de prueba.

Activar

Para activar su Licencia por Volumen, ejecute la siguiente línea de comando como administrador elevado:

- **Acceso Remoto y Autenticación de Dos Factores**
  C:\Program Files (x86)\TSplus\UserDesktop\files>
  AdminTool.exe TwoFactor.Admin.exe
  /Usuarios 1 (1 a 50 o ilimitado)
  /edición Enterprise (Escritorio, Web Móvil, Empresarial)
  /soporteaños 1 (1,2,3 solo)

Ejemplo : C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /users 30 /edition Enterprise /supportyears 1

Ejemplo : C:\Program Files (x86)\TSplus\UserDesktop\files\TwoFactor.Admin.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /supportyears 1

- **Advanced Security**
  C:\Program Files (x86)\TSplus-Security>
  TSplus-Security.exe
  /edición Ultimate Esenciales o Ultimate
  /soporteaños 1 (1,2,3 solo)

Ejemplo : C:\Program Files (x86)\TSplus-Security\TSplus-Security.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /edition Ultimate /supportyears 1

- **Server Monitoring**
  C:\Program Files (x86)\TSplus-ServerMonitoring>

ServerMonitoring.exe
/Usuarios 1 (1 para Startup, 5 para Esencial, 10 para Negocios)
/soporteaños 1 (1 para Startup, 5 para Esencial, 10 para Negocios)

Ejemplo : C:\Program Files (x86)\TSplus-ServerMonitoring\ServerMonitoring.exe /vl /activate TU-CLAVE-DE-LICENCIA-VOLUMEN /usuarios 5 /añosdesoporte 1

- **Puedes agregar mis siguientes parámetros adicionales:**
  — tus comentarios Especifique los comentarios que se adjuntarán a la licencia en el portal de licencias.
  — /verysilent Ejecute el programa de instalación en silencio. Esto permite la integración de este programa de instalación en sus propios scripts de inicialización o automatización.

Ejemplo : C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /users unlimited /edition Enterprise /supportyears 3 /comments "Este es un comentario"*

Parámetros

Este comando toma los siguientes parámetros:

si te gusta usar líneas de comando y te preguntas qué otras líneas de comando están disponibles, por favor ve a este documentación específica)

Actualizar soporte

Para extender su suscripción de actualización/soporte, elija 1, 2 o 3 en función del tiempo de extensión.
Usa este comando:

AdminTool.exe /vl /renewsupport YOUR-VOLUME-LICENSE-KEY /supportyears 1"

Agregar soporte faltante

Este comando es particularmente útil si el cliente olvidó activar el soporte durante la instalación o si necesita establecer una fecha de finalización específica para su período de soporte.

Ejecute este comando como administrador, reemplazando los detalles con su propia información de licencia y la fecha de finalización de soporte preferida:

AdminTool.exe /vl /activate-support SU-CLAVE-DE-LICENCIA-VOLUMEN /users [number] /edition [edition] /endofsupport [YYYY-MM-DD]

Para activar el soporte para un usuario de Remote Access 5 con la edición Printer hasta el 25 de

julio de 2026, ingrese:

AdminTool.exe /vl /activate-support YOUR-VOLUME-LICENSE-KEY /users 5 /edition Printer /endofsupport 2026-07-25

Esta nueva función facilita la gestión de los períodos de soporte, para que los clientes siempre sepan cuándo comienza y termina su período de soporte.

¿Cómo mostrar los créditos de licencia restantes para una clave de Licencia por Volumen?

Para mostrar los créditos de licencia restantes para una clave de Licencia por Volumen, ejecute la siguiente línea de comando como Administrador elevado:

AdminTool.exe /vl /credits-license VOLU-MELI-CENS-EKEY /login JOHNDOE [/edición Essentials] [/silent]

Parámetros

Este comando puede tomar cuatro parámetros:

- VOLU-MELI-CENS-EKEY : use su propia Clave de Licencia por Volumen
- /provide el inicio de sesión del socio asociado con la clave de licencia por volumen
- /edición Essentials: proporcione el parámetro de edición opcional para productos de Advanced Security y Server Monitoring
- /silencio : ejecuta el comando en silencio

La salida se almacenará en la variable de entorno a nivel de usuario llamada CREDITOS_DE_LICENCIA_DE_VOLUMEN Puede ser necesario leer el valor de CREDITOS_DE_LICENCIA_DE_VOLUMEN desde un proceso diferente, utilizando el comando: echo %VOLUME_LICENSE_CREDITS%

Por favor, encuentre a continuación las ediciones esperadas para los productos de Advanced Security y Server Monitoring:

- Seguridad Avanzada: “Esenciales”, “Ultimate”
- Server Monitoring: “Esenciales”, “Inicio”, “Negocios”

Los siguientes ejecutables deben ser utilizados para encontrar el número respectivo de créditos restantes:

- Remote Access: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe
- Seguridad Avanzada: C:\Program Files (x86)\TSplus-Security\TSplus-Security.exe

- Server Monitoring: C:\Program Files (x86)\TSplus-ServerMonitoring\ServerMonitoring.exe
- 2FA: C:\Program Files (x86)\TSplus\UserDesktop\files\TwoFactor.Admin.exe
- RPA: C:\Program Files (x86)\TSplus-RPA\AdminTool.exe
- Trabajo remoto: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe

---

título: “¿Cómo mostrar los créditos de soporte restantes para una clave de licencia por volumen?”

Para mostrar los créditos de soporte restantes para una clave de Licencia por Volumen, ejecute la siguiente línea de comando como Administrador elevado:

AdminTool.exe /vl /credits-support VOLU-MELI-CENS-EKEY /login JOHNDOE [/edición Essentials] [/silent]

Parámetros

Este comando puede tomar cuatro parámetros:

- VOLU-MELI-CENS-EKEY : use su propia Clave de Licencia por Volumen
- /provide el inicio de sesión del socio asociado con la clave de licencia por volumen
- /edición Essentials: proporcione el parámetro de edición opcional para productos de Advanced Security y Server Monitoring
- /silencioso : ejecuta el comando en silencio.

La salida se almacenará en la variable de entorno a nivel de usuario llamada CREDITOS_DE_LICENCIA_DE_VOLUMEN Puede ser necesario leer el valor de CREDITOS_DE_LICENCIA_DE_VOLUMEN desde un proceso diferente, utilizando el comando: echo %VOLUME_LICENSE_CREDITS%

Por favor, encuentre a continuación las ediciones esperadas para los productos de Advanced Security y Server Monitoring:

- Seguridad Avanzada: “Esenciales”, “Ultimate”
- Server Monitoring: “Esenciales”, “Inicio”, “Negocios”

Los siguientes ejecutables deben ser utilizados para encontrar el número respectivo de créditos restantes:

- Remote Access: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe
- Seguridad Avanzada: C:\Program Files (x86)\TSplus-Security\TSplus-Security.exe

- Server Monitoring: C:\Program Files (x86)\TSplus-ServerMonitoring\ServerMonitoring.exe
- 2FA: C:\Program Files (x86)\TSplus\UserDesktop\files\TwoFactor.Admin.exe
- RPA: C:\Program Files (x86)\TSplus-RPA\AdminTool.exe
- Trabajo remoto: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe

¿Cómo deshabilitar una licencia desde el servidor?

Para deshabilitar un servidor que fue activado con una clave de Licencia por Volumen, ejecute la siguiente línea de comando como Administrador elevado:

AdminTool.exe /vl /disable VOLU-MELI-CENS-EKEY

¿Cómo habilitar una licencia desde el servidor?

Para habilitar un servidor que fue activado por primera vez con una clave de Licencia por Volumen y que luego fue deshabilitado, ejecute la siguiente línea de comando como Administrador elevado:

AdminTool.exe /vl /enable VOLU-MELI-CENS-EKEY

¿Cómo deshabilitar una licencia desde el portal de licencias?

Debes primero desactivar la Licencia en el portal de Licencias, luego asegúrate de que el nuevo estado se aplique en tu servidor actualizando su estado desde la aplicación de administración o la línea de comandos.

Primero, desde ambas la lista de Licencias y las páginas de detalles de Licencias, puedes hacer clic en el botón "Deshabilitar" para deshabilitar la Licencia seleccionada.

La licencia pasará del estado "Habilitado" al estado "Deshabilitando...", lo que significa que actualmente está esperando a que el servidor se desactive.
Luego, el servidor se desactivará automáticamente al día siguiente si tiene acceso a internet.

También puedes hacer esto manualmente ejecutando la siguiente línea de comando como Administrador elevado:

AdminTool.exe /license /refresh

Tenga en cuenta que no es necesario ejecutar la línea de comando de actualización para todo el software instalado. La actualización es compatible con todos los productos que son compatibles con el sistema de licencias de 2020.

La licencia se contabilizará en el uso de su licencia hasta que su servidor haya contactado el portal de licencias y reconocido su estado deshabilitado.

¿Cómo instalar un servidor de licencias por volumen en un paso?

Para instalar un servidor de Licencia por Volumen en un solo paso, necesitarás:

- Descargar el programa de instalación del producto
- Utilice su clave de licencia por volumen
- Ejecute el programa de instalación con su clave de licencia por volumen como parámetro.

Tu clave de licencia por volumen es la misma para cualquier instalación de cualquier nuevo servidor. Si no la recuerdas, conéctate a tu cuenta en el portal de licencias. Tu clave de licencia por volumen se muestra en la parte superior de la página de inicio (Licencias).

Para instalar y activar una Licencia por Volumen desde un script, ejecute la siguiente línea de comando como Administrador elevado:

C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate VOLU-MELI-CENS-EKEY /users unlimited /edition Enterprise /supportyears 3 /comments "Este es un comentario"

La activación por script utilizando la Licencia por Volumen 2020 está disponible para los siguientes productos y todas sus versiones reetiquetadas:

- Remote Access
- Seguridad Avanzada (también conocida como RDS-Knight)
- Monitoreo del Servidor (anteriormente Server Genius)
- Autenticación de Dos Factores

Parámetros

Este comando toma los siguientes parámetros:

- **Acceso Remoto y Autenticación de Dos Factores**
  C:\Program Files (x86)\TSplus\UserDesktop\files>
  AdminTool.exe TwoFactor.Admin.exe
  /Usuarios 1 (1 a 50 o ilimitado)

/edición Enterprise (Escritorio, Web Móvil, Empresarial)
/soporteaños 1 (1,2,3 solo)

- **Advanced Security**
  C:\Program Files (x86)\TSplus-Security>
  TSplus-Security.exe
  /edición Ultimate Esenciales o Ultimate
  /soporteaños 1 (1,2,3 solo)

- **Server Monitoring**
  C:\Program Files (x86)\TSplus-ServerMonitoring>
  ServerMonitoring.exe
  /Usuarios 1 (1 para Startup, 5 para Esencial, 10 para Negocios)
  /soporteaños 1 (1 para Startup, 5 para Esencial, 10 para Negocios)

Métodos de Scripting

Para iniciar Setup-PRODUCT.exe con su línea de comandos correcta, puede utilizar 3 métodos:

1. Utiliza tus propios métodos de scripts de gestión

2. Cree un acceso directo de Setup-PRODUCT.exe y edite las propiedades para agregar la línea de comando al final de la ruta.

3. Simplemente abra una "línea de comandos" presionando la tecla de Windows y la tecla "R" simultáneamente, luego escriba "cmd" y presione la tecla "Enter" para confirmar. Este método con el atajo de teclado funciona en todas las versiones de Windows existentes en el momento de redactar este documento.

4. Una vez que aparezca el aviso, cambie el directorio actual al directorio donde se encuentra su programa de instalación (generalmente su carpeta de Descargas). Por ejemplo, escriba:

   cd C:\Program Files (x86)\TSplus\UserDesktop\files

Y finalmente escribe el comando completo para ejecutar el programa de instalación con los siguientes parámetros, proporcionando los valores deseados:

C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate VOLU-MELI-

CENS-EKEY /users unlimited /edition Enterprise /supportyears 3 /comments “Este es un comentario”

Encuentra el programa de administración relevante

Los siguientes programas admiten comandos de Licencia por Volumen.
El nombre del programa y la ubicación dependen del producto y su carpeta de configuración:

Acceso Remoto y Autenticación de Dos Factores
C:\Program Files (x86)\TSplus\UserDesktop\files>
AdminTool.exe TwoFactor.Admin.exe

Advanced Security
C:\Program Files (x86)\TSplus-Security>
TSplus-Security.exe

Server Monitoring
C:\Program Files (x86)\TSplus-ServerMonitoring>
ServerMonitoring.exe

La ejecución del programa es silenciosa. Esto permite la integración de su proceso de activación de licencia en sus propios scripts de inicialización o automatización.

---

título: “Solución de problemas para activar, habilitar, deshabilitar y actualizar comandos”

Si desea investigar cualquier problema y/o al prototipar sus scripts, puede obtener mensajes de éxito y error al mirar el **VolumeLicensing.log** archivo encontrado en la raíz del programa.

---

título: “Cómo configurar un servidor proxy para acceso a Internet”

La configuración del proxy definida durante la instalación se recuerda y se utilizará para realizar operaciones sobre las licencias. Si no se definieron configuraciones de proxy, el programa de Licenciamiento por Volumen utilizará la configuración de proxy de Internet Explorer (si es que hay alguna configurada en la sesión en ejecución y/o para el servicio de Windows).

También puede configurar manualmente la configuración del proxy ejecutando la siguiente línea de comandos como Administrador elevado:

AdminTool.exe /proxy /set /host proxy.company.org /port 80 /username dummy /password pass@word1

Parámetros

#	Parameter	Description
1	/set	Action to be performed on the proxy settings
2	/host (ie | none | custom)	The destination host can be a predefined value (e.g. "ie" or "none") or a user-defined value (ex. 127.0.0.1 or proxy.company.org). This parameter is mandatory.
3	/port 80	The port number used to connect to the proxy server. Required if the hostname value is a custom user-defined value.
4	/username dummy	The username to connect to the proxy server. This setting is optional.
5	/password pass@word1	The user's password must be supplied if a username has been defined. However, its value can be empty.

si te gusta usar líneas de comando y te preguntas qué otras líneas de comando están disponibles, por favor ve a este documentación específica)

---

título: "Cómo obtener soporte para licencias por volumen"

El equipo de Soporte y Servicios de Licencias por Volumen estará más que feliz de ayudarle, si enfrenta algún problema o dificultad al instalar y ejecutar Licencias por Volumen en un servidor.

La forma más fácil de contactar al equipo de Soporte y Servicios de Licencias por Volumen es abrir un ticket en nuestro Helpdesk en línea en: https://support.tsplus.net

¿Cómo actualizar los usuarios de una licencia por volumen desde el servidor?

Para cambiar el número de usuarios asociados con su Licencia por Volumen activada, ejecute la siguiente línea de comando como Administrador elevado:

AdminTool.exe /vl /update VOLU-MELI-CENS-EKEY /users 10

Parámetros

Este comando toma dos parámetros:

- VOLU-MELI-CENS-EKEY : use su propia Clave de Licencia por Volumen
- usuarios ilimitados: use cualquier número del 1 al 50 o "ilimitado"

Por favor, tenga en cuenta que:

- Este comando no se aplica a Advanced Security y 2FA addon.
- Server Monitoring solo acepta los números 1, 5 y 10 correspondientes a las tres ediciones disponibles de Server Monitoring.
- Solo TSplus Remote Work acepta un número de usuarios mayor que 50.

---

título: “¿Cómo actualizar la edición de una licencia por volumen desde el servidor?”

Para cambiar la edición asociada con su Licencia por Volumen activada, ejecute la siguiente línea de comando como Administrador elevado:

AdminTool.exe /vl /update VOLU-MELI-CENS-EKEY /edition Enterprise

Parámetros

Este comando toma dos parámetros:

- VOLU-MELI-CENS-EKEY : use su propia Clave de Licencia por Volumen
- edición Enterprise : use el nombre de la edición

Por favor, tenga en cuenta que:

- Este parámetro no se aplica a Remote Work, Remote Support, Server Monitoring, 2FA addon y Server Genius.
- Las ediciones posibles son "Escritorio", "Web Móvil" o "Empresa" para Remote Access.
- Las ediciones posibles son "Esenciales" o "Ultimate" para Seguridad Avanzada.

si te gusta usar líneas de comando y te preguntas qué otras líneas de comando están disponibles, por favor ve a este documentación específica)

Actualizar soporte

Para extender su suscripción de actualización/soporte, elija 1, 2 o 3 en función del tiempo de extensión.
Usa este comando: AdminTool.exe /vl /renewsupport VOLU-MELI-CENS-EKEY /supportyears 1

Este comando solo está disponible a partir de la versión 15.60.11.8

Licenciamiento por volumen

Volume Licensing es una solución de licencias por scripting impulsada por TSplus para sus soluciones. Los siguientes productos admiten la activación utilizando Volume Licensing 2020: Remote Access, Remote Work, Advanced Security (también conocido como RDS-Knight), Remote Support o Server Monitoring (anteriormente Server Genius).

Cuando se crea su cuenta de Licenciamiento por Volumen en el portal de Gestión de Licencias, el equipo de Licenciamiento por Volumen proporcionará:

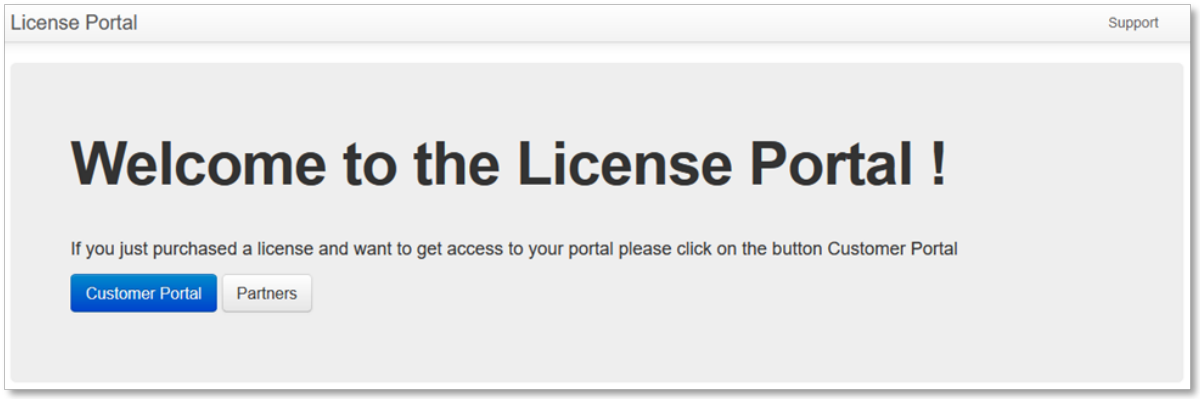
1. Su clave de licencia por volumen (por favor, mantenga esta información confidencial)
2. Tus credenciales para conectarte al portal de Gestión de Licencias
3. Esta Guía del Administrador de Licencias por Volumen 2020

LA IMPRESORA VIRTUAL YA NO ESTÁ LICENCIADA
Por favor, tenga en cuenta que desde el 15 de marzo de 2022 y la versión 15.40.3.14, Virtual Printer ya no está licenciado y está incluido en todas las ediciones de TSplus Remote Access.

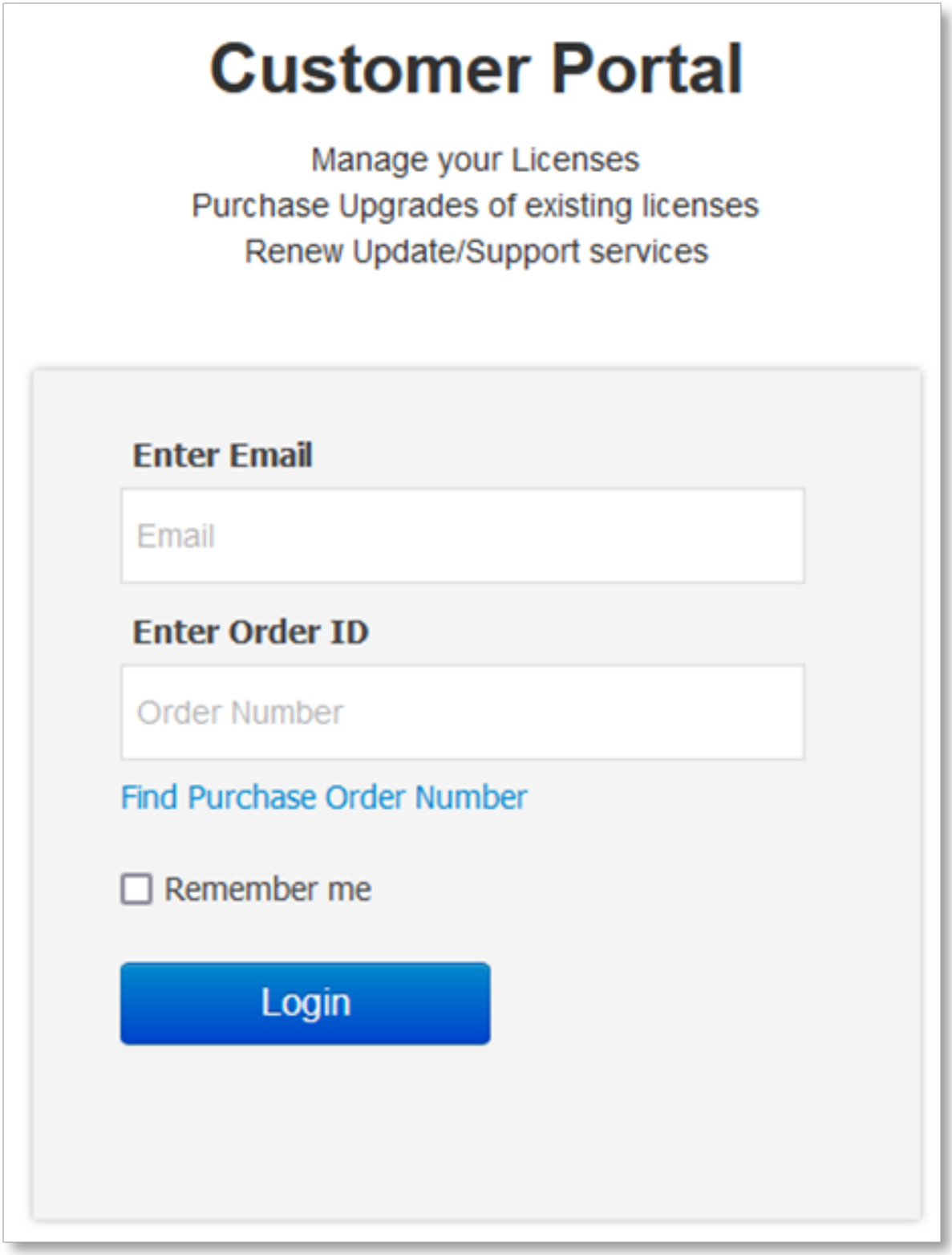
¿Cómo gestionar sus licencias por volumen?

Sus licencias por volumen y saldo de crédito se pueden revisar y gestionar en el portal de licencias de TSplus.
El portal de licencias de TSplus está disponible en la siguiente URL: https://license.tsplus.net

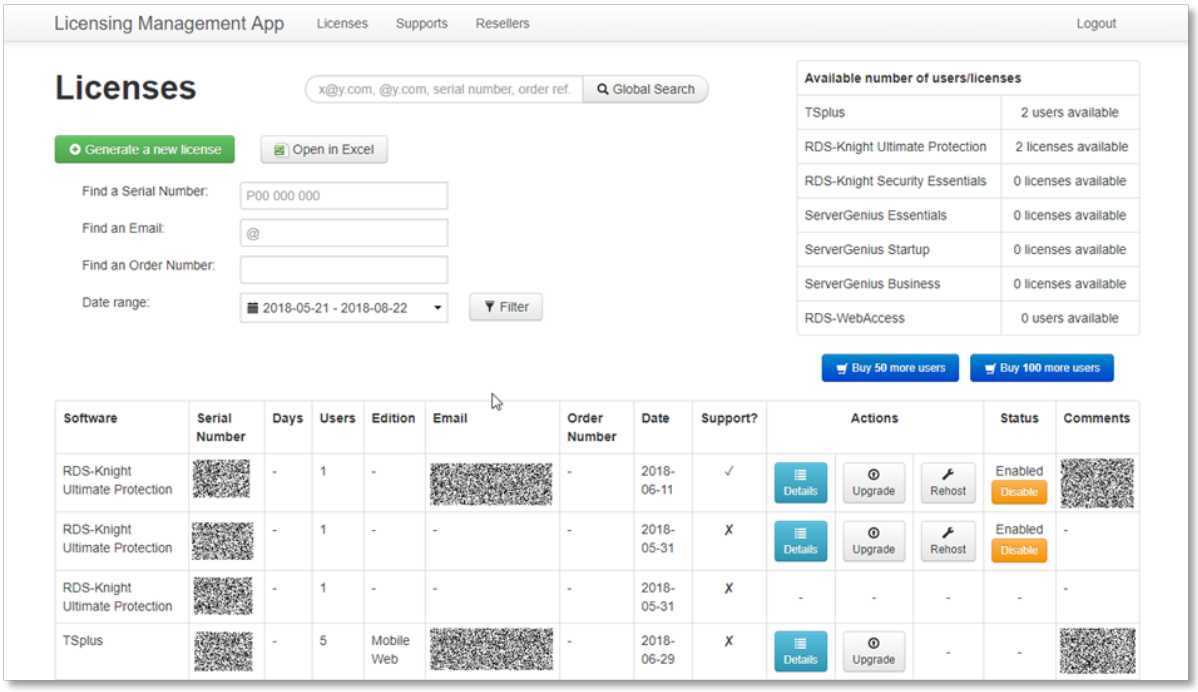
Para conectarse y acceder a su cuenta, comience haciendo clic en Portal del Cliente para llegar a la sección del cliente:



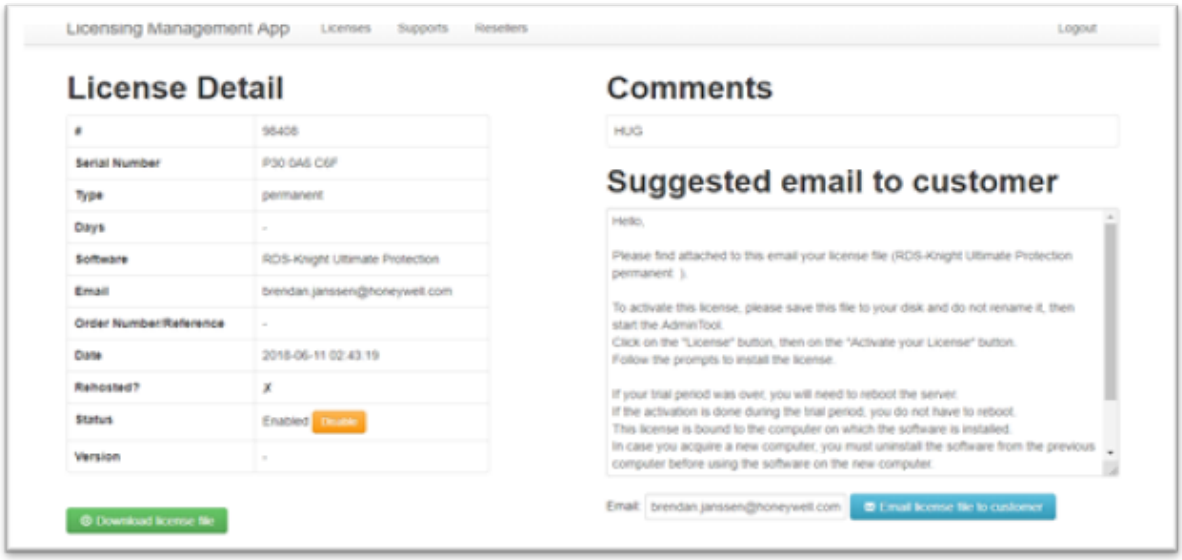
Luego, ingresa tus credenciales para acceder a tu cuenta:



Una vez que inicie sesión, verá la siguiente tabla donde se enumeran todas sus Licencias. Es la página principal donde podrá gestionar todas sus Licencias. Si aún no ha activado ninguna Licencia por Volumen, esta página estará vacía.



Para revisar los detalles del historial de una licencia, haga clic en el botón "Detalles" de la licencia que desea estudiar. Obtendrá la página de detalles de la licencia como se muestra en la imagen a continuación.



TSplus Web App

TSplus Web App es una Aplicación Web Progresiva (PWA) que aprovecha las API modernas de los navegadores para ofrecer una experiencia de acceso remoto sin la necesidad de instalaciones de software engorrosas o clientes de conexión complicados. Diseñada para utilizar protocolos de comunicación y visualización estándar de la industria HTML5, la TSplus Web App aparece como una solución de conexión nativa, sin importar qué tipo de dispositivo utilices.

Beneficios

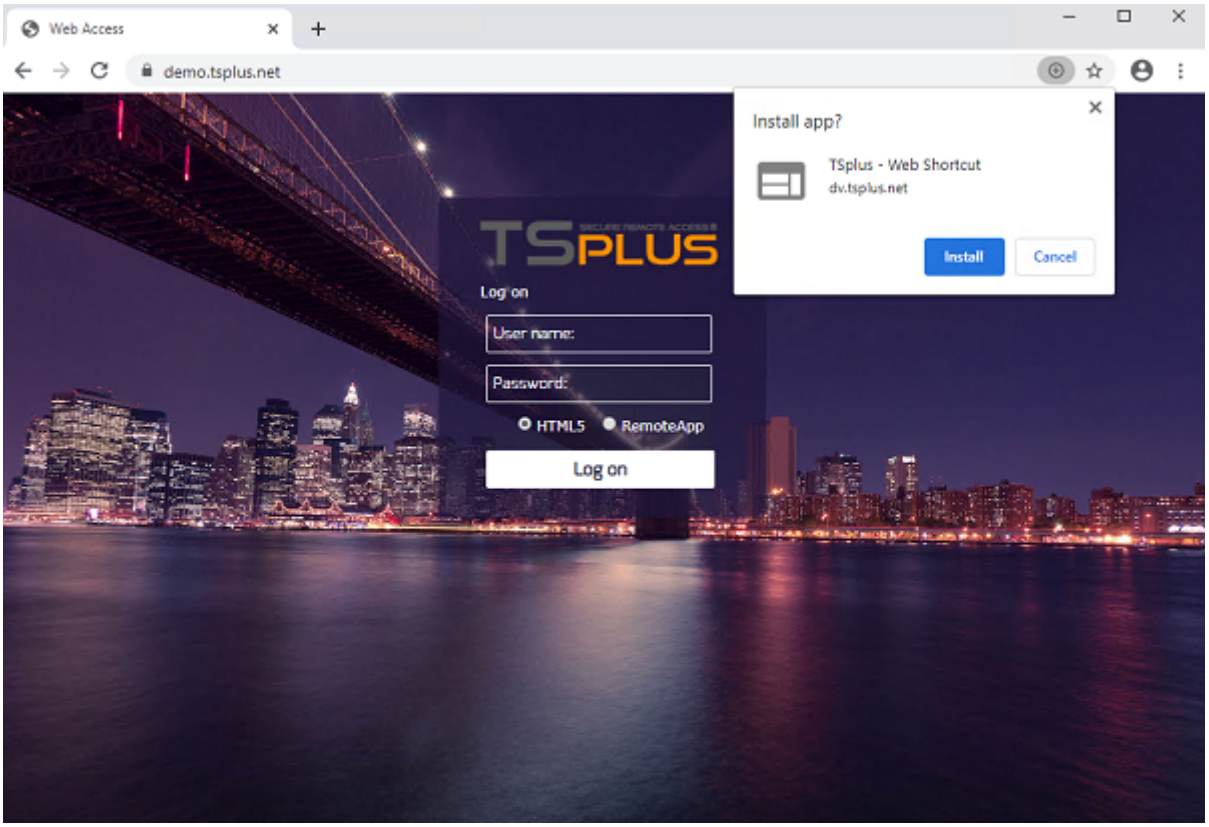
La nueva WebApp de TSplus ofrece un rendimiento y un valor mejorados utilizando las siguientes mejoras en comparación con las aplicaciones y clientes de conexión heredados:

- Tiempos de carga más rápidos debido a la pequeña huella de software.
- Menor uso de datos - TSplus Web App aprovecha la gestión de tráfico basada en navegadores comunes para minimizar el uso de datos.
- Experiencia de usuario sin interrupciones: desde la pantalla de inicio de sesión hasta la representación de la aplicación, TSplus WebApp ofrece al usuario la apariencia de uso de una aplicación nativa.
- No más pestañas del navegador o sesiones perdidas debido a demasiadas ventanas del navegador abiertas. El comportamiento de la aplicación web de TSplus ofrece las mismas opciones de multitarea que cualquier otra aplicación de alto nivel.

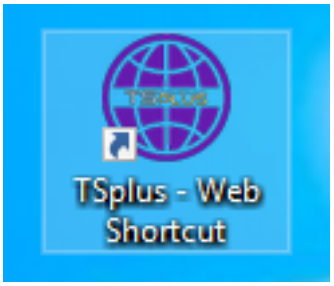
Instalación - PC

Navegue a su portal web corporativo de TSplus utilizando su navegador web común preferido (se requiere configuración HTTPS).
Para usar en Firefox, necesitarás instalar el PWAS complemento.

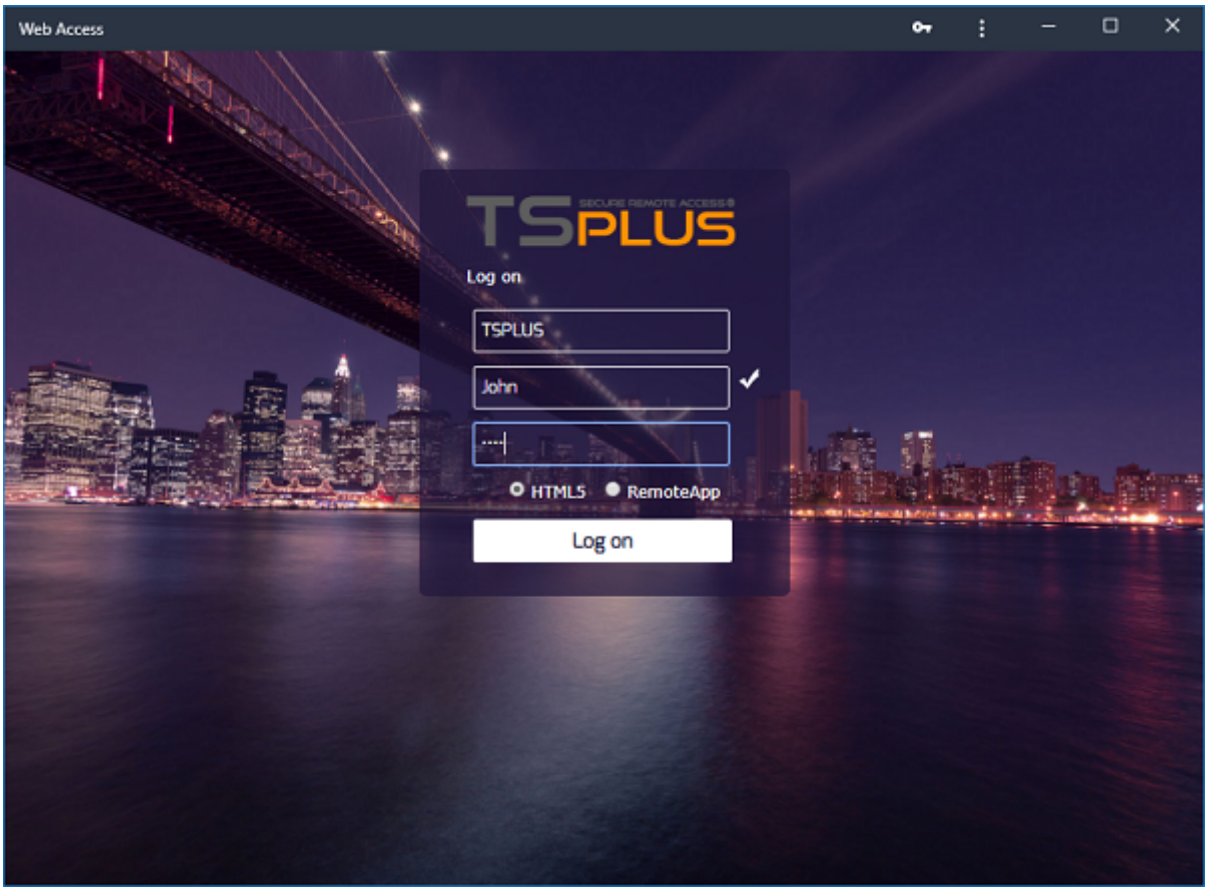
Haz clic en el botón + ubicado en el lado derecho de la barra de navegación. Cuando se te solicite, haz clic en 'Instalar'.



La instalación solo toma un segundo. Creará un ícono en su escritorio:



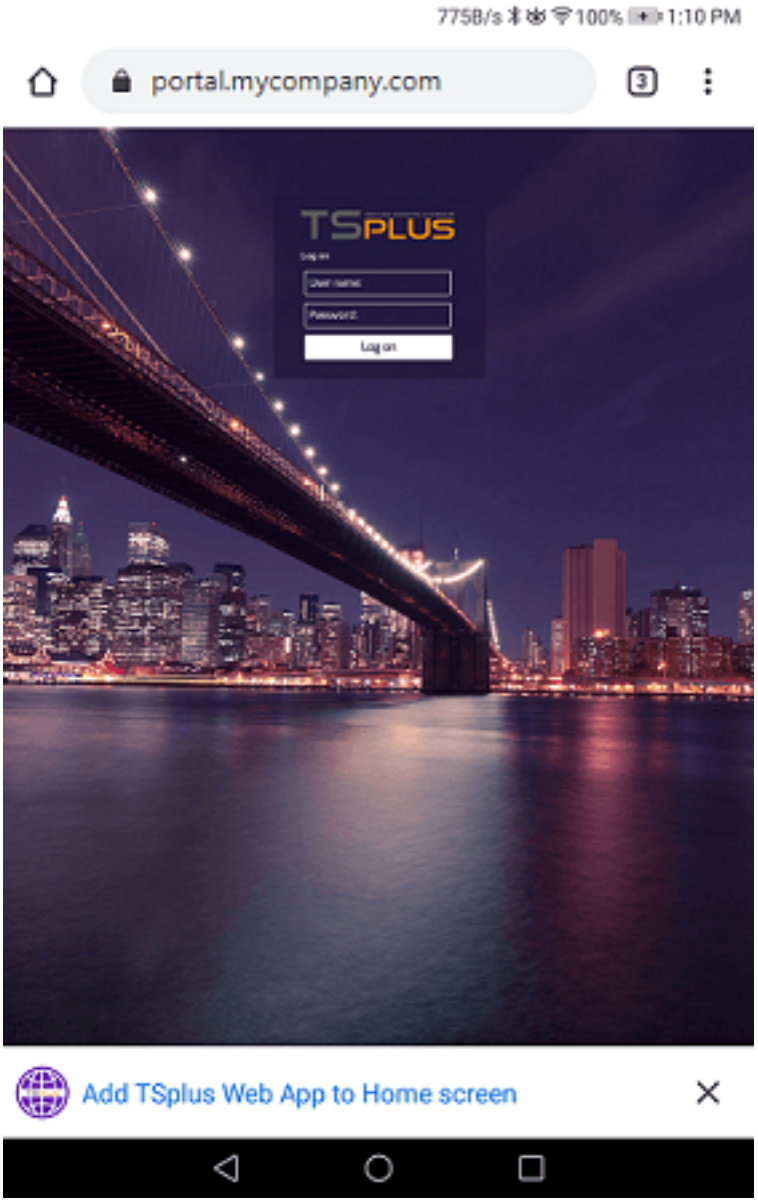
Y la aplicación web se abrirá inmediatamente al finalizar:



Instalación - Dispositivo Móvil Android

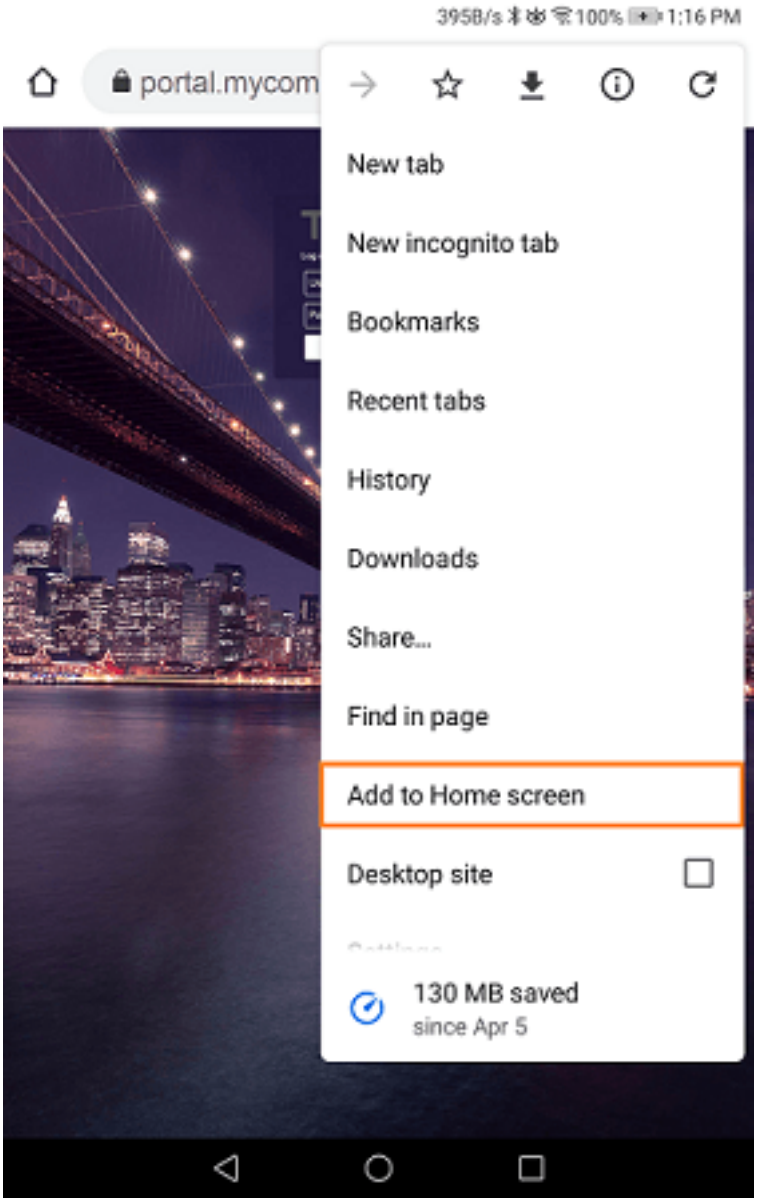
Navegue a su portal web corporativo de TSplus utilizando su navegador web móvil común preferido. **El protocolo HTTPS es necesario en el servidor TSplus.**

El Portal Web ofrecerá la opción de agregar la aplicación web de TSplus a la pantalla de inicio, haciendo clic en el mensaje "Agregar la aplicación web de TSplus a la pantalla de inicio" en la parte inferior de la ventana.

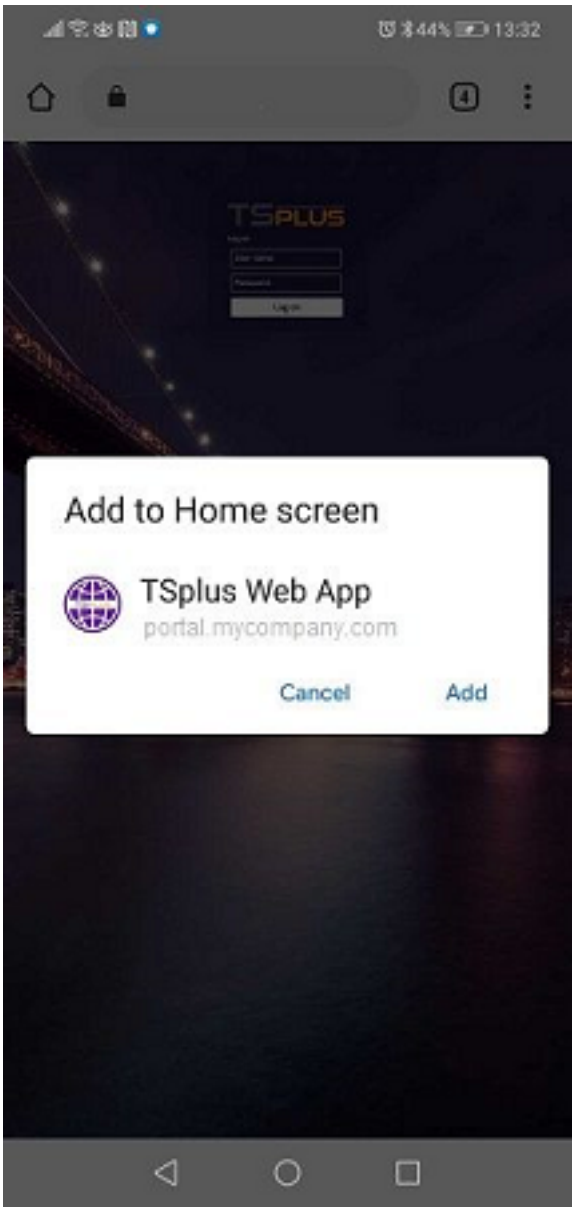


O haciendo clic en el menú de 3 puntos en la parte superior derecha de la ventana y haciendo clic en "Agregar"

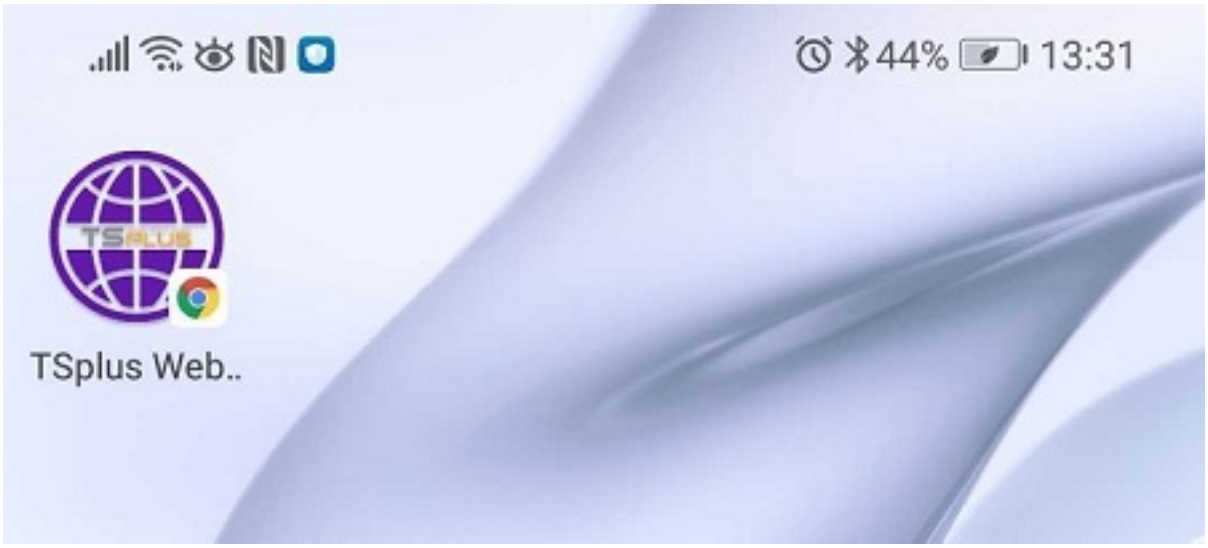
Después de aceptar la opción Agregar a la pantalla de inicio, el usuario verá la siguiente pantalla:



Toque el botón 'Agregar' y el proceso está completo:

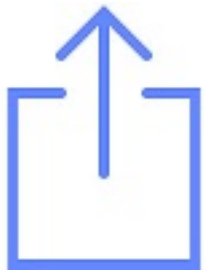


La aplicación web de TSplus ahora será accesible directamente desde la pantalla de inicio de su dispositivo móvil.



Instalación - Móviles Apple iOS

El proceso de instalación de la aplicación web en iOS es similar al proceso de Android. Simplemente navega al Portal Web de TSplus utilizando el navegador Safari. Haz clic en el botón Compartir:

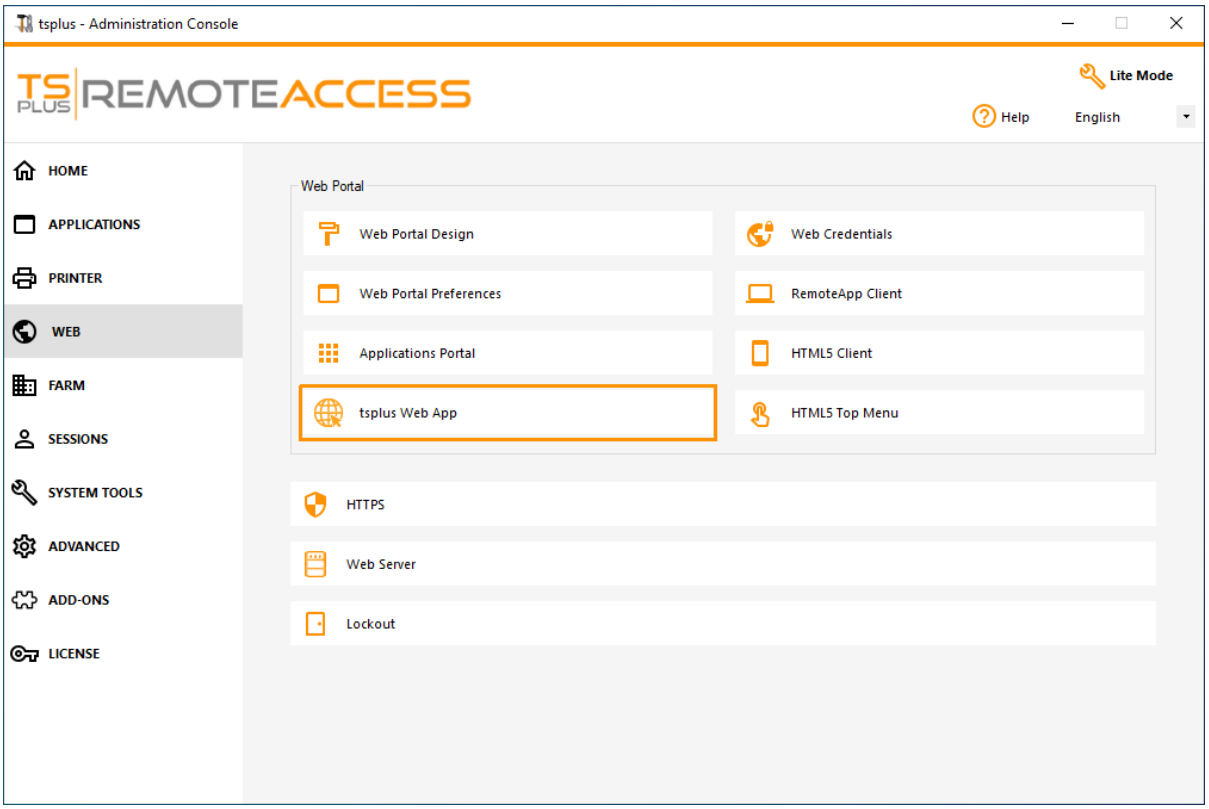


Luego haga clic en "Agregar a la pantalla de inicio".

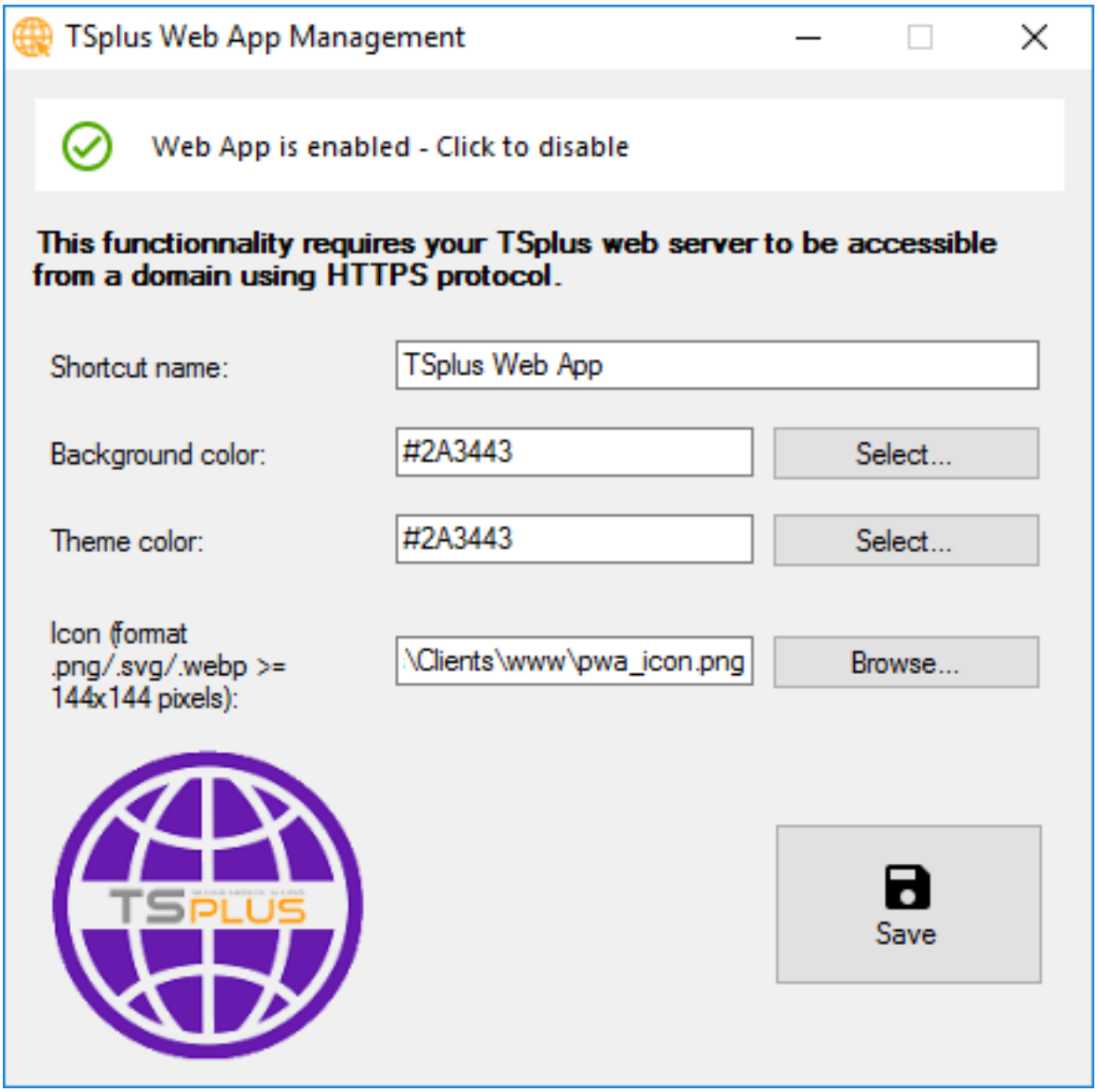
Nota: El navegador Chrome no admite la función de la aplicación web en iOS.

Gestión

Puedes gestionar la aplicación web yendo a la sección Portal Web de la herramienta de administración de TSplus y haciendo clic en el mosaico de la aplicación web de TSplus:



La aplicación web está habilitada por defecto, pero puedes desactivarla. Es posible modificar el nombre del acceso directo, el fondo y los colores del tema, así como el ícono de TSplus Web App.



Solo haz clic en "Guardar" para registrar tus modificaciones.

Portal de Aplicaciones Web: Parámetros en la dirección URL

Si desea omitir la página de acceso web de inicio de sesión estándar de Terminal Service Plus al usar el Portal de Aplicaciones Web y vaya directamente a la página del Portal de Aplicaciones Web, debe especificar varios parámetros en la dirección URL:

- inicio de sesión de usuario
- contraseña de usuario
- dominio de usuario
- servidor
- puerto
- tipo de cliente (HTML5 o Windows)

Aquí hay un ejemplo de una dirección URL completa para el usuario "demo" con la contraseña "demo" en nuestro servidor de demostración con un cliente HTML5:

https://demo.tsplus.net/index_applications.html?user=demo&pwd=demo&domain=&server=127.0.0.1&port=3389&type=html5

El dominio, el servidor, el puerto y los parámetros de tipo son opcionales, la siguiente dirección URL tiene exactamente el mismo comportamiento:

https://demo.tsplus.net/index_applications.html?user=demo&pwd=demo

Para usar un cliente de Windows, utiliza:

&type=acceso remoto

Usando esos parámetros en la dirección URL, puedes ir directamente a la página del Portal de Aplicaciones Web.

No es necesario especificar todos estos parámetros al mismo tiempo: los parámetros no especificados tendrán su valor configurado por defecto.

Si desea omitir el inicio de sesión estándar de Terminal Service Plus al usar la conexión con el cliente HTML5, marque esta página .

Portal de Aplicaciones Web

El portal de aplicaciones web de Terminal Service Plus proporciona una solución única y flexible que puede optimizar la implementación de aplicaciones y escritorios, así como la gestión del ciclo de vida para reducir los costos de TI. Al gestionar de manera centralizada y entregar aplicaciones bajo demanda a través de la web, TI puede mejorar la tasa de éxito de la implementación de aplicaciones, proporcionando gestión basada en roles, control de aplicaciones, seguridad y soporte a los usuarios.

Terminal Service Plus Web Application Portal virtualiza y transforma aplicaciones y escritorios de Windows en un servicio seguro bajo demanda.

Con el Portal de Aplicaciones Web, podrá publicar aplicaciones de Microsoft Windows (aplicaciones empresariales, aplicaciones de Office…) en la web.

Al igual que en Citrix, sus usuarios pueden acceder a sus aplicaciones directamente desde Internet, simplemente haciendo clic en el icono de la aplicación en la página web del Portal, directamente dentro de su propio navegador de Internet.

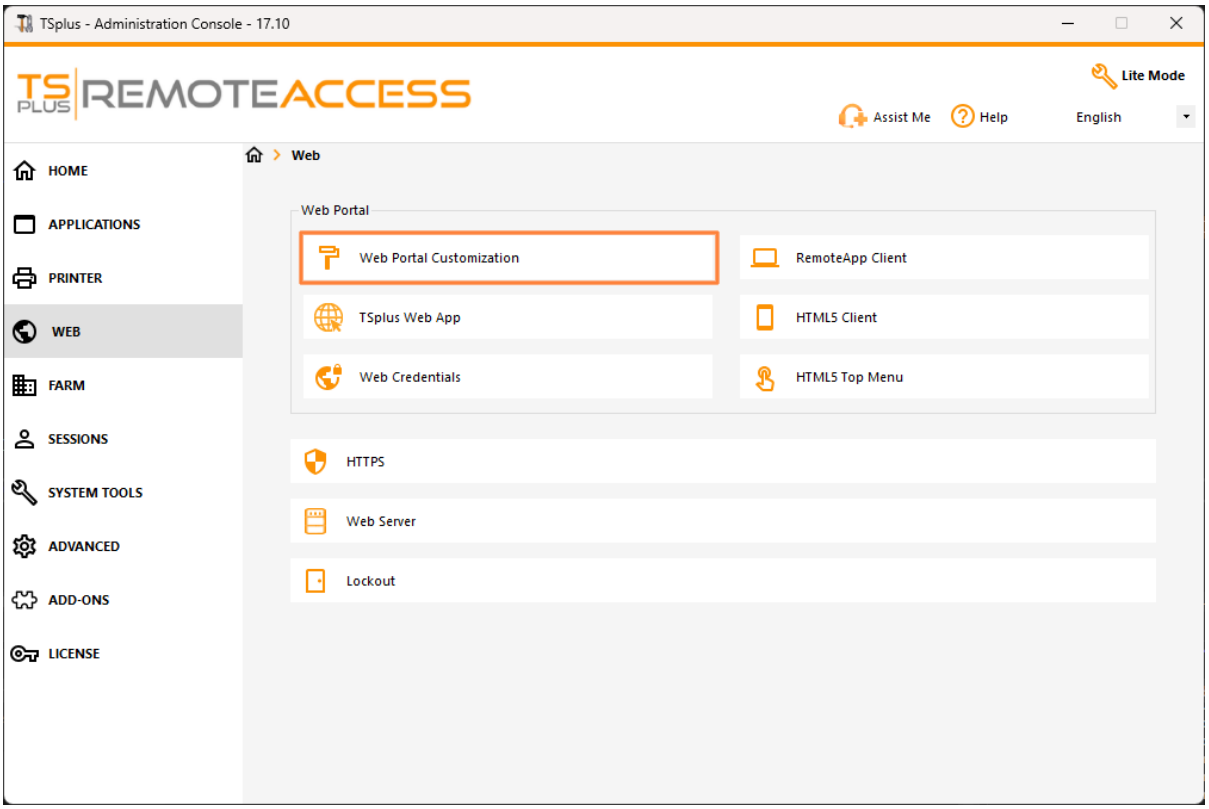
Gestionando tus Aplicaciones Web

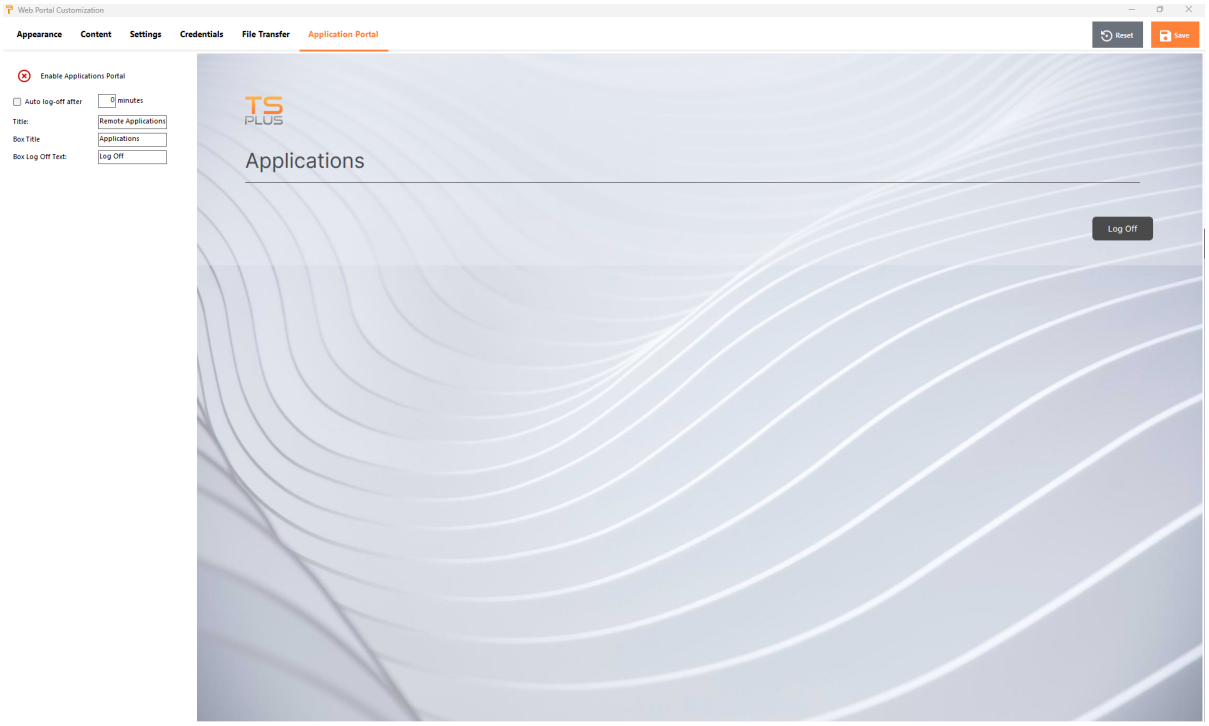
La función del Portal de Aplicaciones Web es **totalmente integrado** en Terminal Service Plus. Esto significa que todas las aplicaciones publicadas por la función de Publicación de Aplicaciones de Terminal Service Plus se pueden utilizar en el Portal de Aplicaciones Web.

Si desea saber más sobre este proceso de publicación, no dude en leer nuestra documentación sobre Publicación de Aplicaciones y Asignación de aplicaciones a usuarios o grupos .

Diseñando su Portal de Aplicaciones Web

En la herramienta de administración, abre la pestaña "Web" y haz clic en el mosaico "Personalización del portal web" y ve al mosaico "Portal de aplicaciones".





Para generar una página de acceso web con la función del Portal de Aplicaciones Web activada, **marque la casilla "Habilitar Portal de Aplicaciones".** Puedes personalizar tu página de acceso web a tu gusto, luego haz clic en "Guardar" para publicar esta nueva página de acceso web.

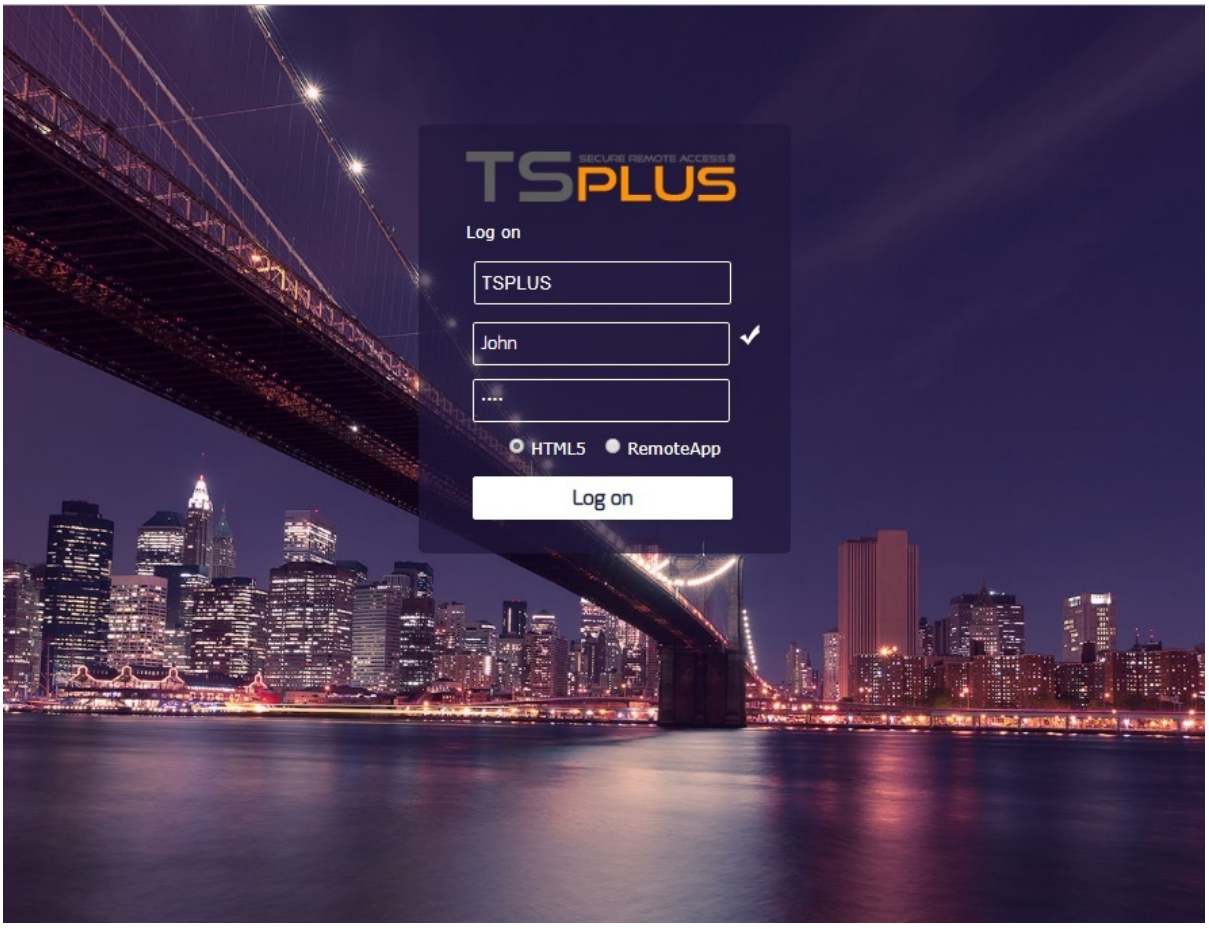
Nota: Solo puedes cambiar los colores de la caja y del borde de la caja para los temas Clásicos, que se pueden cambiar en el Pestaña de apariencia .

Usando el Portal de Aplicaciones Web

En este ejemplo hemos publicado la nueva página de acceso web con el nombre predeterminado "index".

Para acceder, abra un navegador web y vaya a http://your_server_name/ (en este ejemplo usamos http://localhost , directamente desde el servidor mismo).

La primera página web que se muestra es la página de inicio de sesión estándar de Terminal Service Plus:

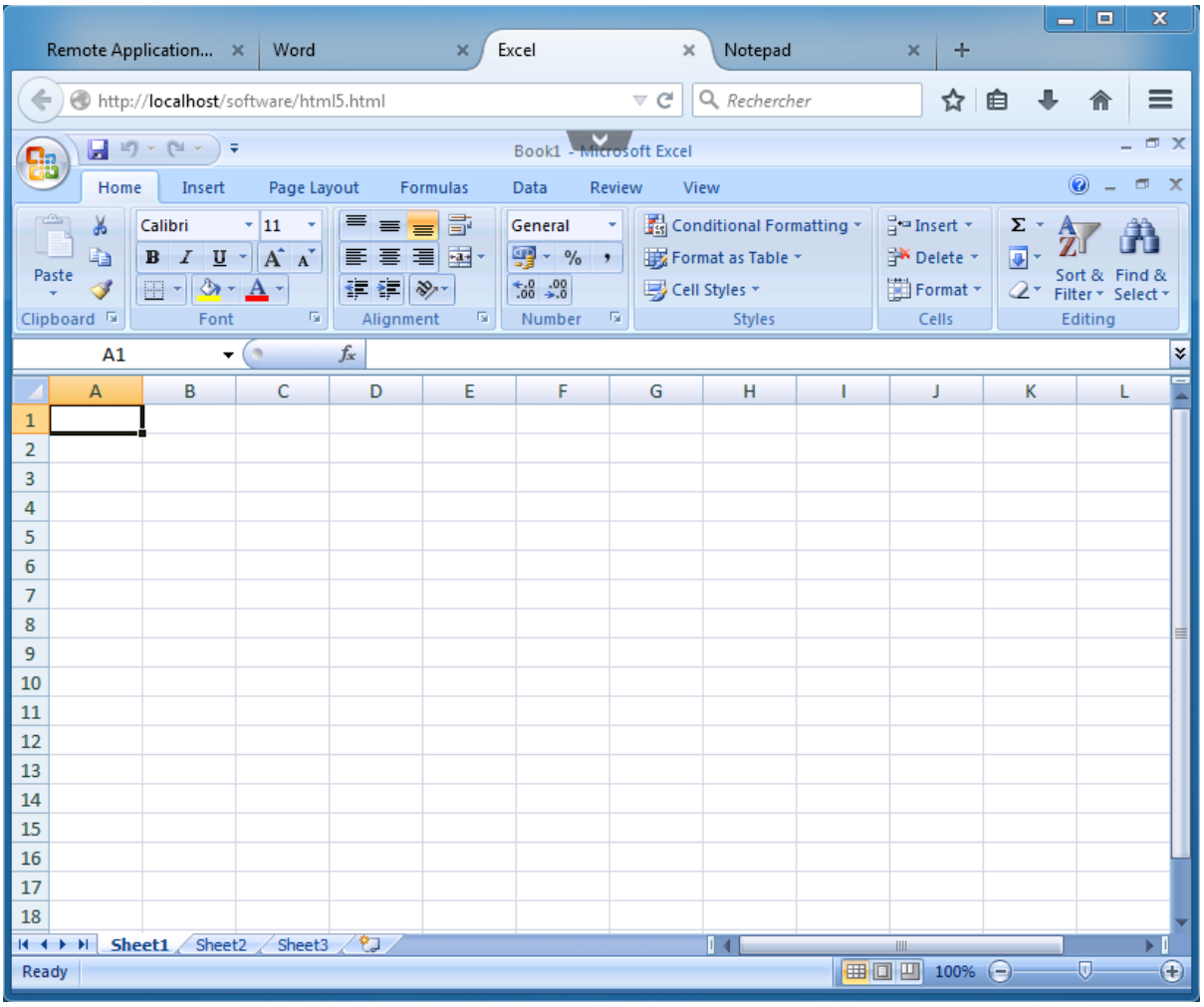


Una vez que inicie sesión, se mostrará una nueva página web, este es el Portal de Aplicaciones Web:

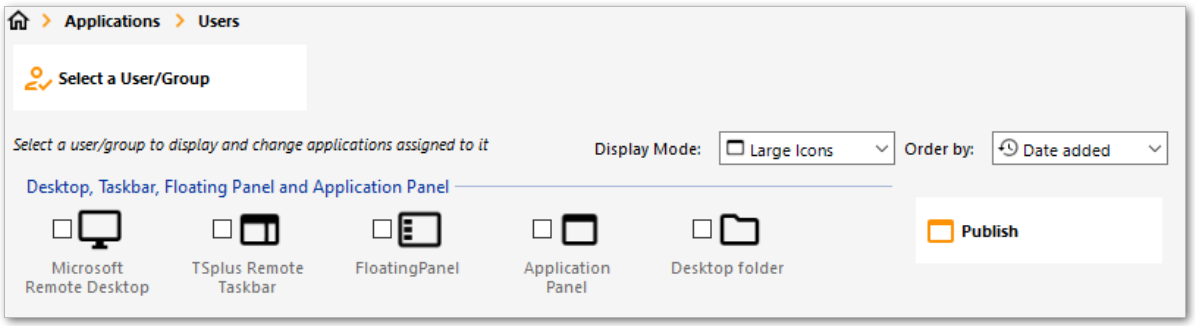


Como puedes ver, el usuario obtiene un ícono por cada aplicación publicada a la que tiene acceso.

El usuario ahora puede hacer clic en uno o más íconos para abrir remotamente la aplicación correspondiente en una nueva pestaña:

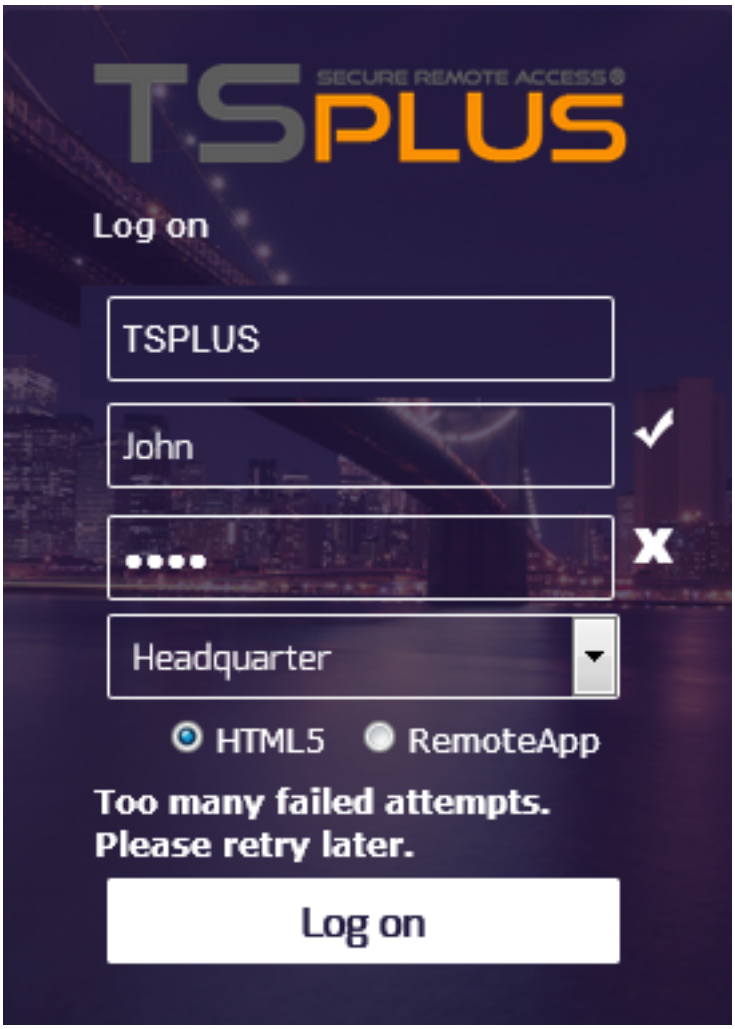


Si desea utilizar solo el portal de aplicaciones sin abrir una sesión de Windows, barra de tareas remota, panel flotante,…, debe desmarcar todas las casillas asociadas con el perfil de usuario.



Desde el lanzamiento de TSplus 11.40, los ataques de fuerza bruta en el Portal Web ahora están bloqueados cuando los usuarios ingresan credenciales incorrectas.

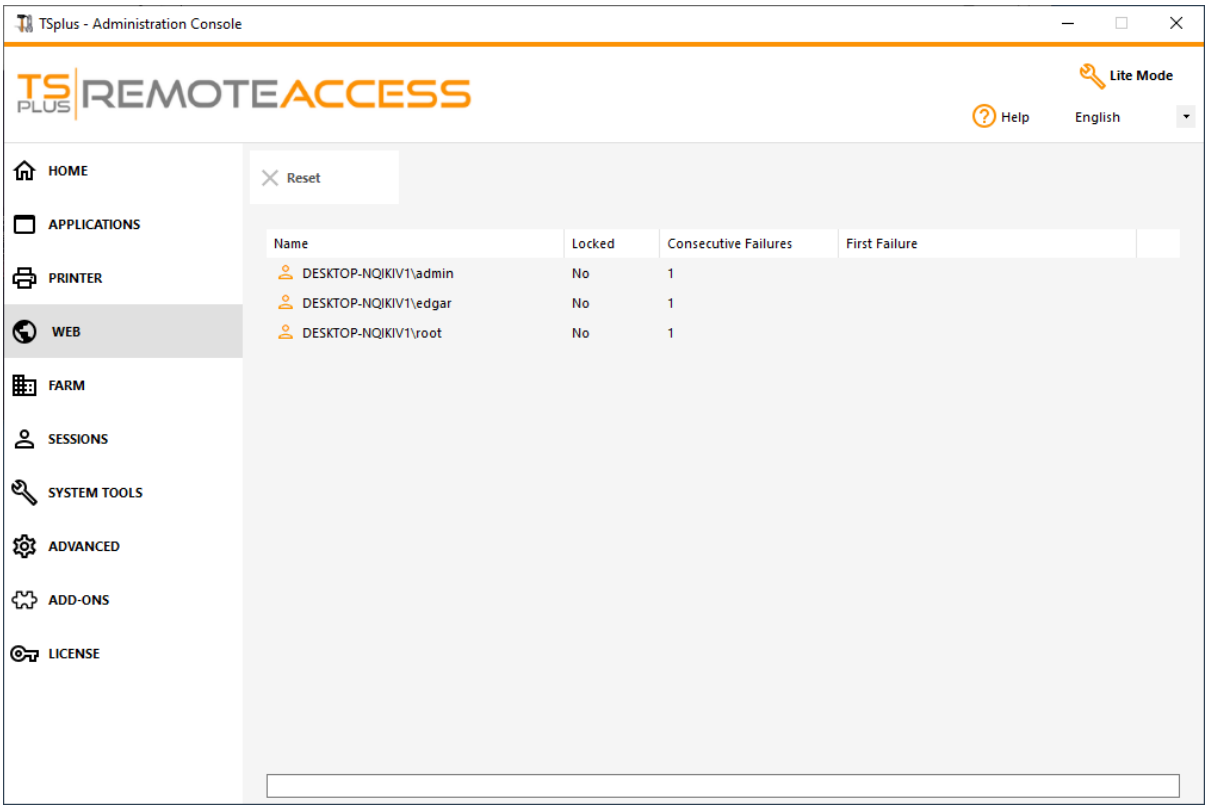
Después de 10 intentos durante un período de 15 minutos, el Portal Web prohibirá al usuario iniciar sesión durante 30 minutos (personalizable en el Advanced - Pestaña de bloqueo de AdminTool) :



Estos son los ajustes predeterminados que se pueden personalizar en el archivo hb.exe.config ubicado en la carpeta de TSplus:

TSplus\Clients\www\cgi-bin\hb.exe.config en el párrafo "appSettings".

Puedes verificar todas las conexiones bloqueadas y los registros de usuarios en la función de bloqueo de TSplus:



Esta funcionalidad es visible y activo después de la primera conexión al Portal Web.

Notas Importantes

- La función del Portal de Aplicaciones Web es compatible con Configuración de granja / puerta de enlace y también admite balanceo de carga .
- En una configuración de Granja / Gateway, las Aplicaciones deben ser publicadas y asignadas en cada servidor de la granja en ese momento.
- En términos de licencias de Terminal Service Plus, un usuario puede abrir varias aplicaciones al mismo tiempo sin contar como más de 1 usuario.

Autologon web: conéctese desde la web sin portal

Resumen

El portal web de Terminal Service Plus permite a los usuarios conectarse a sus servidores remotos desde cualquier navegador web simplemente utilizando sus credenciales de Windows.

A veces, sin embargo, deseas conectarte automáticamente al iniciar una dirección URL determinada. Esta función se llama Autologon Web.

Con Web Autologon, te conectarás utilizando los ajustes (inicio de sesión, contraseña, puertos, …) especificados en archivos específicos de Terminal Service Plus.

Precaución

Al utilizar esta función, su nombre de usuario y contraseña pueden estar expuestos a cualquier persona que visite la página.

Además, si todos sus usuarios comparten el mismo nombre de usuario, puede ser posible que los usuarios vean información sensible de otros usuarios que comparten el mismo nombre de usuario.

Esta función está destinada a casos de uso específicos únicamente y no se recomienda.

Autologon web utilizando cliente HTML5

Podrás conectarte directamente navegando a http://tu-servidor/software/html5.html

Puedes modificar la configuración de la conexión editando el siguiente archivo con Notepad o cualquier editor de texto (como Notepad++ - no uses MS Word):

C:\Program Files (x86)\TSplus\Clients\www\software\html5\settings.js

Deberá especificar al menos un nombre de usuario y una contraseña para beneficiarse de Web

Autologon.

Es posible que necesite actualizar la página en su navegador web después de modificar este archivo.

Autologon web utilizando el cliente web RemoteApp

Podrás conectarte directamente navegando a http://your-server/software/remoteapp2.html

Puedes modificar la configuración de la conexión editando el siguiente archivo con Notepad o cualquier editor de texto (como Notepad++ - no uses MS Word):

C:\Program Files (x86)\TSplus\Clients\www\software\remoteapp2.js

Deberá especificar al menos un nombre de usuario y una contraseña para beneficiarse de Web Autologon.

Es posible que necesite actualizar la página en su navegador web después de modificar este archivo.

Habilitar múltiples sesiones de usuario utilizando las mismas credenciales

Si desea habilitar múltiples sesiones de usuario utilizando las mismas credenciales, puede seguir este procedimiento.

Puedes copiar el archivo index.html ubicado en:

C:\Program Files (x86)\TSplus\Clients\www

tantas veces como tu número de usuarios. Puedes renombrarlo y luego acceder a él con la url: http://nameofyourserver.com/renamedindex.html

Edita el párrafo correspondiente a las credenciales de los usuarios:

Configuración de Acceso ---------- var user = ""; // Inicio de sesión a utilizar al conectarse al servidor remoto (dejar "" para usar el inicio de sesión escrito en esta página) var pass = ""; // Contraseña a utilizar al conectarse al servidor remoto (dejar "" para usar la contraseña escrita en esta página) var domain = "";

Puedes copiar el archivo index.html tantas veces como desees, renombrarlo con el nombre de usuario facilitará que proporciones un enlace personal.

Credenciales Web

Resumen

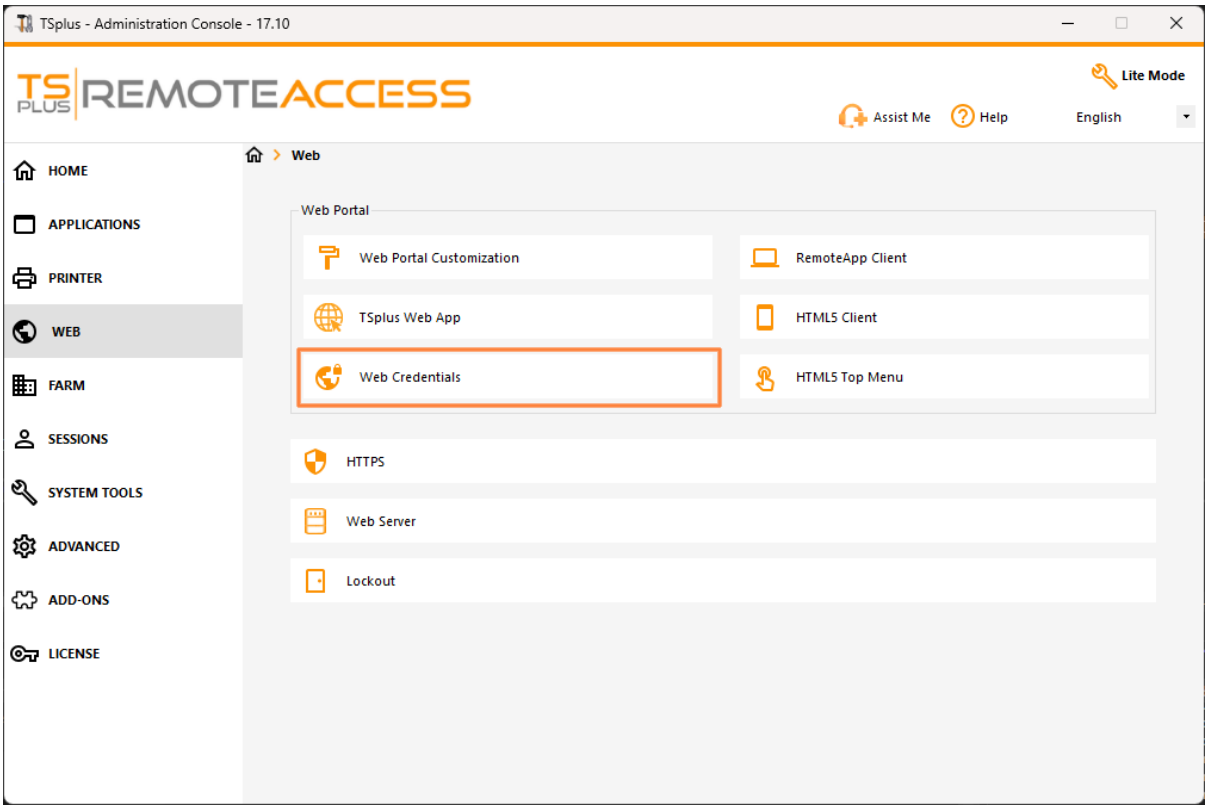
Las credenciales web de Terminal Service Plus son una característica única y de vanguardia, que permite a los usuarios conectarse solo con una dirección de correo electrónico o un código PIN.

Con Web Credentials, puedes asegurar el acceso a tu servidor con la dirección de correo electrónico de un usuario, o con un simple código PIN generado por tu aplicación empresarial. Uno de los grandes beneficios de esta función es que estas credenciales (correo electrónico o código PIN) son credenciales puras de la web: el usuario no conocerá la cuenta de usuario de Windows que está utilizando actualmente, y no necesita conocer un inicio de sesión/contraseña de Windows real para conectarse a su aplicación.

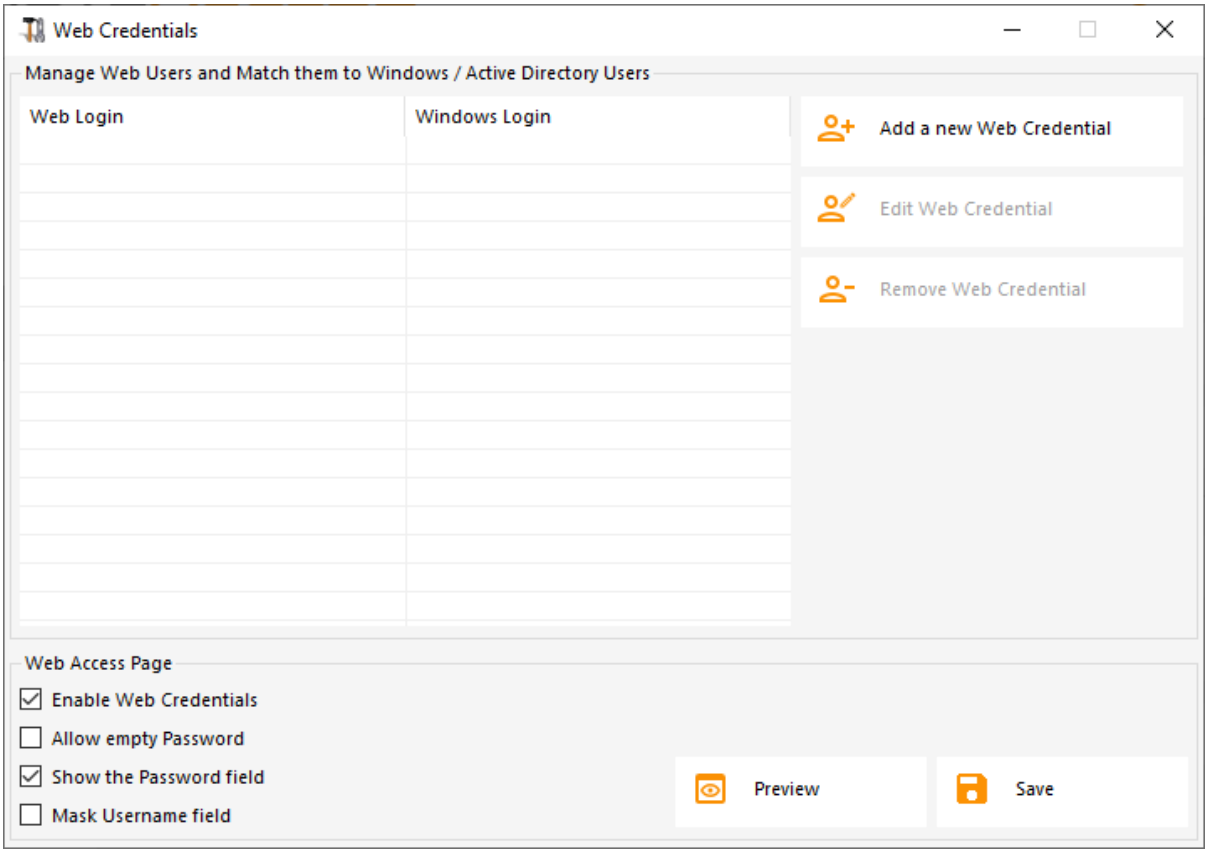
Con Web Credentials, podrá definir credenciales web personalizadas y asociarlas a cualquier cuenta de usuario existente de Windows / Active Directory. El usuario podrá conectarse utilizando estas credenciales personalizadas, en lugar de las de Windows / Active Directory.

Gestionando sus credenciales web

En la herramienta de administración, abre la pestaña "Web" y haz clic en el mosaico "Credenciales web".

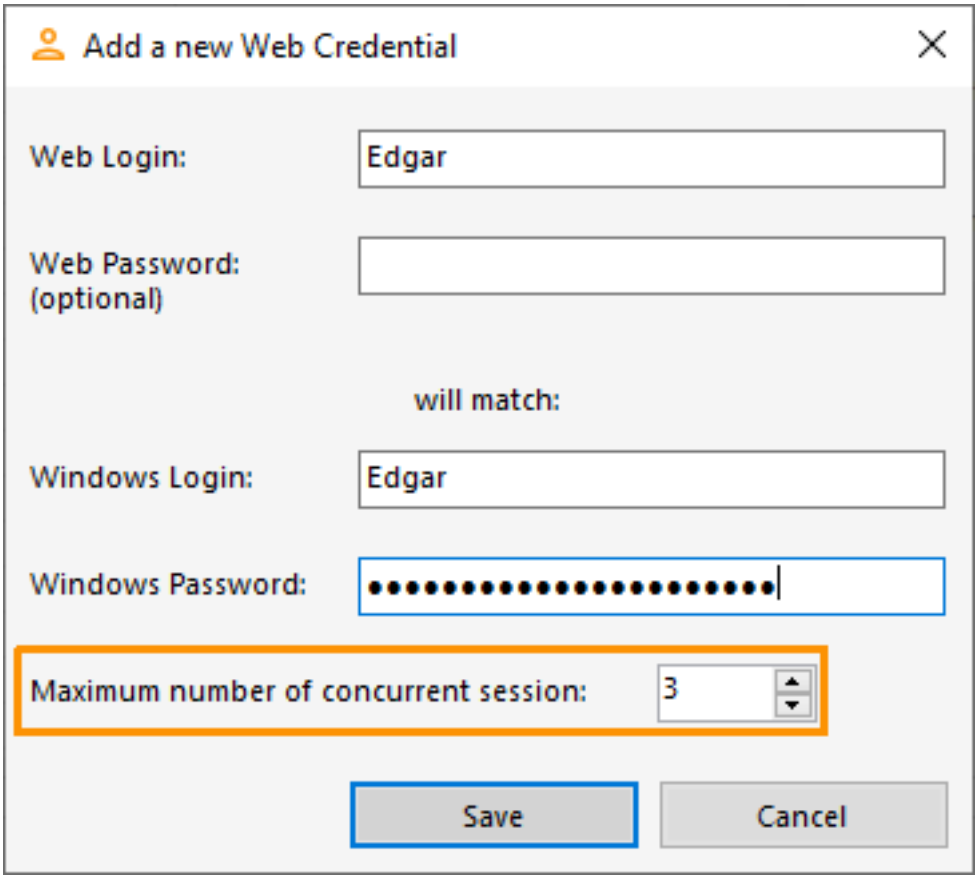


El Administrador de Credenciales Web se abrirá y mostrará esta ventana:



Ahora puede crear una nueva Credencial Web emparejando un inicio de sesión personalizado y una contraseña (opcional) con una cuenta de usuario de Windows / Active Directory existente,

como se muestra a continuación:



Desde la versión 9.50 de TSplus, también puedes decidir el número máximo de sesiones concurrentes para un usuario.

También puedes editar y eliminar una Credencial Web existente, cambiando o deshabilitando cualquier credencial personalizada que hayas configurado.

Alternativamente, puede crear credenciales web a través de una línea de comandos:

- En el menú de inicio de Windows, en el campo de ejecución, escribe: 'cmd.exe' (o en Programas/Accesorios > 'Windows Power Shell')
- Luego, para ir a la carpeta correcta, escribe: cd “C:\Program Files (x86)\TSplus\UserDesktop\files”, luego presiona Enter para validar
- Para agregar una nueva Credencial Web, escribe: AdminTool.exe /webcredentials-add tu_login_web tu_contraseña_web tu_login_windows tu_contraseña_windows sesiones_concurrentes_máximas
- Para agregar una credencial en blanco, escribe dos comillas dobles: "" para indicar un texto en blanco.
- Para eliminar una credencial web, escribe: AdminTool.exe /webcredentials-remove tu_login_web

si te gusta usar líneas de comando y te preguntas qué otras líneas de comando están disponibles, por favor ve a este documentación específica)

Notas Importantes

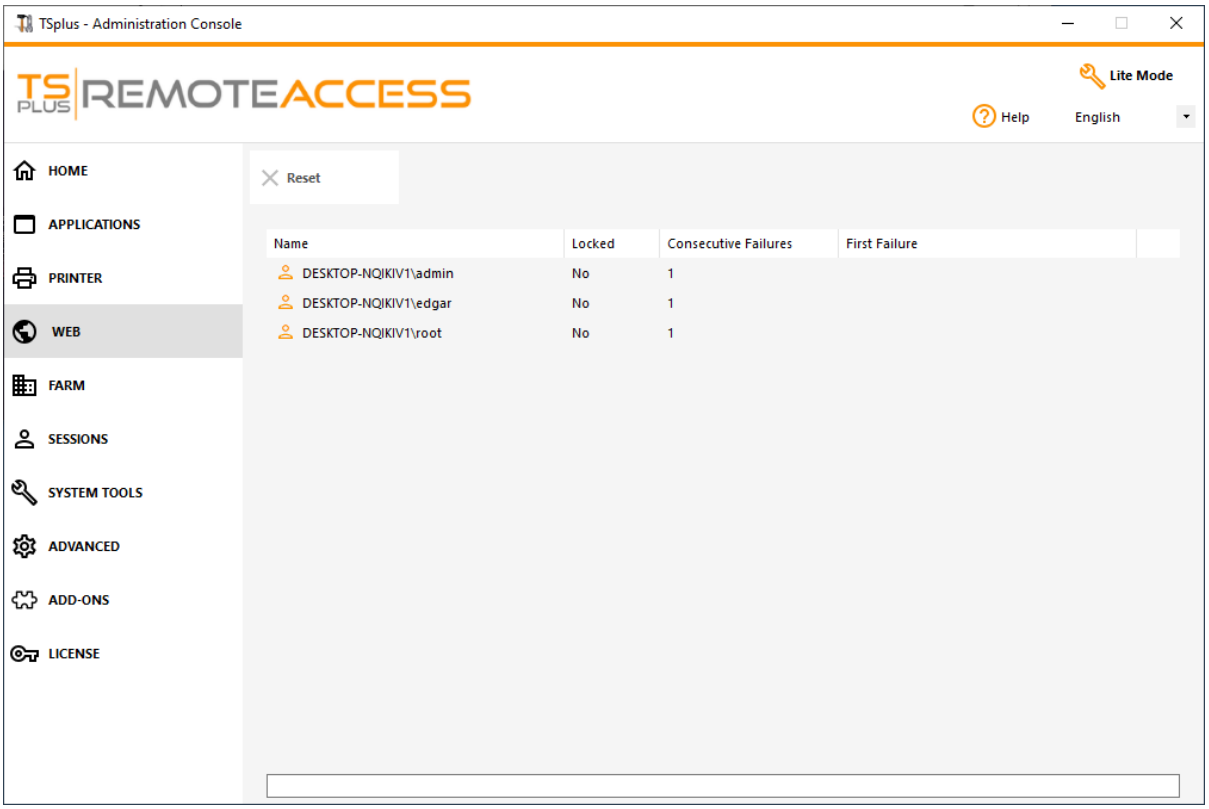
Por favor, tenga en cuenta las siguientes limitaciones:

- Los caracteres '[', ']' y '°' no son compatibles en los campos de contraseña.
- En un Configuración de granja / puerta de enlace Las credenciales web solo son compatibles con el modo de balanceo de carga (no funciona con el modo asignado por el servidor).
- En una configuración de Granja / Gateway con modo de balanceo de carga, las Credenciales Web deben definirse en cada servidor de la granja en ese momento.
- 2FA no es compatible con la función de Credenciales Web.

Bloqueo Web

TSplus Web lockout, introducido con la Versión 12.40, es una interfaz de usuario para la función de bloqueo del Portal Web, para desbloquear cuentas y editar configuraciones avanzadas:

FAQ: sobre cómo configurar la función de bloqueo del Portal Web HTML5

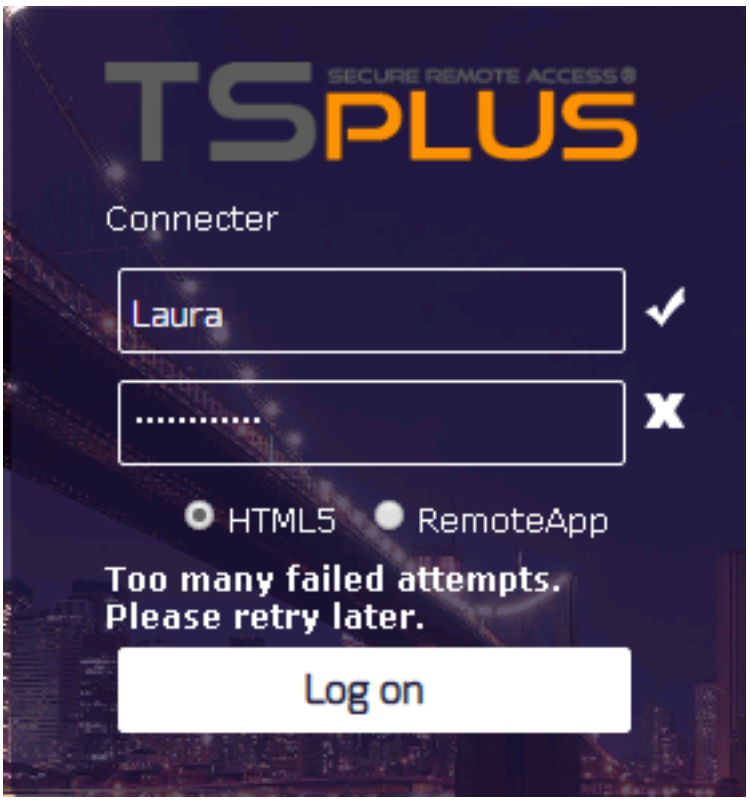


Monitores de bloqueo los intentos de inicio de sesión web fallidos en su servidor TSplus. Registra los intentos y bloquea automáticamente al usuario correspondiente después de que se ha alcanzado el número autorizado de intentos fallidos.

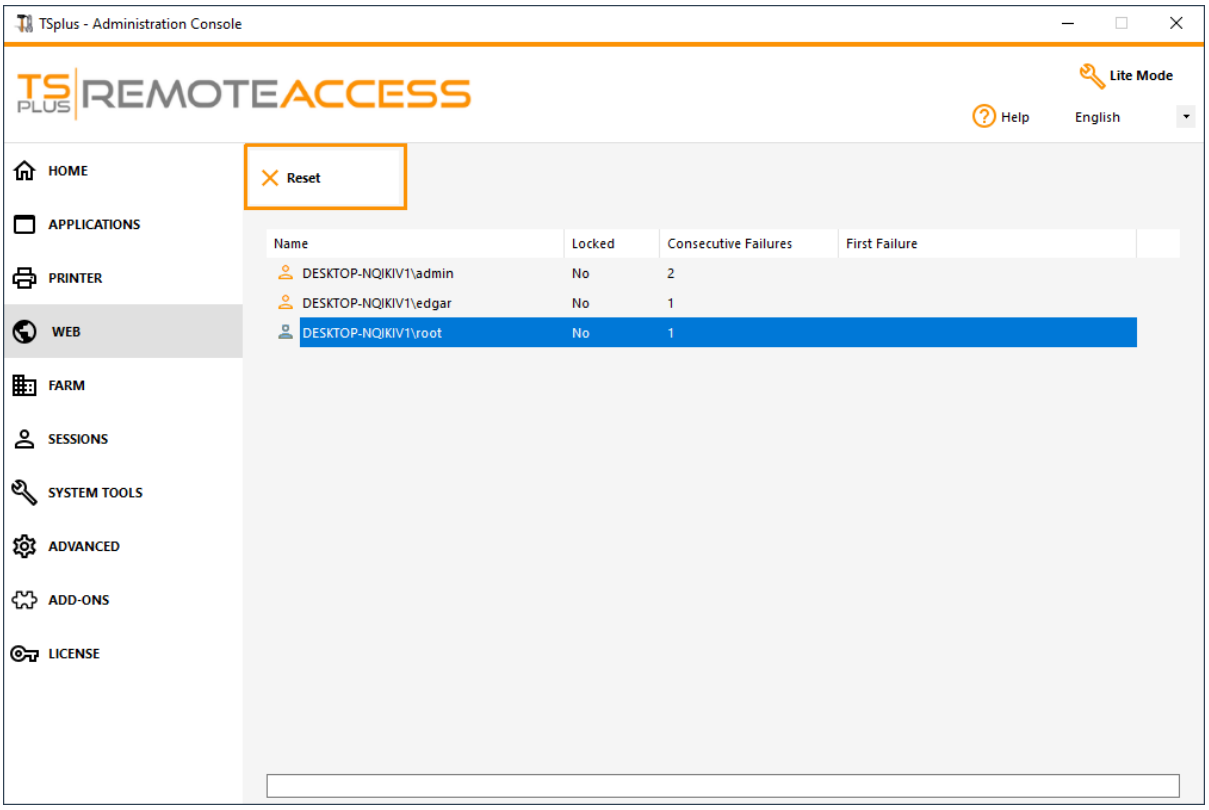
Podrás ver fácilmente si una dirección ha sido bloqueada en la columna "Bloqueado".

La siguiente columna indica el número de fallos consecutivos para cada usuario.

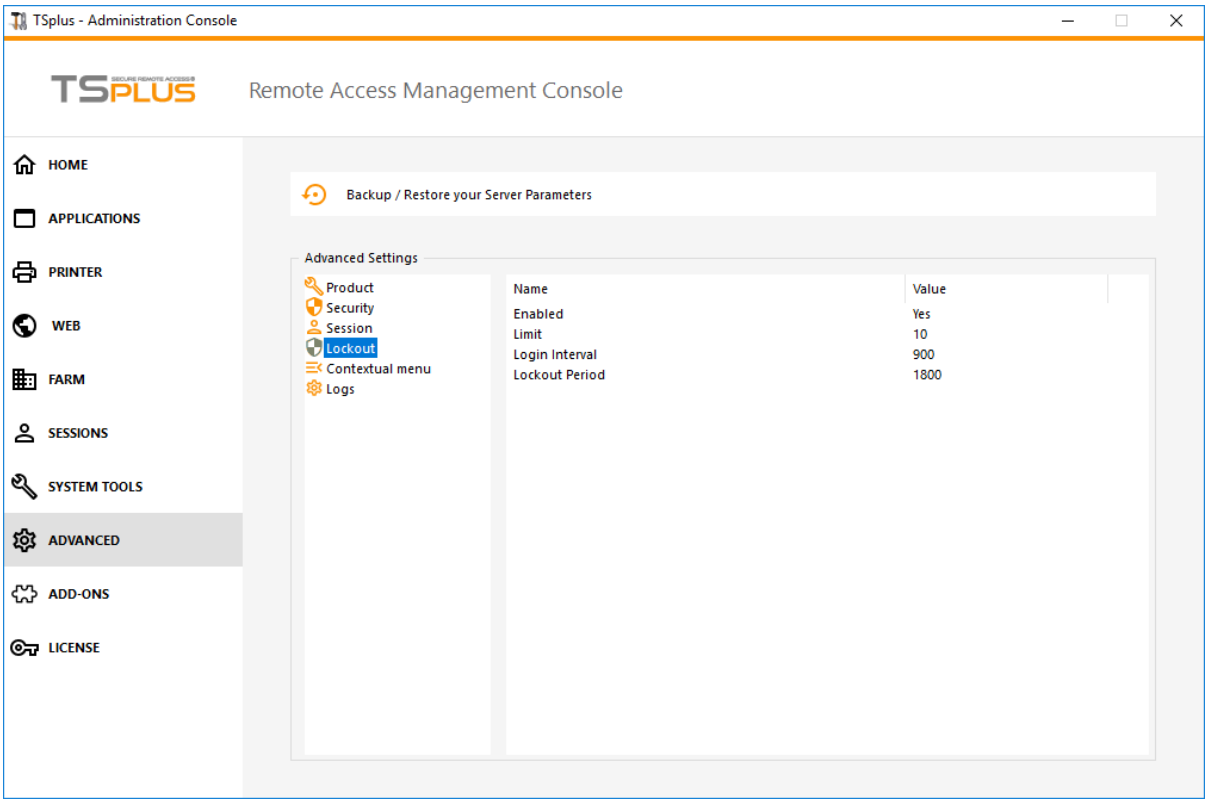
En el Portal Web, un mensaje indica al usuario que se realizaron demasiados intentos fallidos.



Los usuarios pueden ser eliminados rápidamente de esta lista, desbloqueados y añadidos a la lista blanca desde la consola de gestión fácil de usar en la pestaña Web de AdminTool. Simplemente haga clic en el usuario que desea restablecer o desbloquear y luego haga clic en "Restablecer".



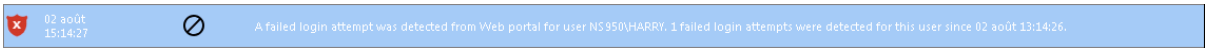
El umbral para el bloqueo de usuarios puede ser configurado por el administrador, en la pestaña de Configuración Avanzada de la AdminTool:



Verifique la documentación para configurar la configuración de bloqueo.

Integración de TSplus Advanced Security con bloqueo

Si se ha detectado un intento de inicio de sesión fallido en el Portal Web, TSplus Advanced Security indicará el **Evento de bloqueo, correspondiente a un nombre de usuario en el Visor de eventos de seguridad** :



Se detectó un intento de inicio de sesión fallido desde el Portal Web para el usuario … Se detectó 1 intento de inicio de sesión fallido para este usuario desde…

TSplus Advanced Security Protección contra BruteForce

TSplus Advanced Security Protección contra ataques de fuerza bruta cubre el **Aspecto de direcciones IP del cliente** Por lo tanto, también funciona para conexiones RDP.

Intentos fallidos de conexiones por fuerza bruta , también son visibles en el registro de eventos de TSplus Advanced Security (se excluyen las direcciones IP privadas para evitar el bloqueo de proxies):



“Se detectó un intento de conexión fallido desde la dirección IP … . Esta dirección IP no está en la lista blanca y será bloqueada tras varios intentos fallidos de conexión. Nombre de usuario proporcionado: Harry.”

Para más información sobre la protección contra bloqueos y BruteForce, consulte esta documentación y el Documentación de Protección contra Fuerza Bruta

Página de inicio de sesión web: Cómo cambiar la pantalla de inicio de sesión

Resumen

Cuando se está cargando la conexión remota, el cliente HTML5 muestra una pantalla de presentación predeterminada como la captura de pantalla a continuación:



Puedes personalizar este contenido modificando un archivo de configuración de JavaScript.

Cliente HTML5

Creando el contenido de su Splashscreen personalizado

Cualquier contenido en texto o HTML se puede utilizar para la pantalla de presentación.

Además, si necesitas usar comillas simples (’) o comillas dobles (”) tendrás que escribir una barra invertida antes de (’ y ”) en lugar de solo las comillas.

Finalmente, tenga en cuenta que el contenido debe escribirse en una sola línea.

El siguiente ejemplo es un contenido válido para la pantalla de presentación:

Esta es mi pantalla de inicio personalizada

¡Por favor, di "hola"!
Se mostrará un título (“Este es mi splashscreen personalizado”), un texto (“¡Por favor, di hola!”) y la imagen del anillo animado como en el splashscreen estándar de TSplus.

Modificando los datos de la pantalla de inicio para usar su propio contenido

Si no tiene un archivo llamado “settings.js” en la carpeta “C:\Program Files (x86)\TSplus\Clients\www\software\html5”, entonces su versión de TSplus es más antigua y esta documentación no se aplica. Por favor, actualice su sistema primero o contacte con el soporte.

Edita el archivo “settings.js” ubicado en la carpeta “C:\Program Files (x86)\TSplus\Clients\www\software\html5”. Te aconsejamos que uses un editor de texto como Notepad o Notepad++. no usa Word).

Busca la línea que comienza con esto:

W.splashscreencontent = ”

Reemplázalo completamente por la siguiente línea:

W.splashscreencontent = “su contenido personalizado aquí”;

No olvides las comillas dobles finales y el punto y coma (”;).

Si desea alargar la duración de la pantalla de inicio de sesión en HTML5, puede hacerlo modificando el valor en milisegundos:

W.splashscreentime = 5000; // tiempo de reproducción de la pantalla de inicio.

Recomendamos que limpie la caché de su navegador después de guardar la página html modificada.

Página de inicio de sesión web: Cómo cerrar el formulario de inicio de sesión después del inicio de sesión

Resumen

En la página de inicio de sesión web, cuando el usuario hace clic en el botón "Iniciar sesión", el cliente elegido (HTML5 o Windows) se abre en una nueva pestaña del navegador.

A veces, y más específicamente al usar el cliente de Windows, es posible que desee ocultar el formulario de inicio de sesión al usuario, por ejemplo, para evitar que el usuario haga clic nuevamente en el botón "Iniciar sesión".

Dependiendo del navegador de Internet utilizado, tienes dos opciones sobre cómo cambiar este comportamiento predeterminado. Ambas soluciones requieren que modifiques un archivo JavaScript.

Solución A: Cerrar la pestaña de inicio de sesión - Solo para Internet Explorer

En esta solución, cuando el usuario hace clic en el botón "Iniciar sesión", el cliente elegido se abrirá en una nueva pestaña del navegador y la pestaña de inicio de sesión se cerrará automáticamente. Dependiendo de la versión de Internet Explorer, puede aparecer una pequeña ventana de mensaje para el usuario, pidiéndole que confirme que desea cerrar esta pestaña.

Edita el archivo "common.js" que se encuentra en la carpeta "C:\Program Files (x86)\TSplus\Clients\www\software". Te recomendamos usar un editor de texto como Notepad o Notepad++. no usa Word).

Buscar estas líneas:

```
p = 'software/remoteapp.html';
window.name = " " + window.opforfalse;
if (cpwin != false) {
  cpwin.name = window.opforfalse;
  cpwin.location.replace(hostGateway + jwtsclickLinkBefore(getside(), p));
} else {
  window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);
}
```

Y reemplázalos por esas líneas:

```
p = 'software/remoteapp.html';
window.name = " " + window.opforfalse;
if (cpwin != false) {
  cpwin.name = window.opforfalse;
  cpwin.location.replace(hostGateway + jwtsclickLinkBefore(getside(), p));
} else {
  window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);
}
window.open('','_parent','');
window.close();
```

Recomendamos que limpie la caché de su navegador después de guardar el archivo

JavaScript modificado.

Solución B: Redirigir la pestaña de inicio de sesión a otra página web - Para todos los navegadores

En esta solución, cuando el usuario hace clic en el botón "Iniciar sesión", el cliente elegido se abrirá en una nueva pestaña del navegador y la pestaña de inicio de sesión navegará automáticamente a otra página web.

Puedes usar cualquier dirección de Internet (URL) existente como “ http://google.com o “http://your_intranet/your/page.html”, o puedes crear tu propia página web utilizando “thankyou.html” como la URL y creando un archivo llamado “thankyou.html” en la carpeta “C:\Program Files (x86)\TSplus\Clients\www” y colocando contenido HTML en él.

Edita el archivo "common.js" que se encuentra en la carpeta "C:\Program Files (x86)\TSplus\Clients\www\software". Te recomendamos usar un editor de texto como Notepad o Notepad++. no usa Word).

Buscar estas líneas:

```
p = 'software/remoteapp.html';
window.name = " " + window.opforfalse;
if (cpwin != false) {
  cpwin.name = window.opforfalse;
  cpwin.location.replace(hostGateway + jwtsclickLinkBefore(getside(), p));
} else {
  window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);
}
```

Y reemplázalos por esas líneas:

```
p = 'software/remoteapp.html';
window.name = " " + window.opforfalse;
if (cpwin != false) {
  cpwin.name = window.opforfalse;
  cpwin.location.replace(hostGateway + jwtsclickLinkBefore(getside(), p));
} else {
  window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);
}
window.location.href = "http://google.com";
```

Recomendamos que limpie la caché de su navegador después de guardar el archivo JavaScript modificado.

Página de inicio de sesión web: Cómo abrir el cliente HTML5 en la misma pestaña

Resumen

En la página de inicio de sesión web, cuando el usuario hace clic en el botón "Iniciar sesión", el cliente HTML5 se abre en una nueva pestaña del navegador.

Puedes cambiar este comportamiento y hacer que el cliente HTML5 se abra en la misma pestaña del navegador que la página de inicio de sesión web modificando un archivo JavaScript.

Modificando el archivo custom.js

Edita el archivo “custom.js” que se encuentra en la carpeta “C:\Program Files (x86)\TSplus\Clients\www”. Te aconsejamos usar un editor de texto como Notepad o Notepad++. no usa Word).

Agrega esta línea:

var openinsamewindow = true;

Recomendamos que limpie la caché de su navegador después de guardar el archivo JavaScript modificado.

Modificando el archivo common_applications.js

Si está utilizando la función del Portal de Aplicaciones Web de Terminal Service Plus, entonces necesita editar un segundo archivo. Edite el archivo "common_applications.js" que se encuentra en la carpeta "C:\Program Files (x86)\TSplus\Clients\www\software". Le aconsejamos que utilice un editor de texto como Notepad o Notepad++. no usa Word).

Buscar estas líneas:

```
if (childurl != '') {
  window.name = childname;
  location.href = childurl + '#';
}
```

Y reemplázalos por esas líneas:

```
  if (childurl != '') {
    window.name = childname;
    location.href = childurl + '#';
  }
```

Recomendamos que limpie la caché de su navegador después de guardar el archivo JavaScript modificado.

Portal web con SSO (beta)

Requisitos y limitaciones clave

Portal Web 2026 con SSO está diseñado para el **Creativo** tema y utiliza todas las personalizaciones de AdminTool > Web > Personalización del Portal Web. Si el tema seleccionado no es **Creativo** , el Portal Web no se muestra.

Cuando está habilitado en una granja, todos los servidores deben ejecutar el **mismo versión de Remote Access** y estar habilitado para **Portal Web 2026 con SSO**

Esta función es **Beta** y debería **no** ser implementado en servidores de producción.

¿Por qué un nuevo portal web?

Comparado con el Portal Web anterior, esta implementación ofrece mayor fiabilidad y mejor rendimiento bajo carga. Además, permite:

- **Capacidades avanzadas de SSO**
  - Autenticación integrada de Windows (Negociar / Kerberos / NTLM)
  - Integración de proveedor de identidad de terceros (actualmente SAML)
- **Controles de seguridad más fuertes**
  - Protecciones antifalsificación integradas
  - Limitación de tasa de endpoint
  - Autenticación moderna y controles de cookies/sesiones

Su arquitectura nos permitirá abordar fácilmente cualquier comentario de auditoría de seguridad potencial.

También es un **producto más accesible** a través de recomendaciones y un mejor contraste.

Flexibilidad del servidor web (Kestrel por defecto)

La aplicación no está vinculada a un único servidor web front-end. Por defecto, se ejecuta en **Kestrel** Puerto HTTP 81. Puede ser precedido por **IIS** o **Apache** como un proxy inverso al cambiar la configuración del servidor web.

Ejemplo: proxy inverso de Apache al servicio del Portal Web

```
# Apache VirtualHost example
ProxyPreserveHost On
ProxyPass        /  http://127.0.0.1:81/
ProxyPassReverse /  http://127.0.0.1:81/

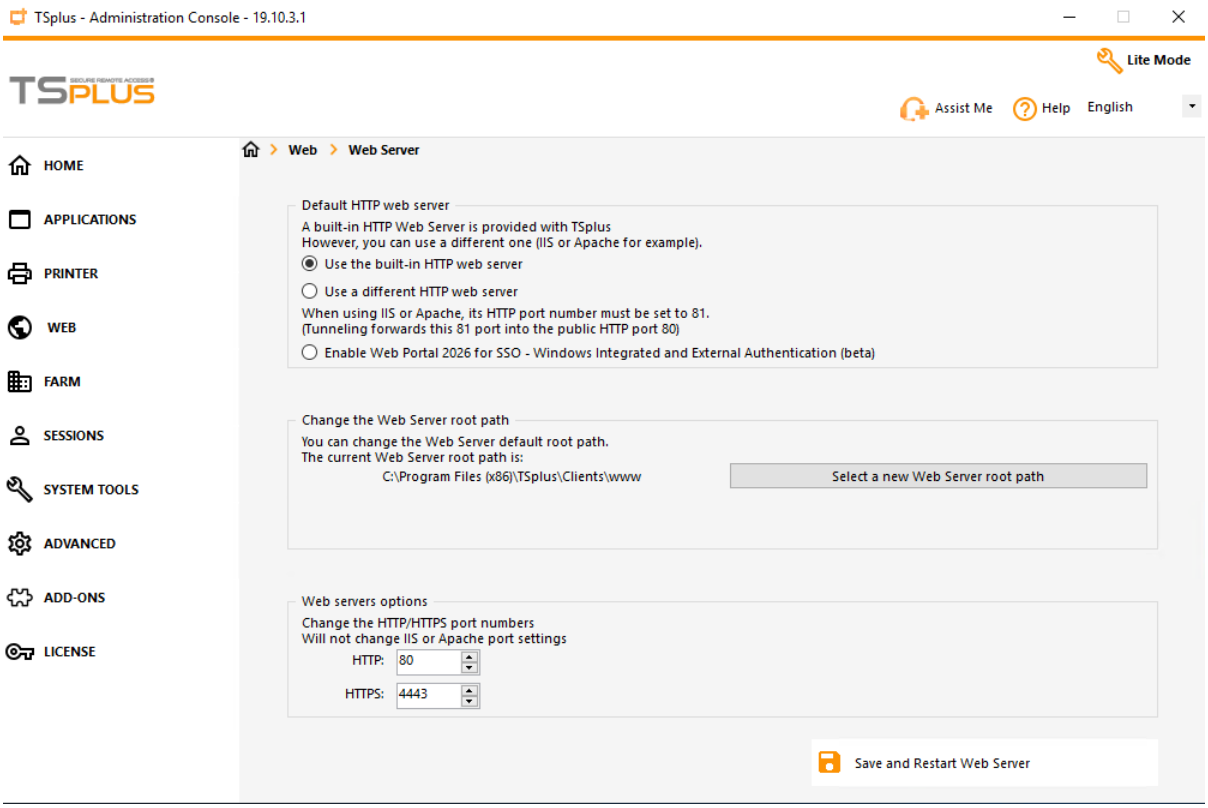
RequestHeader set X-Forwarded-Proto "https"
RequestHeader set X-Forwarded-For "%{REMOTE_ADDR}s"
```

Esto mantiene la lógica del Portal Web sin cambios mientras Apache maneja la exposición pública de HTTP/HTTPS.

Por favor, contacte al equipo de desarrollo si está interesado, ya que este escenario aún no es accesible desde el programa AdminTool y debe configurarse manualmente.

Habilitar Portal Web 2026 con SSO

1. Abrir **AdminTool**
2. Ir a: Web > Servidor web
3. Habilitar: **Portal web 2026 con SSO**



Importante esta opción es Beta. Úselo solo en entornos de prueba.

Modos de inicio de sesión compatibles

Portal Web 2026 con SSO soporta:

- Formulario de inicio de sesión tradicional utilizando credenciales de Windows
- Credenciales web. Ver: https://docs.tsplus.net/tsplus/web-credentials/
- Autenticación integrada de Windows (automática en escenarios de confianza / locales)
- Proveedor de identidad externo a través de **SAML** como Entra ID (anteriormente Azure AD) o Okta

Nota: Soporte para autenticación externa a través de **OIDC** planificado más tarde, a pedido

comportamiento de 2FA

2FA se aplica a los flujos de cuentas estándar, incluyendo:

- Formulario de inicio de sesión utilizando credenciales de Windows
- Credenciales web
- Autenticación integrada de Windows

Los proveedores de autenticación externa a menudo imponen su propio MFA / 2FA. Por lo tanto, la configuración de 2FA establecida en el complemento de 2FA de Remote Access no se aplica a este escenario.

El bypass de red local está disponible a través de CustomSettings:Bypass de 2FA para red local parámetro ubicado en el archivo: C:\Program Files (x86)\TSplus\Clients\webportal\appsettings.json , donde C:\Program Files (x86)\TSplus es la carpeta de configuración de TSplus Remote Access. Cuando está habilitado, el bypass ocurre solo si el cliente y la puerta de enlace están en la misma subred privada.

Configurar el flujo de autenticación de Windows

Para los usuarios que inician sesión con autenticación de Windows, se requiere uno de los siguientes:

1. Pre-registre credenciales con el comando TSplus: AdminTool.exe /windowscredential-agregar o actualizar . Consulte la documentación en https://docs.tsplus.net/tsplus/commands-list/#agregar-o-actualizar-credenciales-en-el-gestor-de-credenciales-de-windows-windowscredential-addorupdate
2. O deje que el usuario inicie sesión una vez a través del formulario de inicio de sesión del Portal Web con credenciales de Windows.

Para configurar la autenticación integrada de Windows, consulte: Habilitar la autenticación integrada de Windows en un dominio de Active Directory. Dado que este modo de autenticación es arduo de configurar, los clientes a menudo prefieren establecer un proveedor de identidad externo.

Configurar la autenticación externa (SAML)

Configuraciones requeridas para la aplicación externa

La aplicación externa debe configurarse de la siguiente manera:

- URL de inicio de sesión único debe configurarse en el punto final del servicio de consumidor SAML del Portal Web, por ejemplo https://mywebportal.company.com/Saml/acs
- URI de audiencia (ID de entidad SP) debe establecerse en el nombre de dominio o dirección IP del Portal Web, p. ej. https://mywebportal.company.com
- Formato de ID de nombre debe estar configurado en **Dirección de correo electrónico**
- Nombre de usuario de la aplicación debe estar configurado en **Correo electrónico** , ya que la parte izquierda identificará el nombre de usuario de la cuenta de Windows

Configuraciones requeridas en appsettings.json

El archivo appsettings.json se encuentra en C:\Program Files (x86)\TSplus\Clients\webportal , donde C:\Program Files (x86)\TSplus es la carpeta de configuración de TSplus Remote Access.

Edita el Saml2 sección:

- IdPMetadata
- Emisor
- Destino de inicio de sesión único opcional si los metadatos lo proporcionan
- Destino de cierre de sesión único opcional si los metadatos lo proporcionan
- Campos relacionados con el certificado

Por ejemplo, utilizando el proveedor de identidad de terceros okta:

```
"Saml2": {
  "IdPMetadata": "https://mycompany.okta.com/app/abcdfegh12345678/sso/saml/metadata",
  "Issuer": "https://portal.mycompany.com",
  "SingleSignOnDestination": "https://mycompany.okta.com/app/mycompany_portalsaml_1/
abcdfegh12345678/sso/saml",
  "SingleLogoutDestination": "https://mycompany.okta.com",
  "SignatureAlgorithm": "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256",
  "SigningCertificateFile": "",
  "SigningCertificatePassword": "",
  "SignatureValidationCertificateFile": "okta.identity.saml2.portal.cert",
  "CertificateValidationMode": "ChainTrust",
  "RevocationMode": "Offline",
  "XmlCanonicalizationMethod": "http://www.w3.org/2001/10/xml-exc-c14n#"
}
```

La configuración del emisor establece la URI de audiencia, según lo definido en el lado del proveedor de identidad externo.

si el Archivo de certificado de validación de firma la configuración está establecida en un valor diferente a **Ninguno** , entonces asegúrese de que el certificado se considere válido en el servidor de aplicaciones. Esto puede requerir agregar el certificado a la lista de certificados de

confianza a nivel de máquina.

Disponibilidad de contraseña de Windows para el lanzamiento de sesión

Para la autenticación SAML externa, el lanzamiento de sesiones aún requiere credenciales de Windows utilizables. Utilice uno de:

1. Registrar credenciales de Windows con el comando: AdminTool.exe /windowscredential-agregar o actualizar . Consulte la documentación en https://docs.tsplus.net/tsplus/commands-list/#agregar-o-actualizar-credenciales-en-el-gestor-de-credenciales-de-windows-windowscredential-addorupdate
2. O reenvíe la contraseña de la reclamación de IdP configurando CustomSettings:UseSamlPasswordClaim al tipo de reclamación que contiene la contraseña de Windows.

Típicamente, el Portal Web tomará la parte antes del ' @ ' de la dirección de correo electrónico del usuario como el nombre de usuario de la cuenta de Windows.

Tenga en cuenta que la autenticación externa funciona con usuarios locales en este momento.

Si no hay contraseña disponible en la reclamación o en el almacén de credenciales, la validación del usuario falla.

Referencia completa del archivo de configuración appsettings.json

El archivo appsettings.json se encuentra en C:\Program Files (x86)\TSplus\Clients\webportal , donde C:\Program Files (x86)\TSplus es la carpeta de configuración de TSplus Remote Access.

Registro

Parámetro	Propósito	Valores posibles	Predeterm
Registro:NivelDeRegistro:Predeterminado	Nivel mínimo de registro global.	Rastro , Depurar , Información , Advertencia , Error , Crítico ,	Informaci

		Ninguno	
Registro:NivelDeRegistro:Microsoft.AspNetCore	Nivel de registro del marco ASP.NET Core.	Igual que arriba	Advertenc
Registro:NivelDeRegistro:Microsoft.AspNetCore.Autenticación	Nivel de registro del subsistema de autenticación.	Igual que arriba	Advertenc

Configuración global del host

Parámetro	Propósito	Valores posibles	Predeterminado
HostsPermitidos	Filtrado de encabezados de host para la protección del host de ASP.NET Core.	* (todos) o lista de hosts separados por punto y coma	*

Limitación de tasa de IP

Parámetro	Propósito	Valores posibles	Predeterminado
IpRateLimiting: HabilitarLimitaciónDeTasaDePuntoFinal	Habilita reglas de limitación específicas para el endpoint.	verdadero / falso	verdadero
IpRateLimiting:StackBlockedRequests	Si verdadero , las solicitudes bloqueadas continúan aumentando contadores.	verdadero / falso	falso
IpRateLimiting:HttpStatusCode	Estado HTTP devuelto cuando la solicitud es bloqueada.	Código HTTP entero (típicamente 429)	429
IpRateLimiting:EncabezadoRealIp	Encabezado utilizado para resolver la IP del cliente detrás del	Nombre del encabezado	X-Forwarded-For

	proxy.		
IpRateLimiting:ClientIdHeader	Encabezado de client-id opcional para limitación de tasa personalizada.	Nombre del encabezado	X-ClientId

IpRateLimiting:ReglasGenerales

Cada objeto de regla tiene:

Parámetro	Propósito	Valores posibles	Predeterminado en el archivo enviado
Endpoint	Ruta/método patrón para proteger.	Formato VERBO:/ ruta	Múltiples valores predeterminados (ver más abajo)
Período	Ventana de tarifas.	e.j. 1s , 1m , 5m , 1h , 1d	5m (for all default rules)
Límite	Máx. solicitudes en el período.	Número entero positivo	5 (for all default rules)

Saml2

Parámetro	Propósito	Valores posibles	Predetermin
Saml2:IdPMetadata	URL de metadatos de IdP utilizada para cargar la configuración del proveedor SAML.	URL HTTPS válida	""
Saml2:Emisor	ID de entidad SP (esta identidad del Portal Web).	cadena URI	""
Saml2:DestinoDeInicioDeSesiónÚnico	URL del endpoint IdP SSO (se puede resolver automáticamente a partir de los metadatos).	URL HTTPS	""

Saml2:DestinoDeCierreDeSesiónÚnico	URL del endpoint SLO de IdP (se puede resolver automáticamente a partir de los metadatos).	URL HTTPS	""
Saml2:SignatureAlgorithm	Algoritmo de firma XML.	Valor URI aceptado por la biblioteca SAML	http://www.w3.org/xmldsig-more sha256
Saml2:ArchivoDelCertificadoDeFirma	Archivo de certificado de firma de SP local (relativo a la ruta base de la aplicación).	Nombre/ruta del archivo	""
Saml2:ContraseñaDelCertificadoDeFirma	Contraseña para el archivo del certificado de firma.	Cadena	""
Saml2:ArchivoDelCertificadoDeValidaciónDeFirma	Archivo de certificado IdP utilizado para validar firmas (opcional si los metadatos proporcionan certificados).	Nombre/ruta del archivo	""
Saml2:ModoDeValidaciónDeCertificado	Modo de validación de la cadena de certificados.	Ninguno , PeerTrust , ChainTrust , Confianza entre pares o cadena , CustomRootTrust	ChainTrust
Saml2:ModoDeRevocación	Comportamiento de revocación de certificados.	NoCheck , En línea , Sin conexión	Sin conexión
Saml2:XmlCanonicalizationMethod	Algoritmo de canonicalización XML URI.	URI de canonicalización XML-DSig	http://www.w3.org/xml-exc-c14r

ConfiguracionesPersonalizadas

En appsettings.json , estos valores se almacenan como cadenas (true / falso) y mapeado a booleanos mediante la configuración de enlace de .NET.

Parámetro	**Propósito**	**Valores posibles**	**Predeter**
CustomSettings:UsarRutaCompletaDeAplicación	Controla si se utiliza la ruta completa de la aplicación al listar/ iniciar aplicaciones asignadas.	true / falso	falso
CustomSettings:EnableAutoWindowsAuthenticationOnLocalhost	Permite la autenticación automática de Windows en el escenario de localhost/ loopback.	true / falso	falso
CustomSettings:EnablePasswordEncryption	Encripta el dominio/ nombre de usuario/ contraseña en la cadena de conexión de lanzamiento HTML5 utilizando parámetros RSA.	true / falso	true
CustomSettings:Bypass de 2FA para red local	Elimina la autenticación de dos factores del portal web cuando el cliente está en la misma subred	true / falso	falso

	privada que el servidor.		
CustomSettings:UseSamlPasswordClaim	Tipo de reclamación SAML utilizado como contraseña de Windows reenviada para el lanzamiento de sesión.	Tipo de reclamación URI/nombre o cadena vacía	""

Solución de problemas

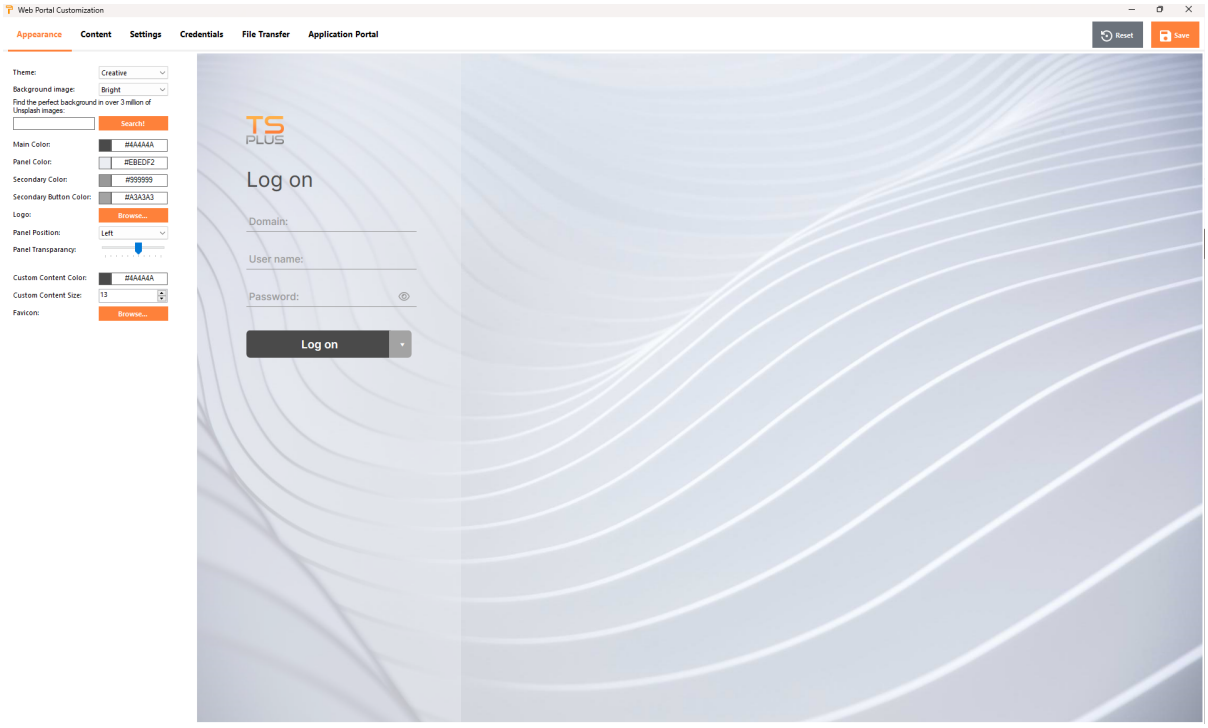
Portal Web 2026 con registros SSO se puede habilitar desde AdminTool > Avanzado > Registros > Registro del Portal Web.

El resultado WebPortal.log el archivo de registro se encuentra en C:\Program Files (x86)\TSplus\Clients\webportal , donde C:\Program Files (x86)\TSplus es la carpeta de configuración de TSplus Remote Access.

Creando y personalizando páginas de acceso web HTML utilizando la personalización del portal web

Usando la personalización del portal web, podrá crear sus propias páginas de acceso web HTML personalizadas - y hay no es necesario ser un desarrollador web !

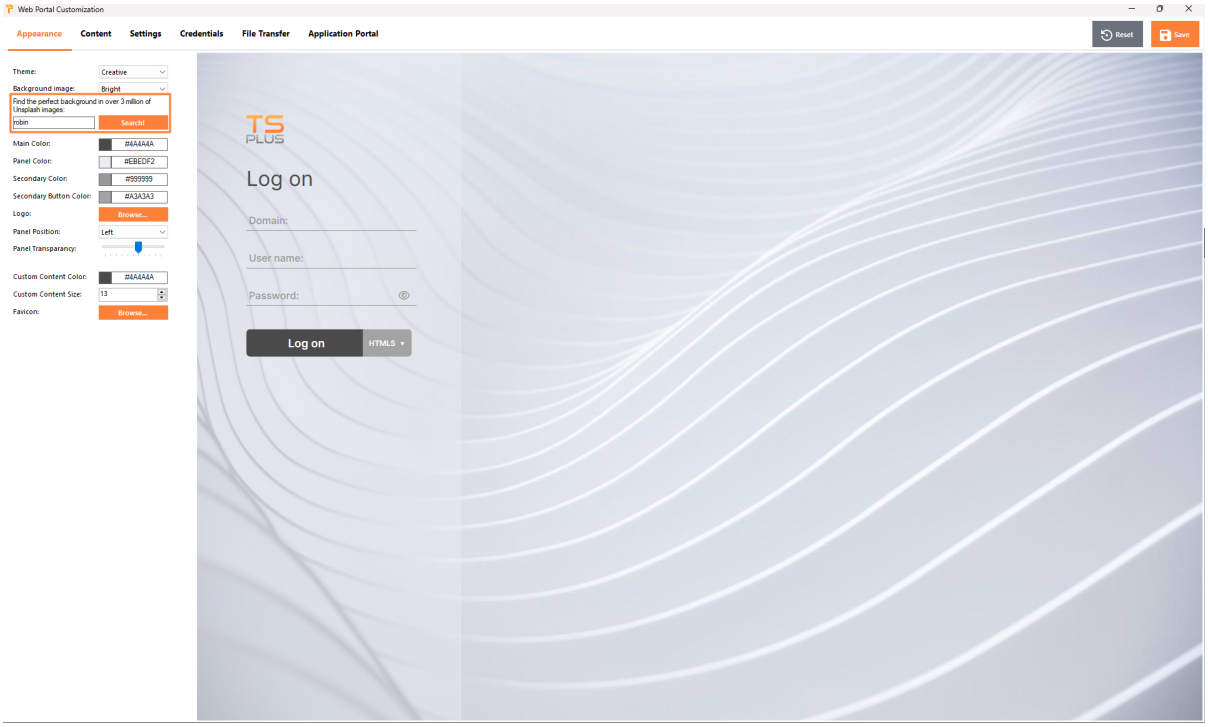
Personalización del portal web - Apariencia



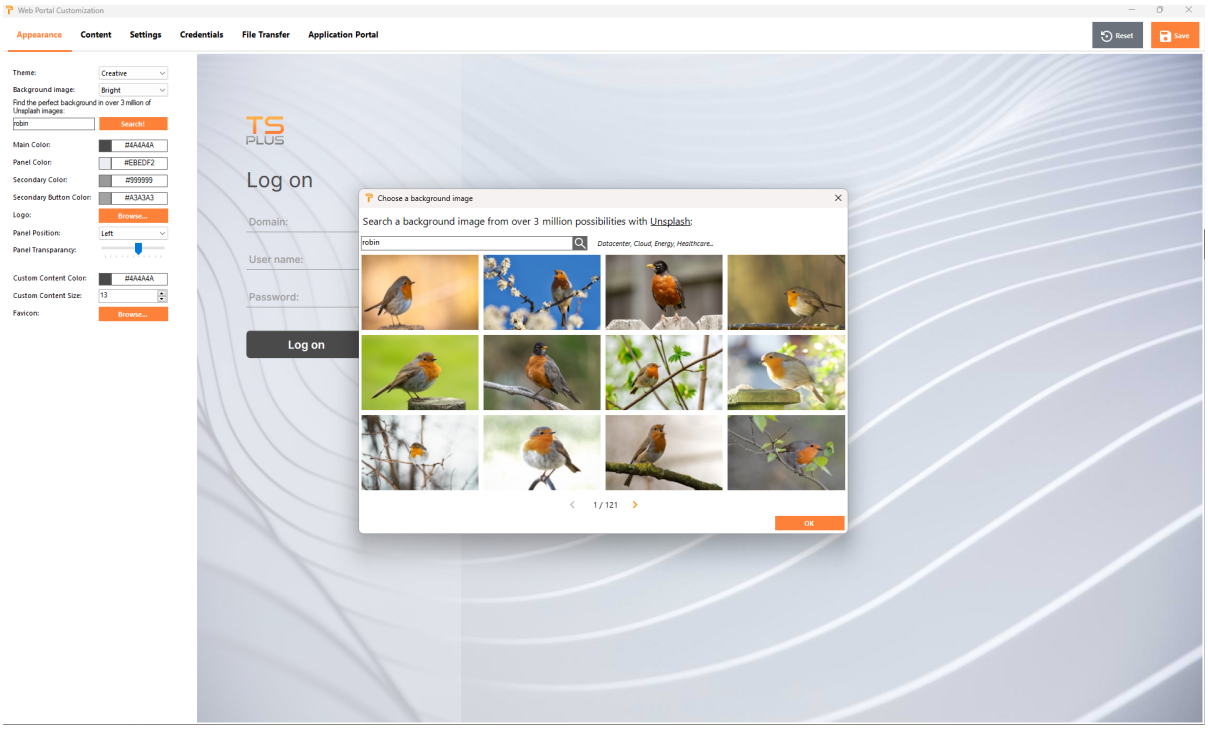
Con la pestaña de Apariencia, podrás personalizar todos los ajustes gráficos, así como añadir tu propio logotipo.

Tienes la opción entre una colección de fotos, o puedes agregar las tuyas. También puedes establecer cualquier tema de color con el color de fondo de tu elección o puedes usar uno de los temas clásicos.

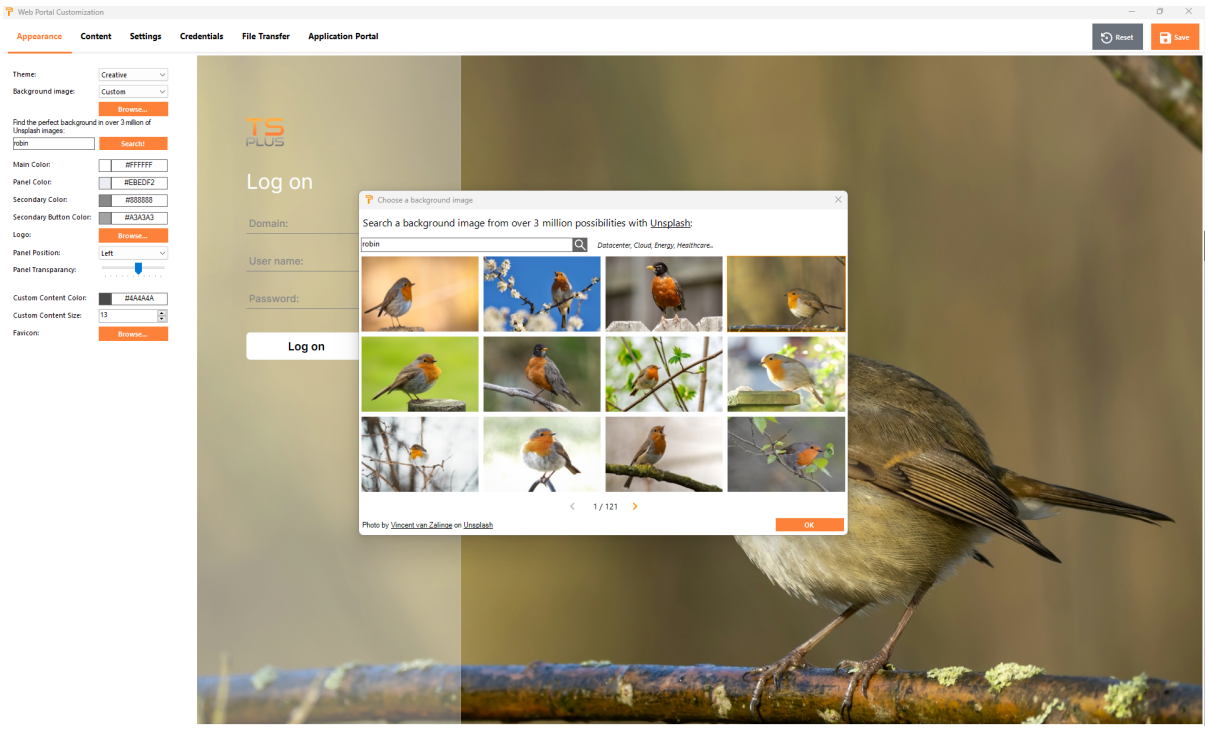
También puedes escribir una palabra clave para buscar una imagen de fondo en la biblioteca de Unsplash:



Mostraré una colección de imágenes para elegir.

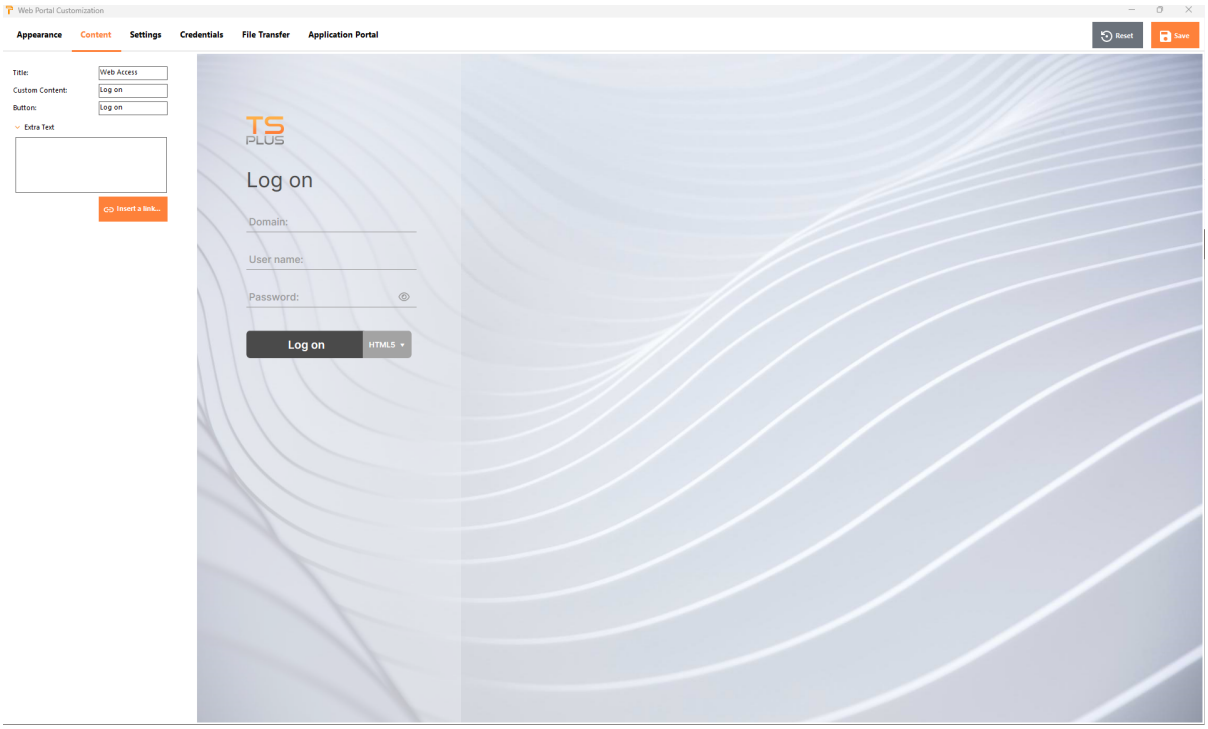


Selecciona tu imagen favorita para ver el resultado en tu portal web:

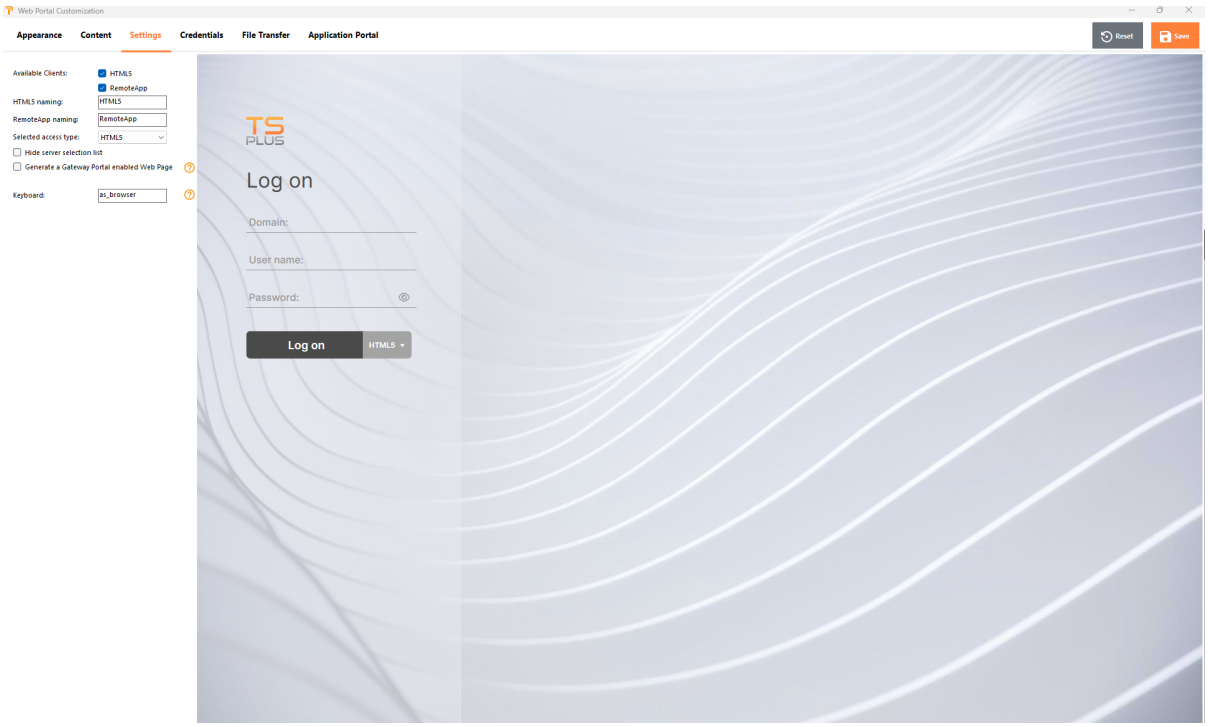


Los colores del tema se adaptarán automáticamente a la imagen elegida una vez que valides tu elección con el botón "Ok". Por supuesto, aún puedes personalizar los colores como desees.

Personalización del Portal Web - Contenido

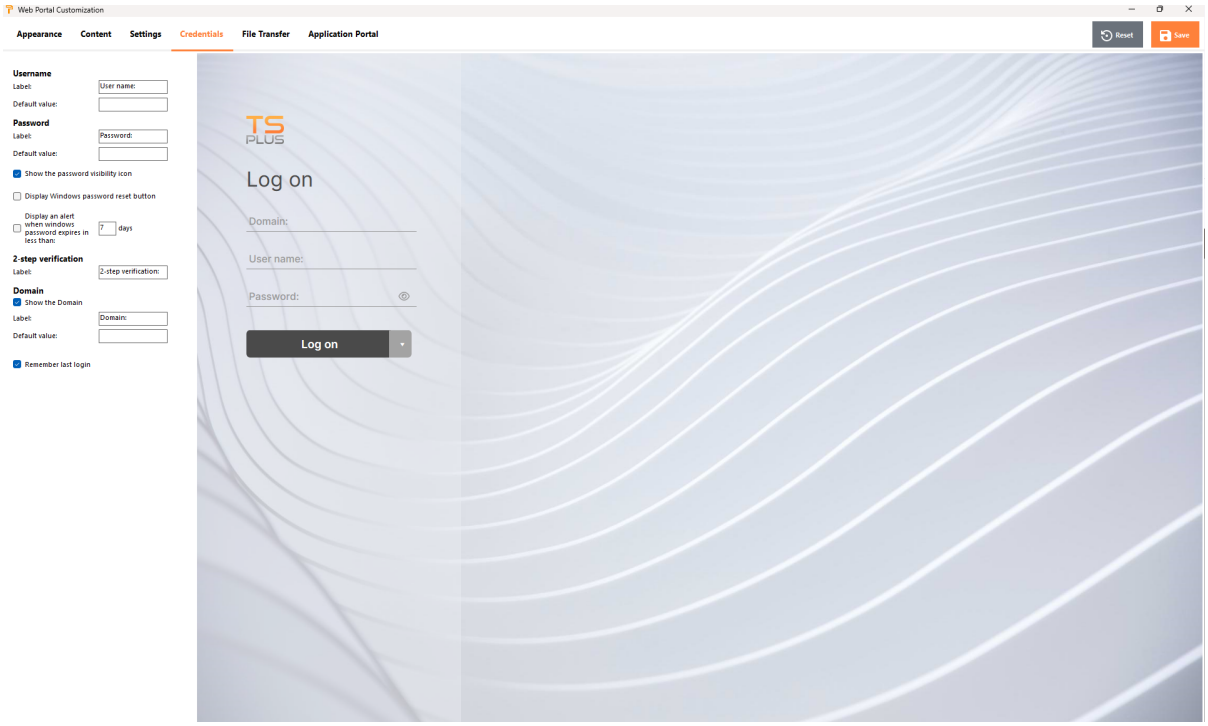


Personalización del Portal Web - Configuración

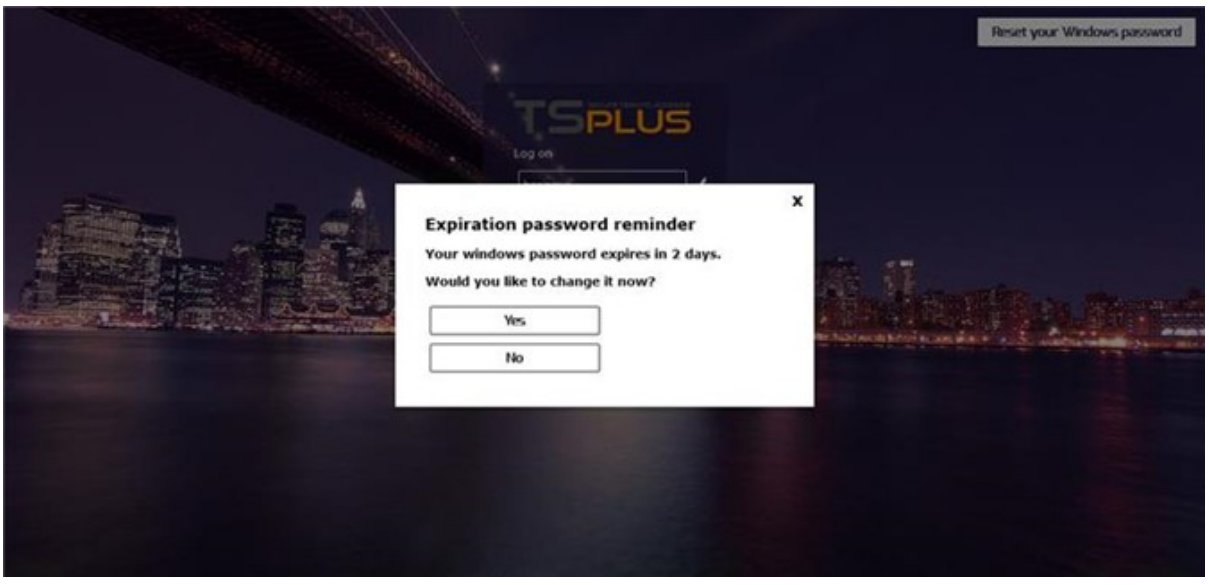


- “ **Clientes Disponibles** Elija entre 2 tipos de clientes de conexión web. Si ambos están marcados, el usuario tendrá la opción. Puede cambiar el nombre utilizado para estas opciones en su Portal Web. También puede elegir qué opción se selecciona por defecto si ambas opciones están disponibles.
- “ **Portal de Gateway** Marque esto para activar una página habilitada para el Portal de Gateway. Esta función añade un paso adicional de autenticación cuando asigna un servidor a un usuario o grupo.
- “ **Teclado** Solo para administradores avanzados que tienen requisitos especiales de teclado.

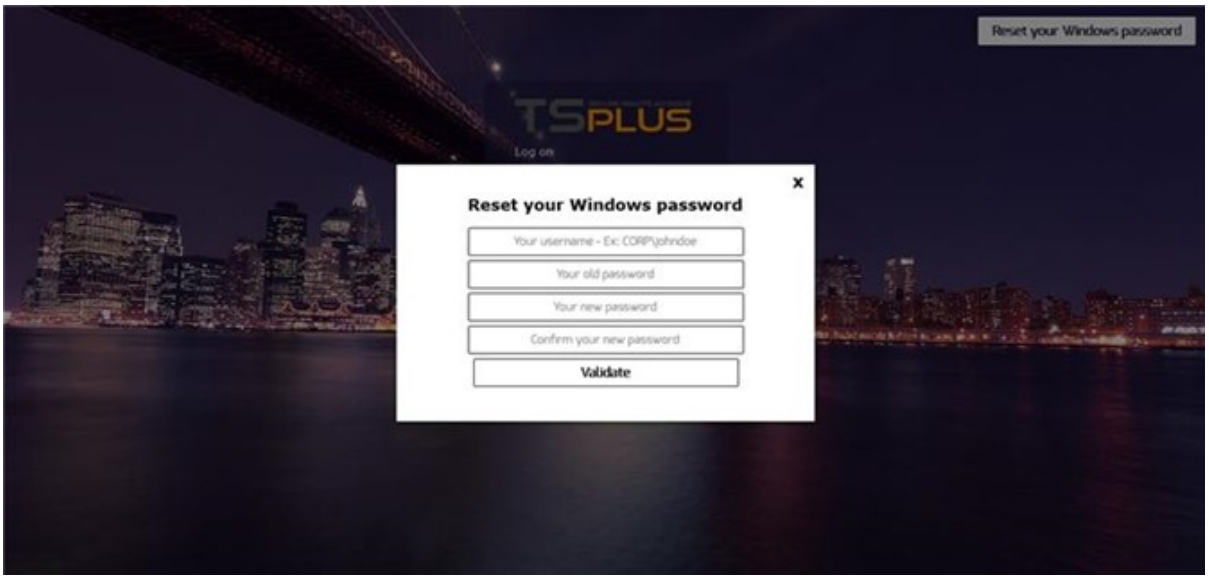
Personalización del portal web - Credenciales



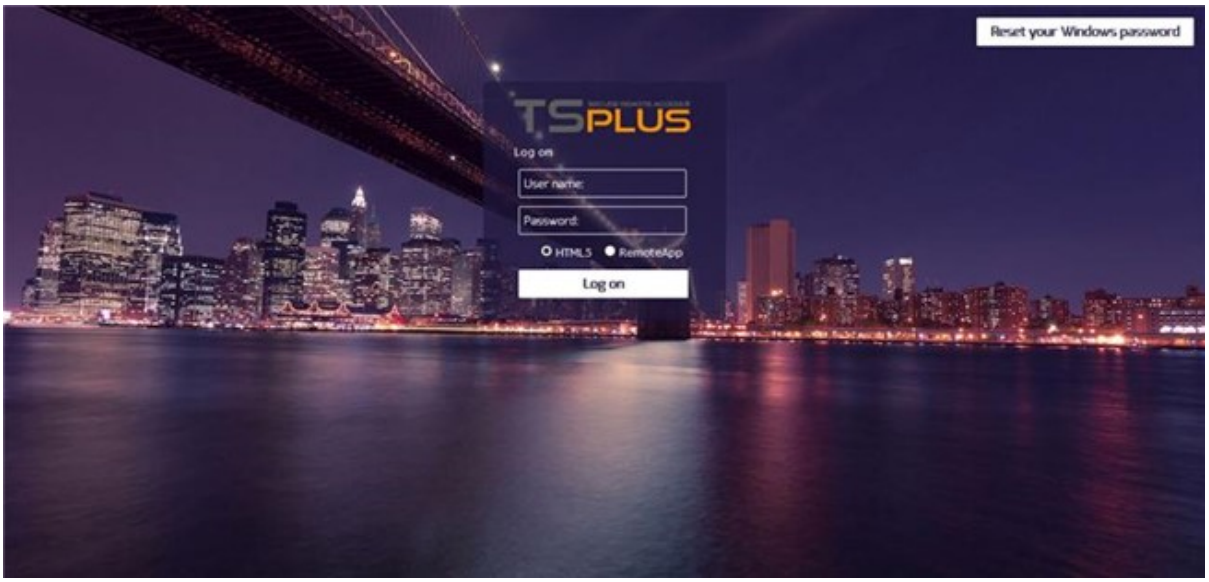
- “ **Etiqueta** Puedes cambiar el texto utilizado para designar el nombre de usuario, la contraseña, …
- “ **Valores predeterminados** Puedes especificar un inicio de sesión predeterminado, contraseña y dominio que se autocompletarán en los campos de inicio de sesión. Todos los ajustes presentes aquí se guardan en el archivo index.html, que se puede copiar y renombrar según tu preferencia.
- “ **Mostrar el campo de dominio** Cuando está marcado, el campo de Dominio se incluye en la solicitud de información de inicio de sesión.
- “ **Contraseña** Puedes agregar un mensaje de alerta que se muestre durante la conexión a través del portal web, para informar al usuario sobre la fecha de expiración de su contraseña. Por ejemplo, el siguiente mensaje emergente se mostrará si la contraseña de Windows del usuario expira en menos de 3 días:



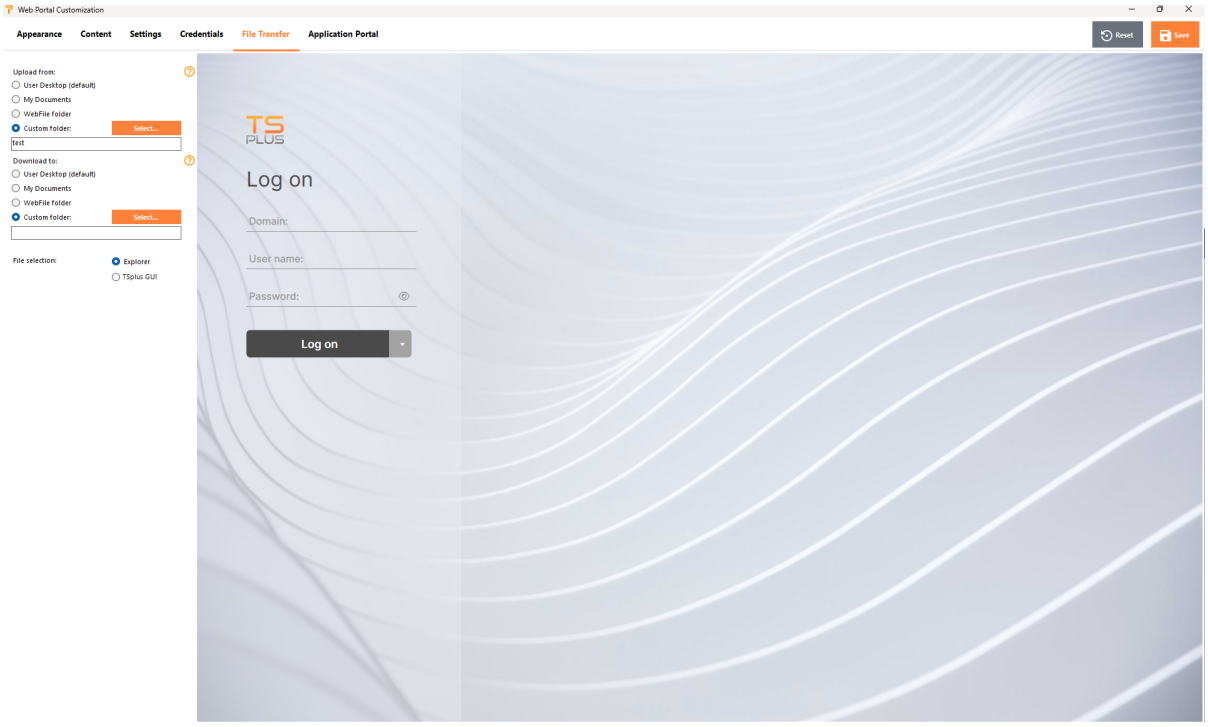
Como se mencionó, le da la posibilidad de cambiarlo directamente desde el Portal Web utilizando el pop-up que se muestra justo debajo:



También puede permitir que el usuario cambie su contraseña de Windows en cualquier momento, marcando la opción "Mostrar botón de restablecimiento de contraseña de Windows".

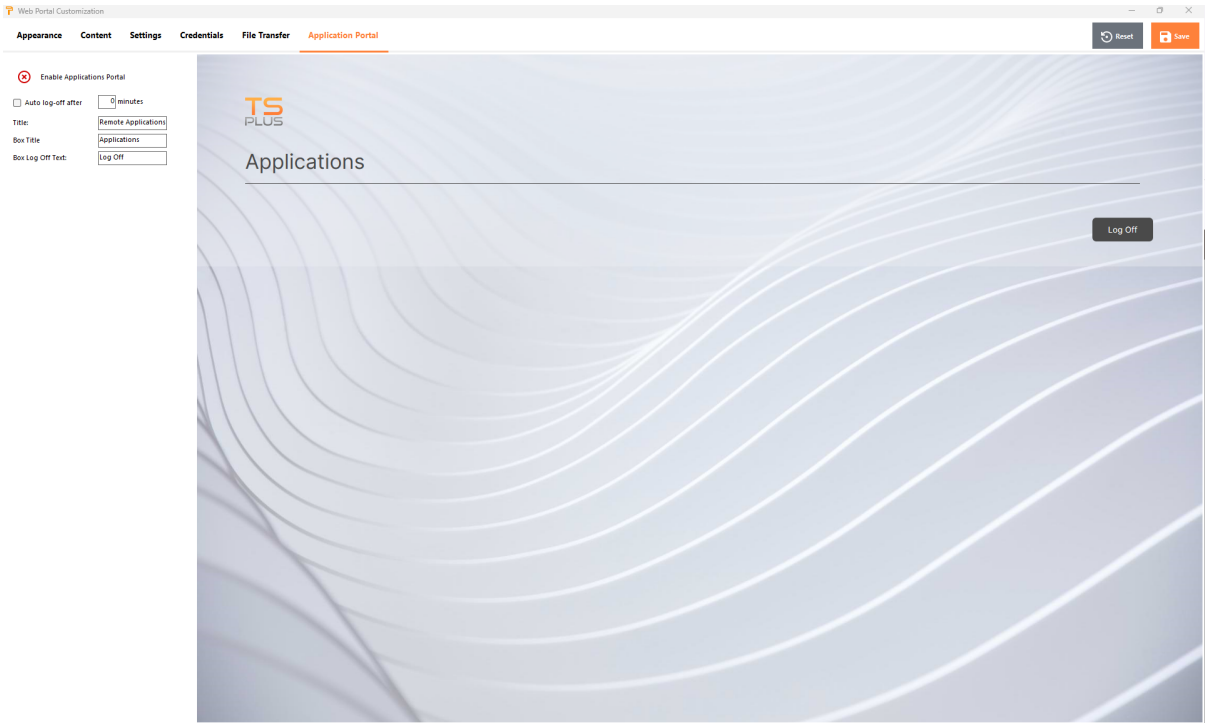


Personalización del portal web - Transferencia de archivos



- “ **Subir - Descargar** : elige las rutas de origen y destino para las cargas y descargas de archivos.

Personalización del Portal Web - Panel de Aplicaciones



Más información sobre el Portal de Aplicaciones se puede encontrar aquí .

Guardar valores escritos y restablecer a los predeterminados

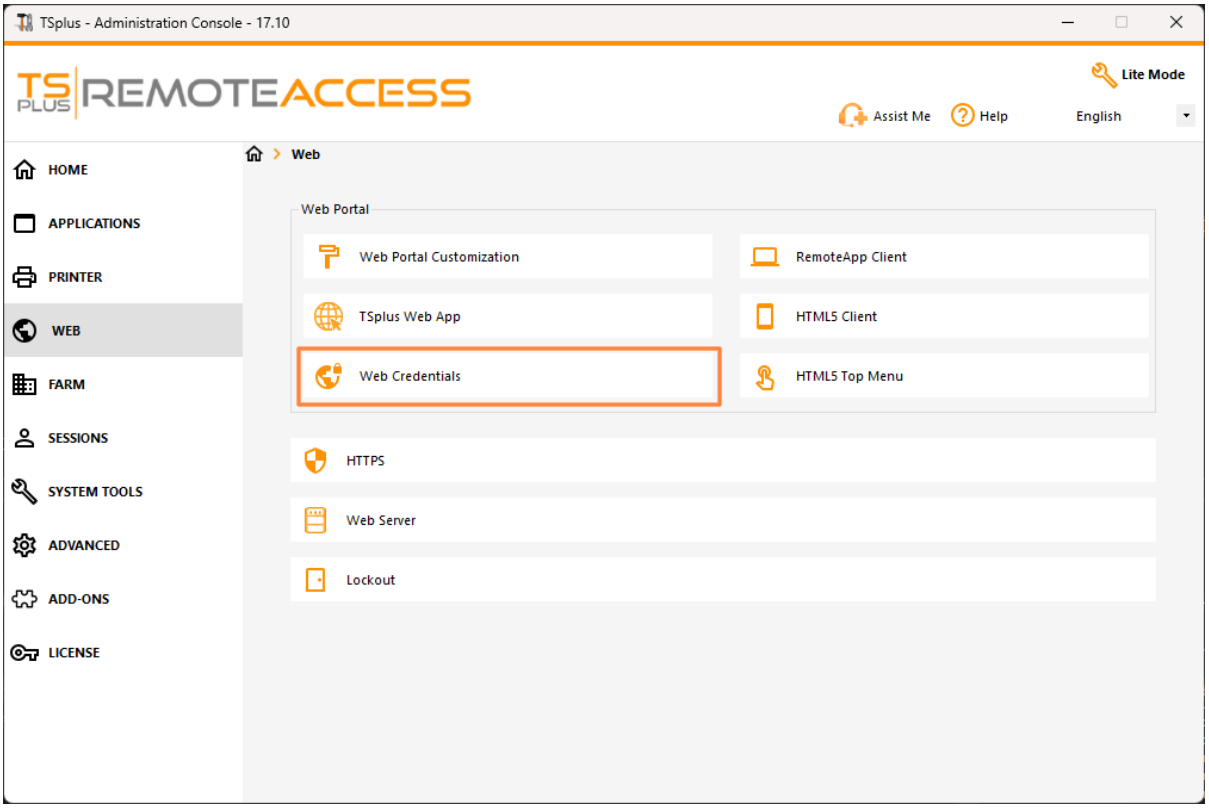
No olvides hacer clic en el botón "Guardar" para guardar todas tus modificaciones.

Si desea restablecer estos valores a los valores originales, haga clic en el botón "Restablecer".

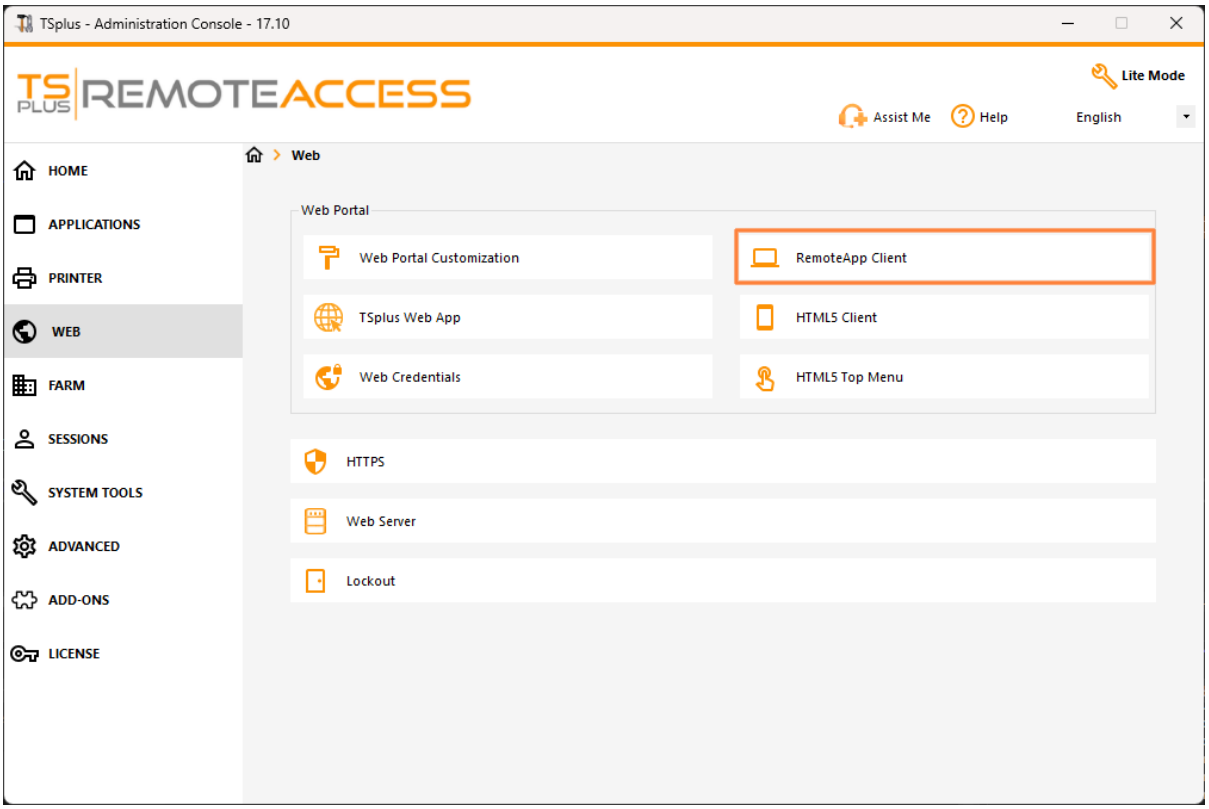
Credenciales Web

La sección "Credenciales web" te permite habilitar (o deshabilitar) el Credenciales Web característica.

Al utilizar Credenciales Web, es posible que desee permitir contraseñas vacías. Si solo tiene Credenciales Web con contraseñas vacías, le recomendamos que desmarque la opción "Mostrar campo de contraseña" para simplificar aún más la página de inicio de sesión web.

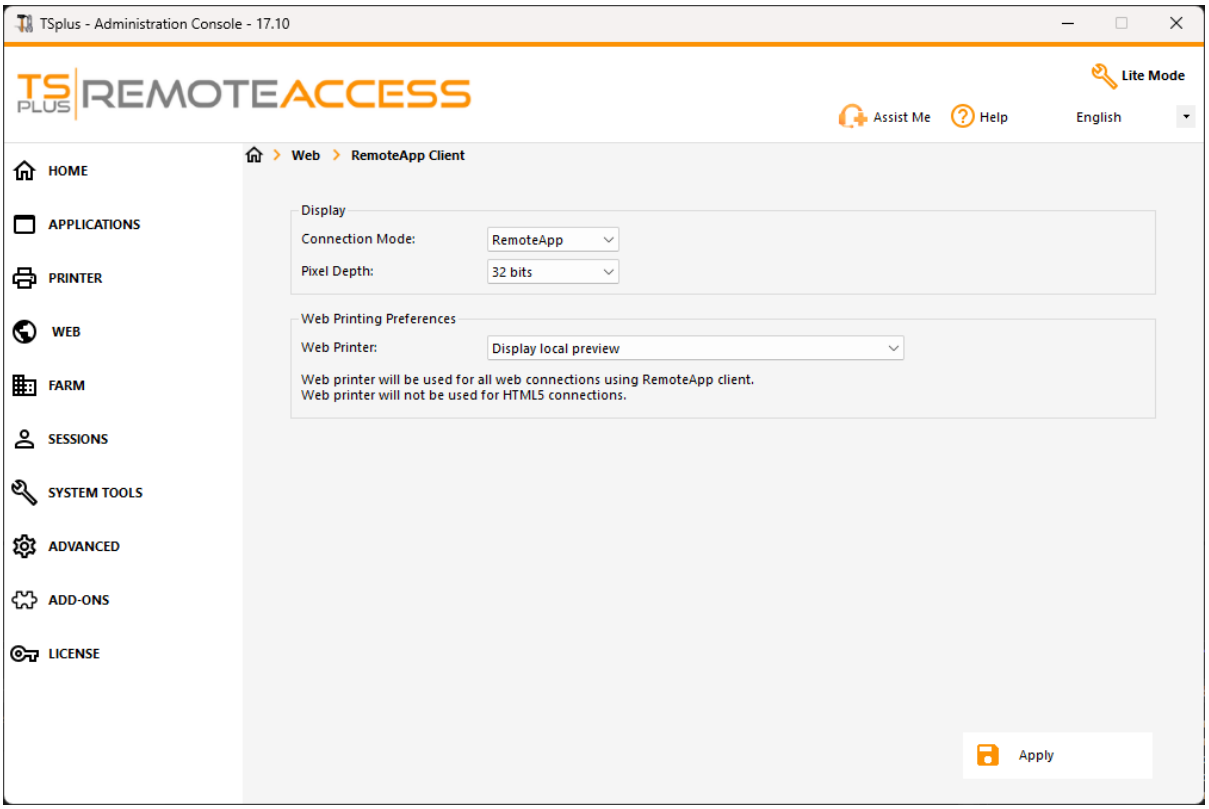


Tile de aplicación remota

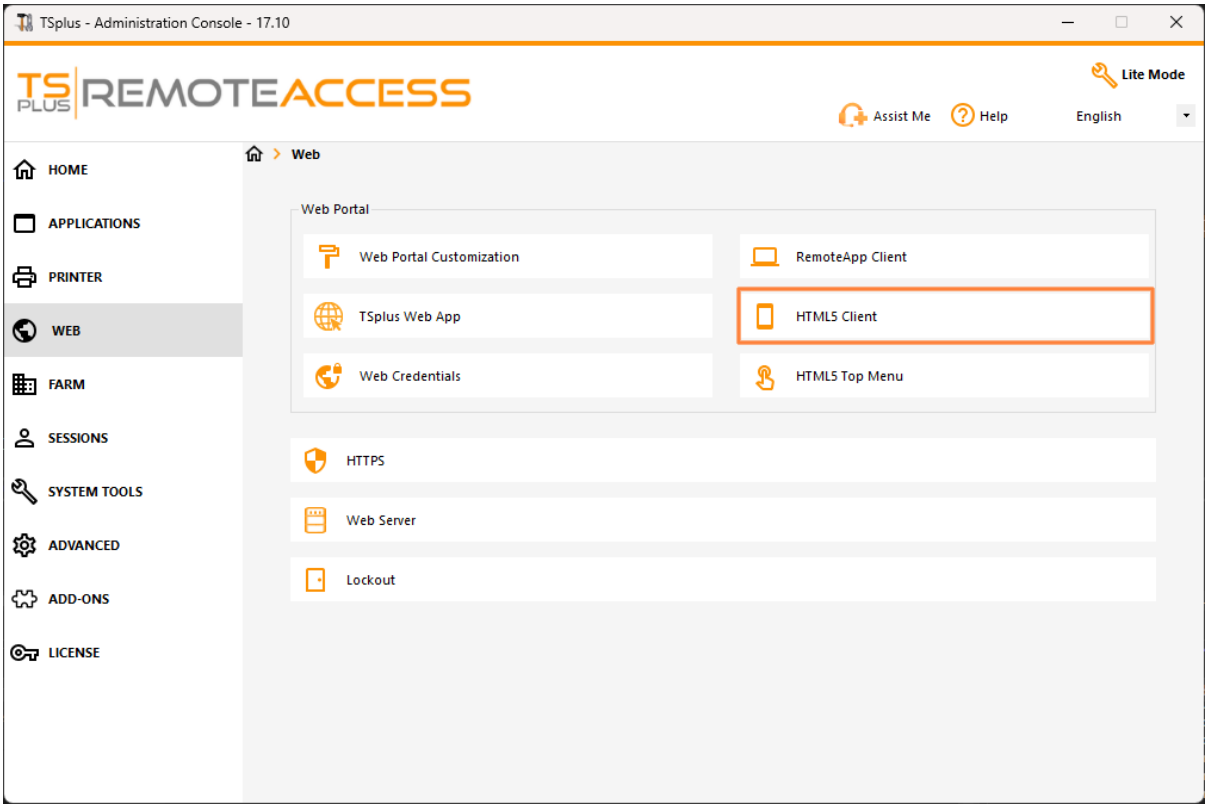


Este mosaico es para la configuración específica de clientes de Windows.

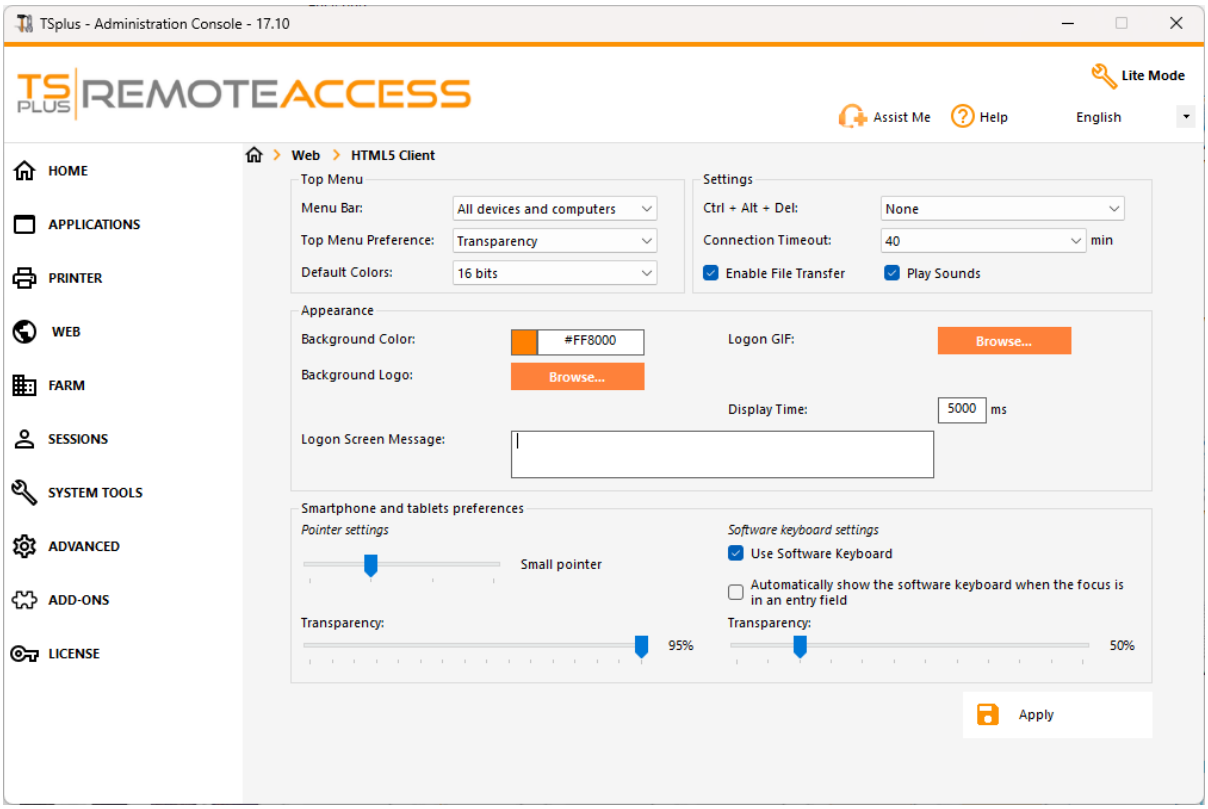
Puedes elegir tu visualización entre RemoteApp (conexión remota sin el escritorio remoto) o RDP estándar. También puedes decidir si deseas que los documentos se impriman en la impresora predeterminada del usuario, mostrar una vista previa local o la elección de la impresora local.



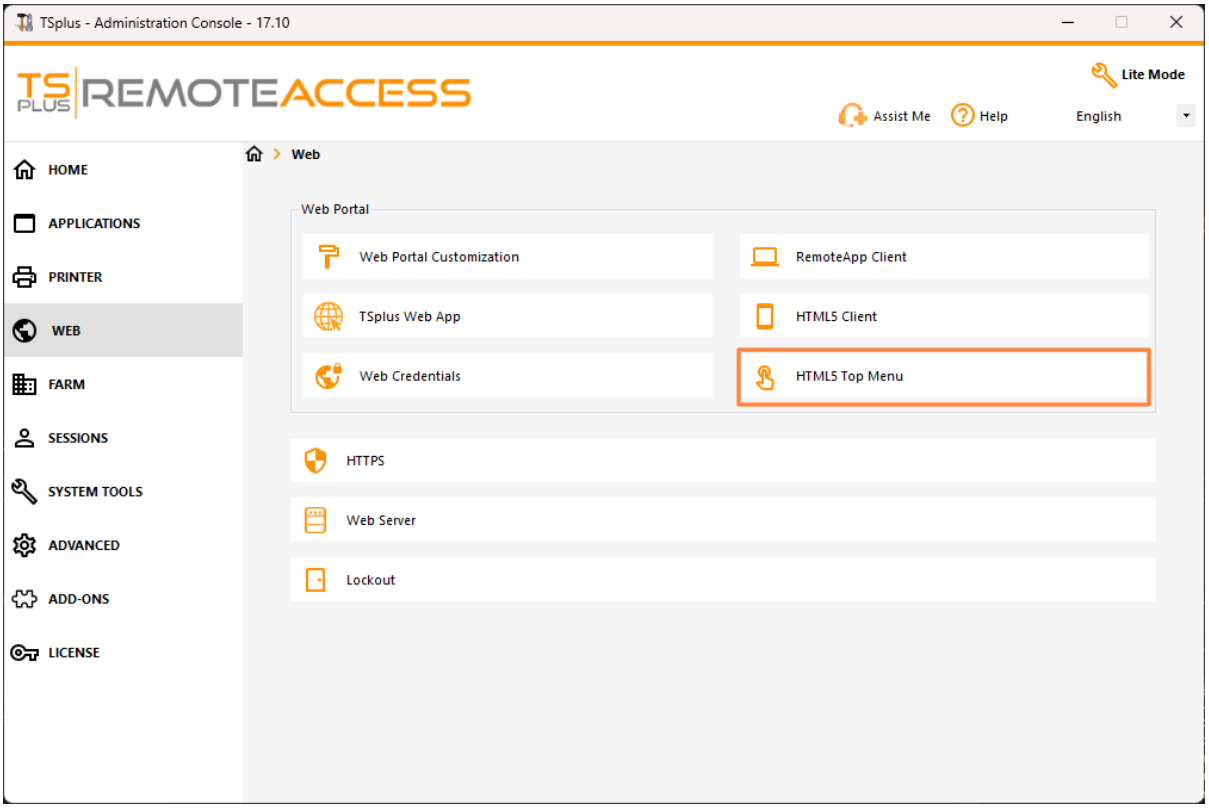
tile del cliente HTML5



En este mosaico, puedes editar los parámetros para la visualización web del cliente HTML5. Más información sobre esta página .



HTML5 Menú Superior Tile



Este mosaico le permite elegir las aplicaciones que se mostrarán en el nivel 1 o 2 del menú superior de su sesión web remota generada. También puede editar estas aplicaciones para que

aparezcan en un tipo de cliente específico: pc, móvil, ios… o en todos ellos.

