Two-factor Authentication

Tabla de contenidos

- Visión general
- Requisitos
- Active su licencia
- Habilitar la autenticación de dos factores
- Agregar usuarios y grupos
- Editar usuarios
- Quitar usuarios y grupos
- Restablecer la configuración para los usuarios
- Inscribir al usuario para la autenticación de dos factores
- Recibir códigos con una aplicación de autenticación
- Configurar SMS para recibir códigos de autenticación
- Inicie sesión con autenticación de dos factores
- Sincronización horaria

Configuración

Visión general

La autenticación de dos factores agrega una capa adicional de seguridad y **evita 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 saben, **una contraseña**.
2. Algo que tienen, un **dispositivo, como un teléfono inteligente, con una aplicación de autenticación instalada.**.

Puede 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 desde 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 fuera de línea.

O puede decidir recibir códigos de verificación por **SMS**. En este caso, tendrás que crear una cuenta gratuita en Twilio.

Los **códigos 2FA generados son TOTP** (contraseña de un solo uso basada en el tiempo) y, por lo tanto, son de un solo uso.

Por lo tanto, no es posible reutilizar un código 2FA que ya se ha utilizado. Esto evita el robo y luego el uso de un código 2FA al observar al usuario mientras ingresa su código.

Requisitos

La autenticación de dos factores requiere TSplus Remote Access **Mobile Web** o **Enterprise** Editions.

La autenticación de dos factores es compatible con:

1. Portal web de **acceso remoto TSplus**, para conexiones HTML5 y Remoteapp
2. TSplus Connection Client, para clientes generados desde la versión 15.30.3.15, con soporte 2FA habilitado explícitamente. Ver

Compatibilidad con Portable Client Generator para autenticación de dos factores : 2FA está relacionado con usuarios de Windows y no con credenciales web

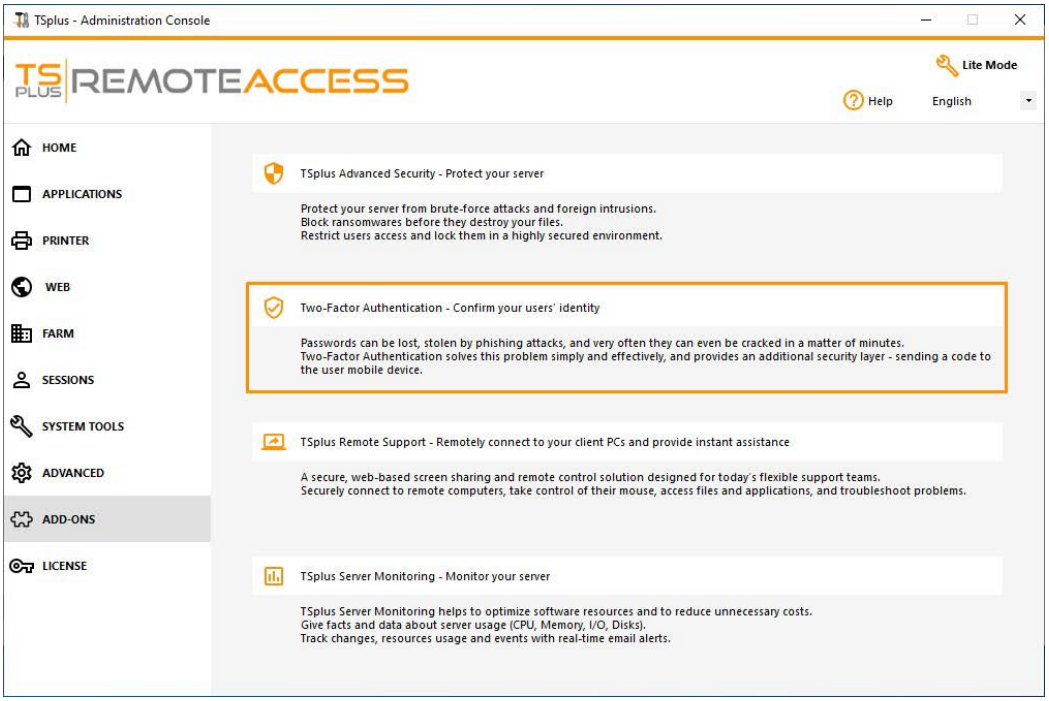
Este modo de autenticación no admite el inicio de sesión a través del cliente de escritorio remoto de Microsoft estándar (mstsc.exe).

Con el fin de proporcionar una solución aún más segura, las conexiones RDP se niegan para los usuarios habilitados para 2FA.

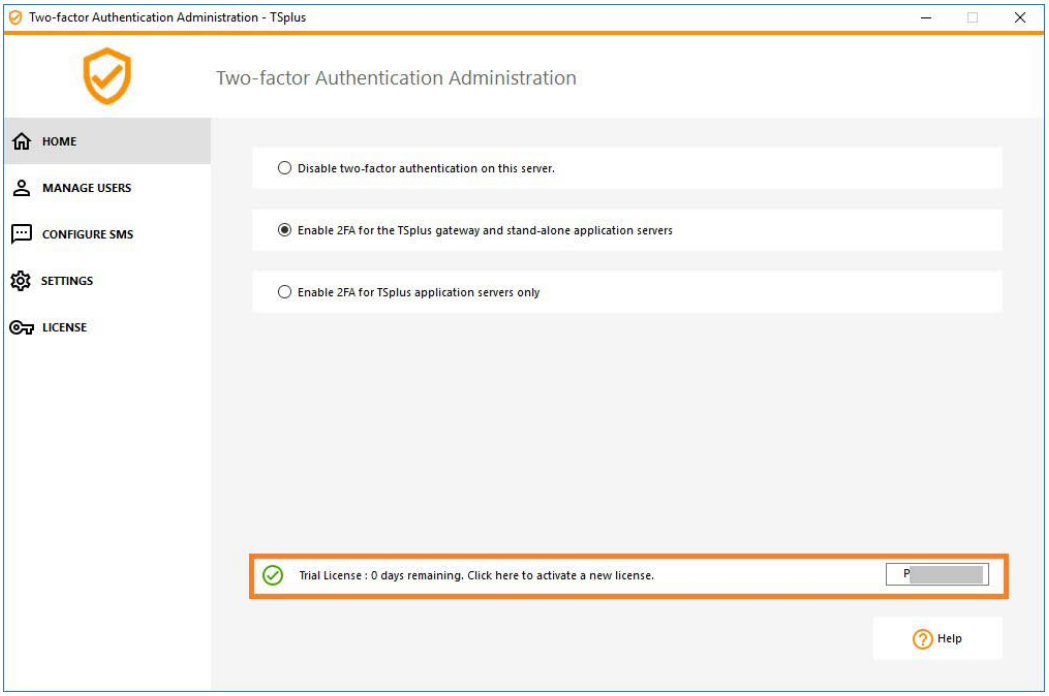
Como requisito previo, el servidor TSplus y los dispositivos deben llegar a tiempo. Consulte las secciones Sincronización de hora y Configuración para obtener más información sobre la configuración.

Activación de la licencia complementaria de autenticación de dos factores

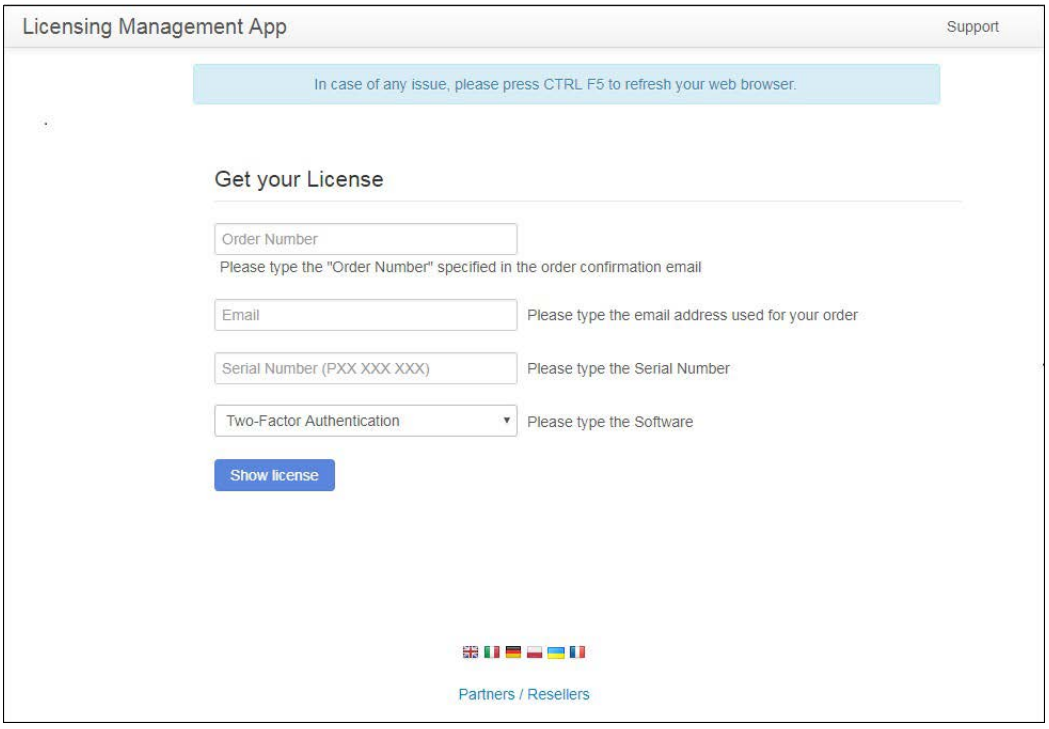
La función de autenticación de dos factores se puede encontrar en la pestaña Complemento de la AdminTool:



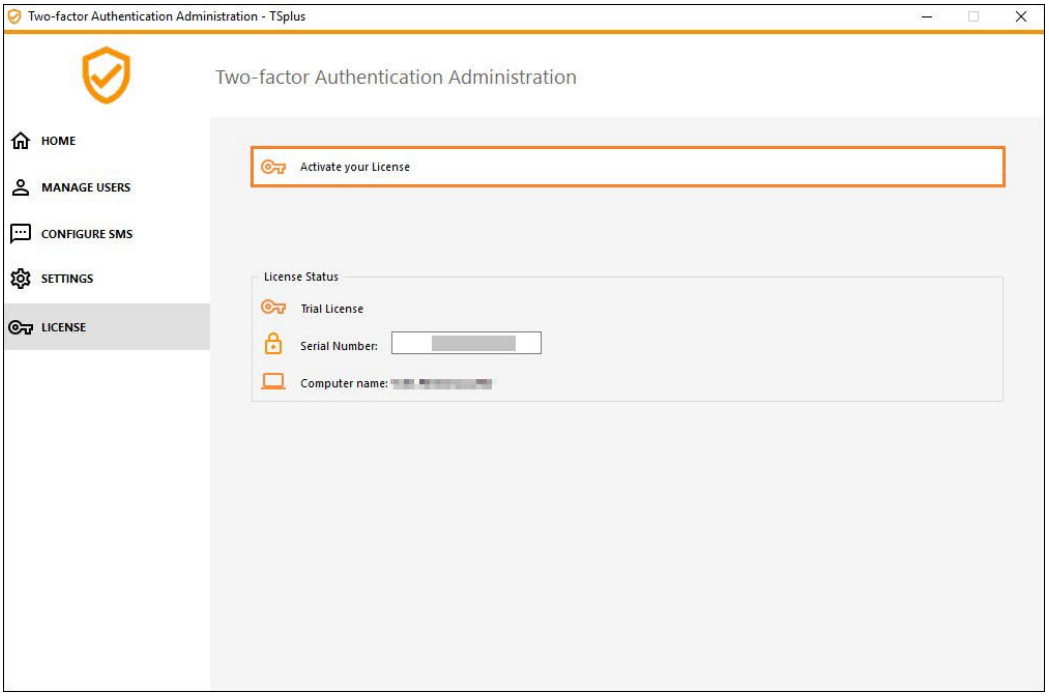
Está disponible como una prueba de 30 días para 10 usuarios. Para activar su licencia, copie el número de serie que puede encontrar en la parte inferior del mosaico Inicio:

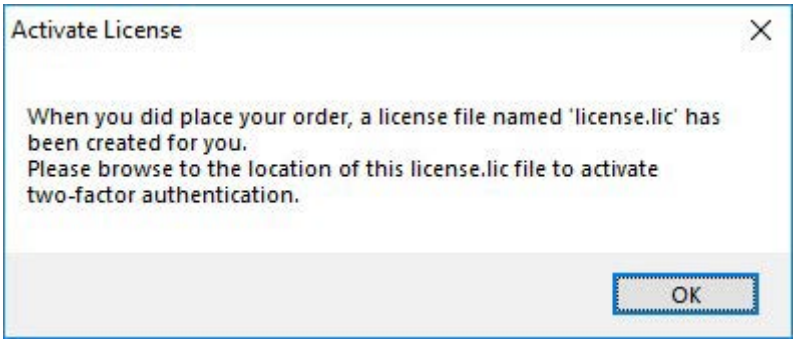


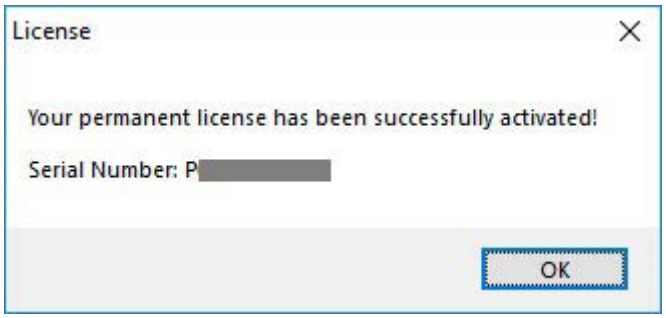
Luego, conéctese a nuestro Portal de licencias e ingrese su número de pedido, su dirección de correo electrónico, número de serie y seleccione "Autenticación de dos factores" en la lista desplegable a continuación:



Obtendrá su archivo license.lic. Luego, vaya a la pestaña *Licencia* y active el botón "Activar su licencia":



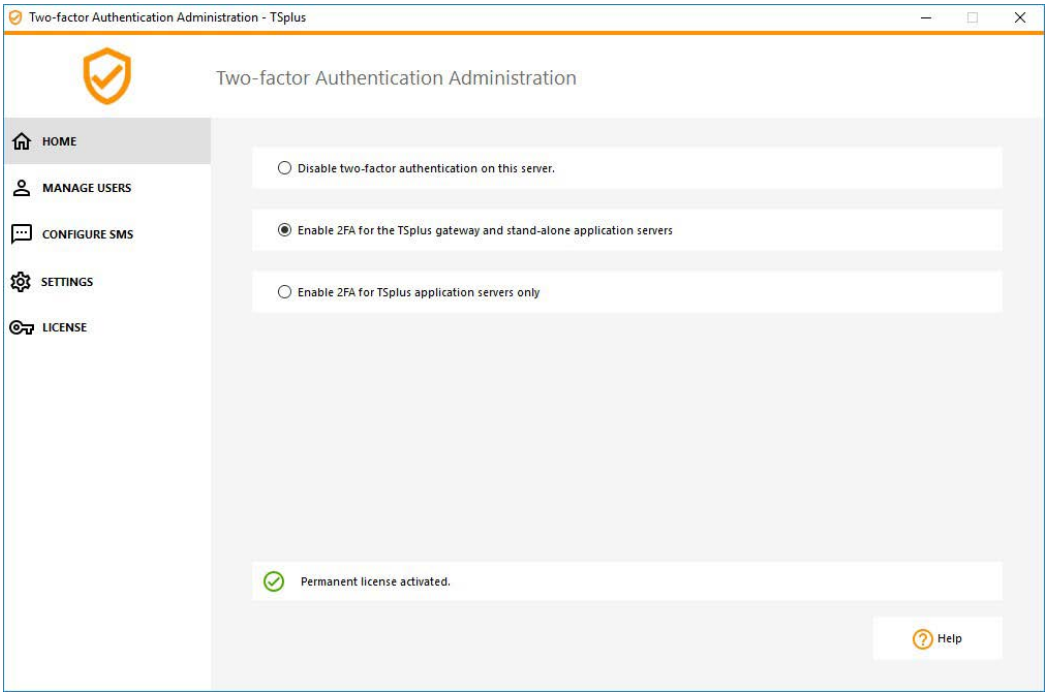




Habilitar la autenticación de dos factores

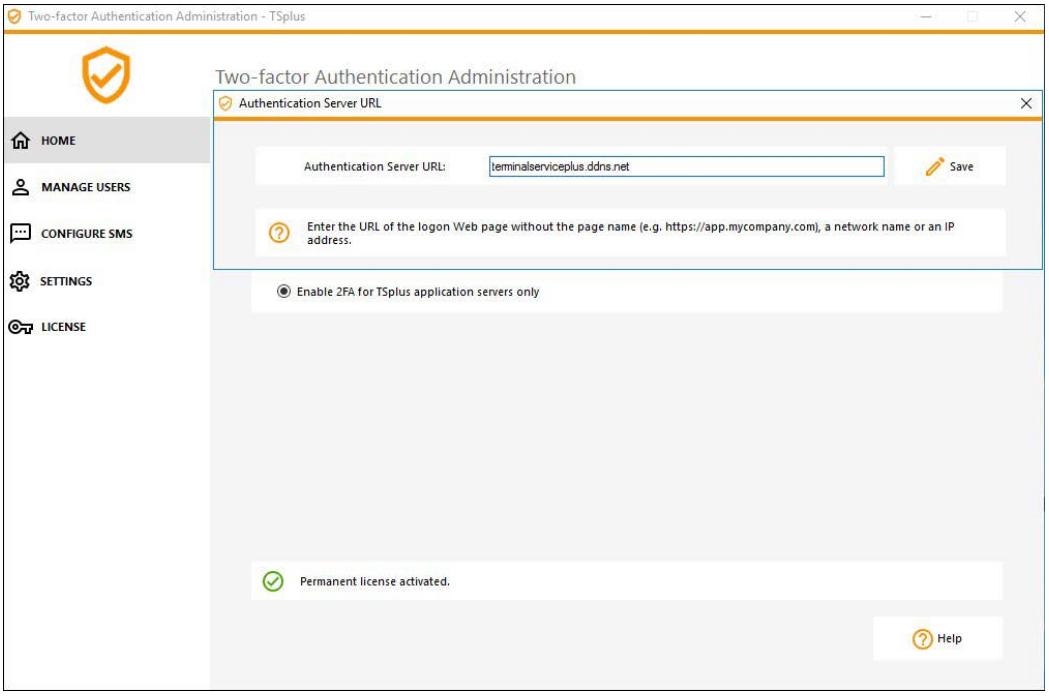
Realice los pasos siguientes para habilitar la autenticación de dos factores para su servidor TSplus o implementación. Si la implementación de TSplus está configurada para utilizar varios servidores, realice esta tarea en el servidor TSplus expuesto como punto de entrada único para los usuarios o con el rol de proxy inverso.

1) Abra la aplicación de administración de autenticación de dos factores. Se muestran el estado de autenticación de dos factores y el estado de la licencia:

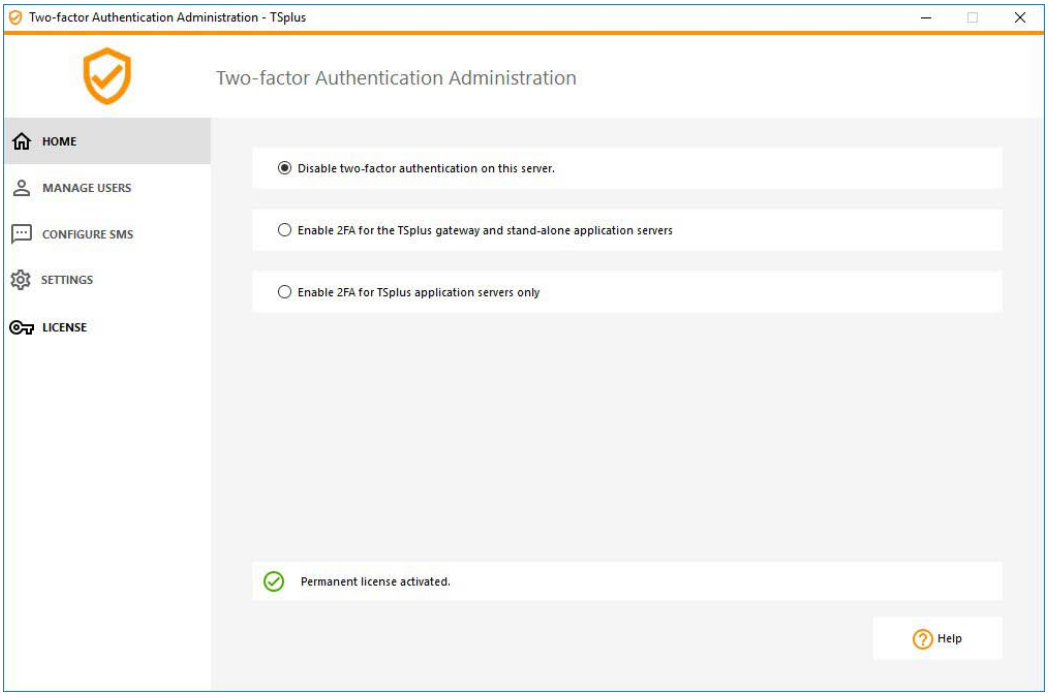


De forma predeterminada, 2FA está habilitado para la puerta de enlace TSplus y los servidores de aplicaciones independientes.

Puede habilitarlo solo para servidores de aplicaciones TSplus, introduciendo la URL del servidor de autenticación:



O desactívelo:

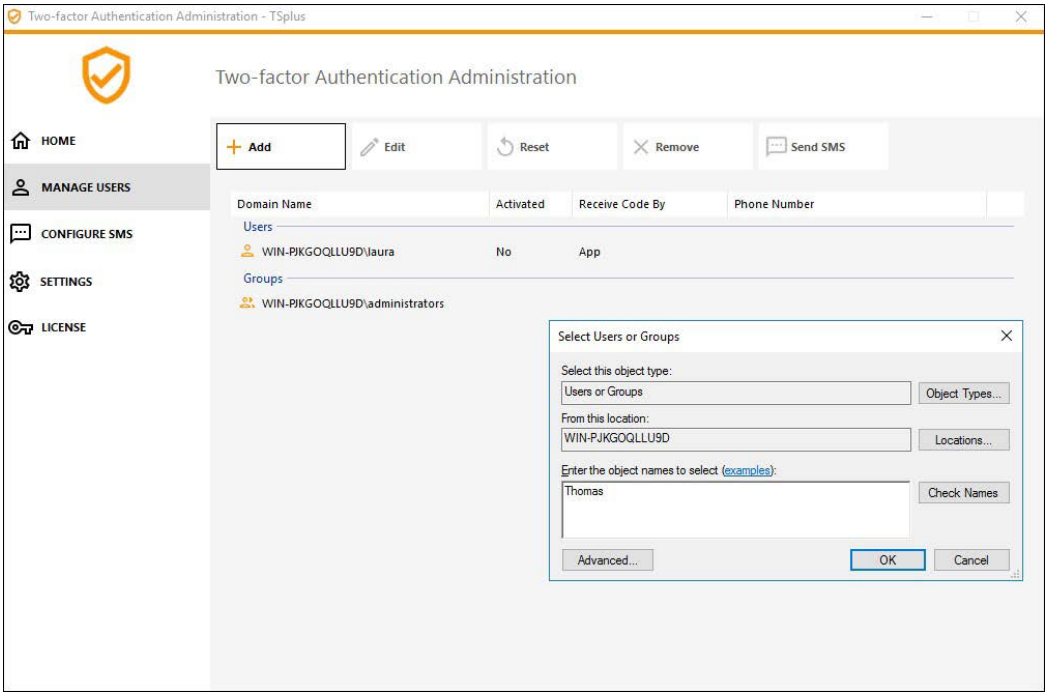


Agregar usuarios y grupos

Una vez habilitada la autenticación de dos factores, puede configurar usuarios para la autenticación de dos factores.

1. Desde la aplicación de administración de autenticación de dos factores, haga clic en la *pestaña Administrar usuarios*.

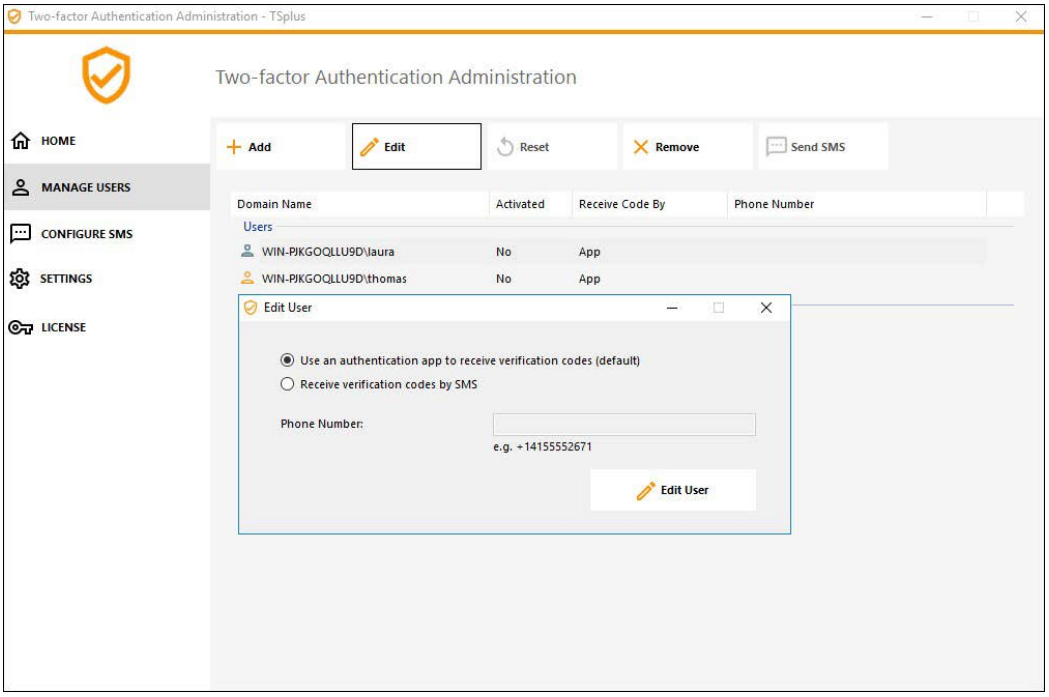
1. Luego, haga clic en *Agregar* para seleccionar usuarios y / o grupos de usuarios. Se abrirá el *cuadro Seleccionar usuarios o grupos*.



1. Agregue tantos usuarios y grupos como sea necesario y, a continuación, haga clic en *Aceptar*. Los usuarios y grupos se agregan a la lista y se habilitan para la autenticación de dos factores.

Editar usuarios

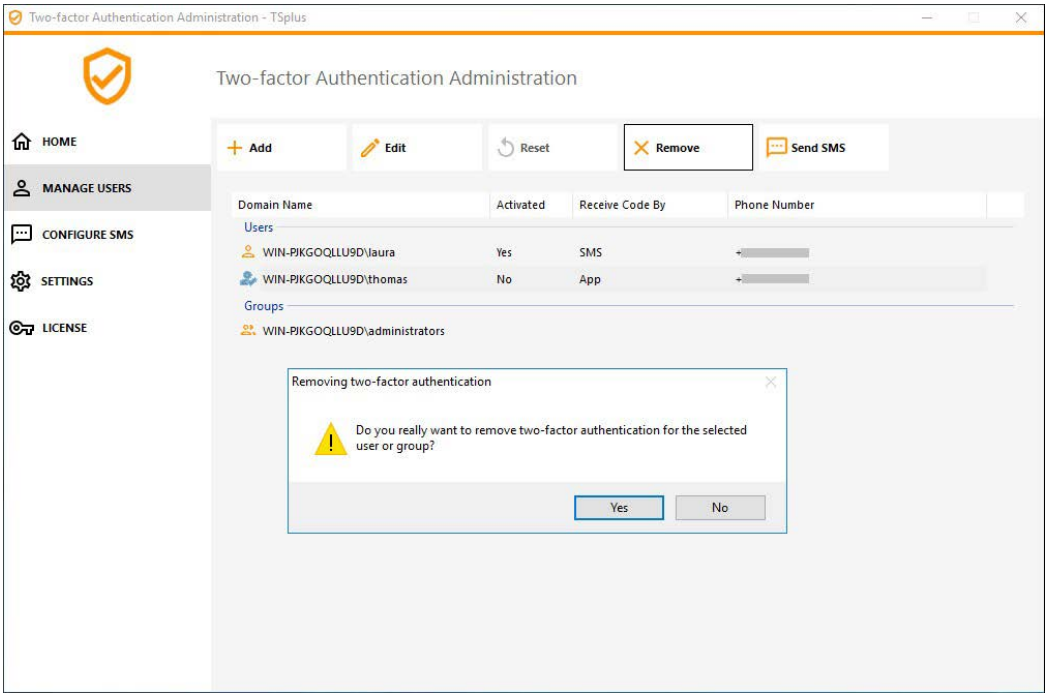
En el mismo mosaico, puede editar la forma en que los usuarios reciben los códigos de verificación seleccionando un usuario y haciendo clic en el botón "Editar":



El usuario recibe códigos de verificación en la aplicación de autenticación de forma predeterminada. Puede elegir que lo reciba por SMS seleccionando la opción y agregando el número de teléfono del usuario en el campo a continuación.

Quitar 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.



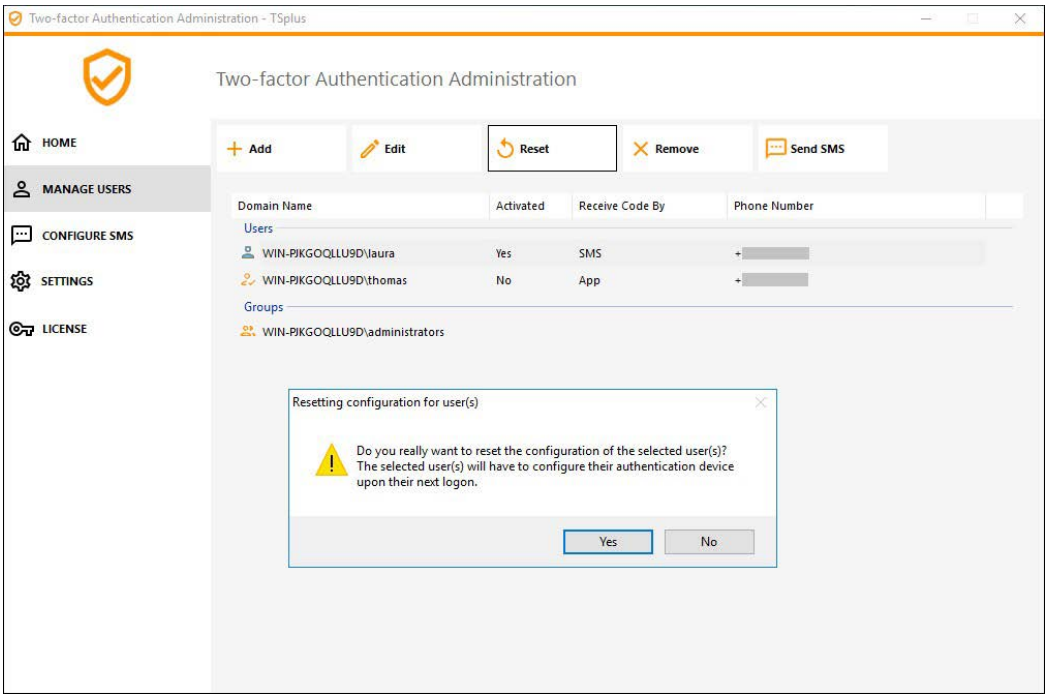
Haga clic en *Sí*. El usuario o el grupo se eliminan de su lista y ya no se conectarán mediante la autenticación de dos factores.

Restablecer la configuración para los usuarios

En caso de pérdida del dispositivo de autenticación para un usuario, o si el usuario necesita mostrar el código QR secreto nuevamente, debe restablecer la configuración de autenticación del usuario.

1. Desde la aplicación de administración de autenticación de dos factores, haga clic en la *pestaña Administrar usuarios*.

2. Seleccione uno o varios usuarios activados y luego haga clic en *Restablecer*. Se muestra un mensaje de confirmación:



1. Haga clic en *Sí*. A los usuarios seleccionados se les presentará un nuevo código QR en el próximo inicio de sesión y tendrán que escanearlo en la aplicación de autenticación de su dispositivo.

También puede modificar el número de teléfono del usuario para que pueda recibir un código de verificación en su nuevo dispositivo.

Inscribir al 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, tiene 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.

Puede 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

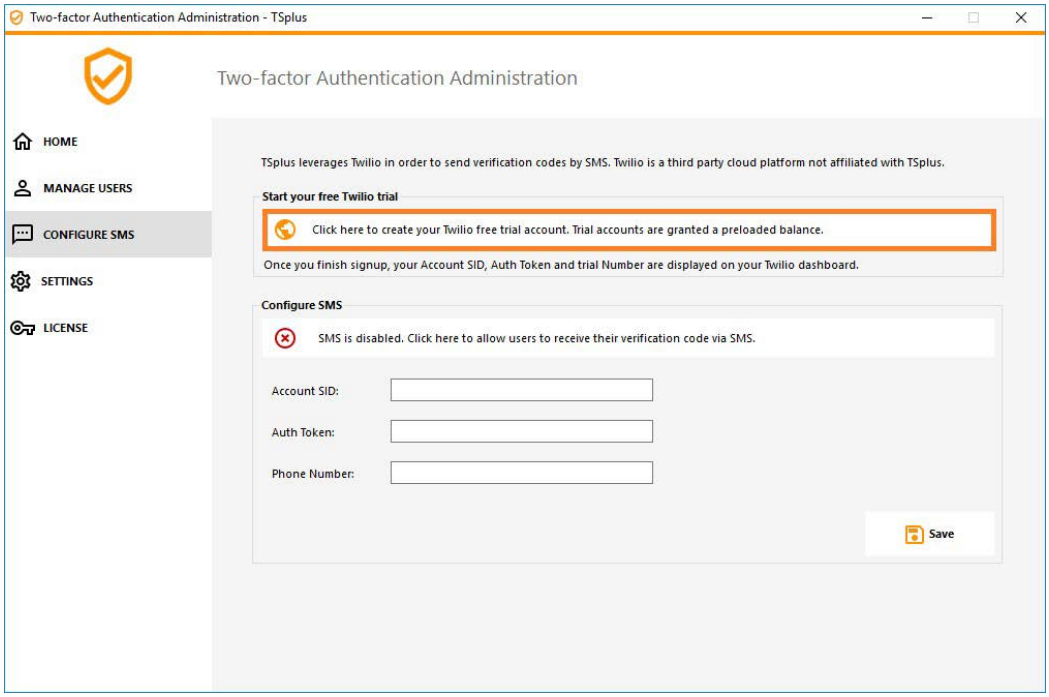
Utilice la documentación de cada aplicación para obtener más detalles sobre cómo proceder para agregar su cuenta TSplus.

Configurar SMS

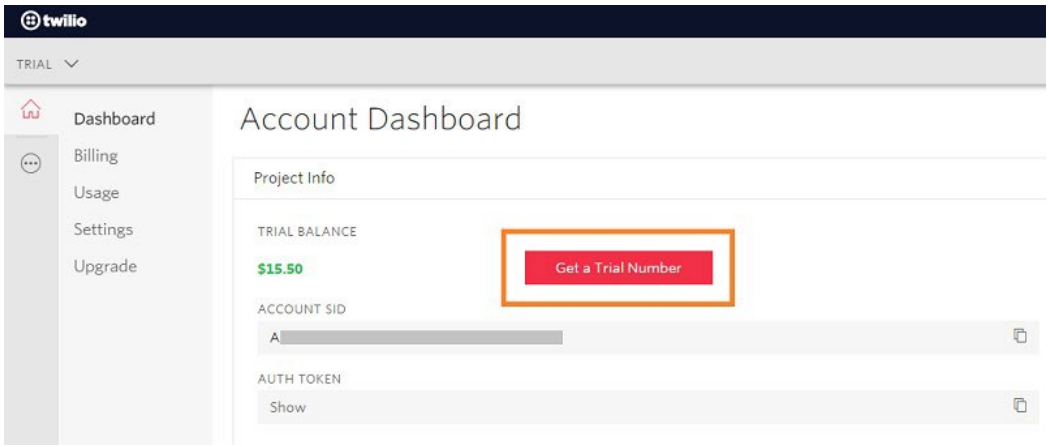
Para que el usuario reciba códigos de verificación por SMS, primero debe habilitarlo. Haga clic en la *pestaña Configurar SMS*:

TSplus aprovecha Twilio para enviar códigos de verificación por SMS. Twilio es una plataforma en la nube de terceros, no afiliada a TSplus.

1. Simplemente cree una cuenta gratuita en Twilio haciendo clic en el botón de abajo "Comience su prueba gratuita con Twilio":

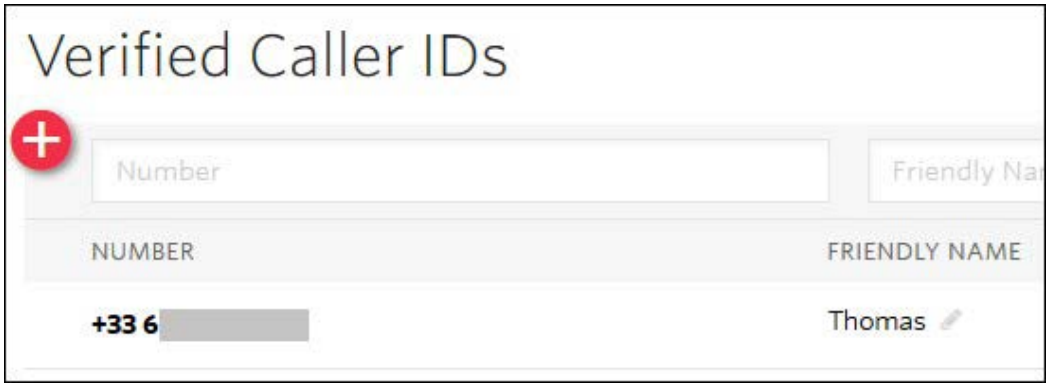


1. En el panel de control de tu cuenta de Twilio, tendrás que activar tu número de prueba:

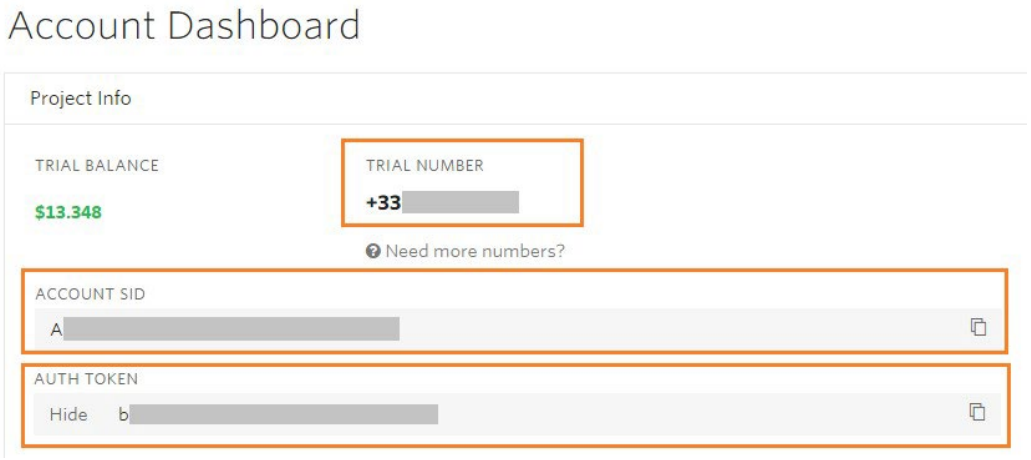


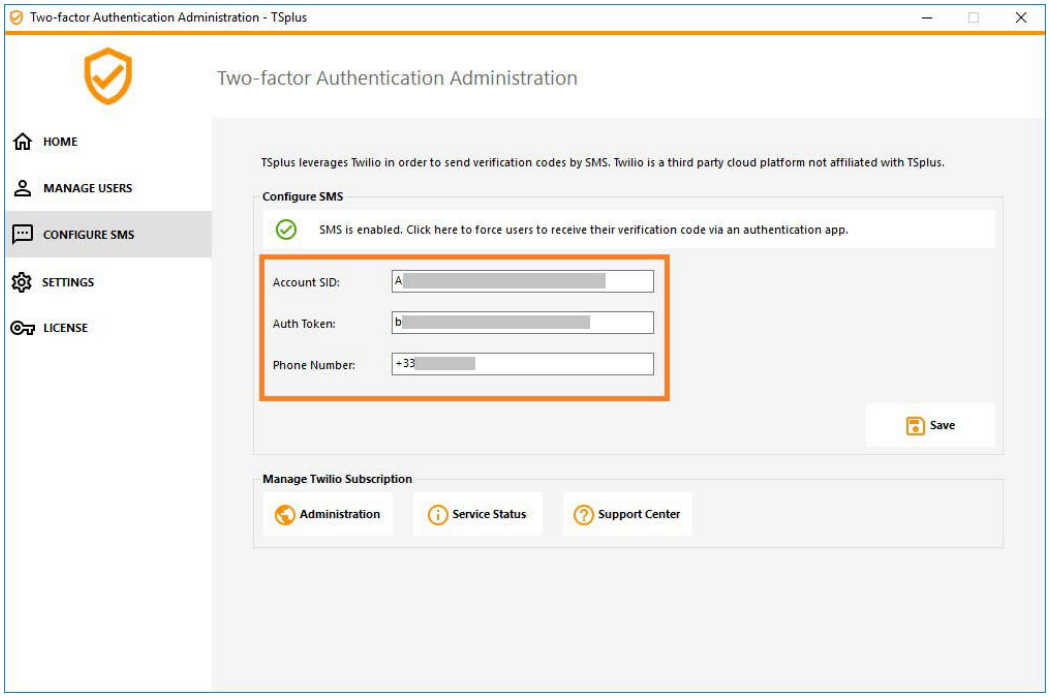
1. El siguiente paso solo es necesario para las versiones de prueba. Permite a Twilio verificar el número de teléfono real en el que se enviarán los SMS.

Ingrese este número en el menú "Números de teléfono" - pestaña "Identificadores de llamadas verificados" :

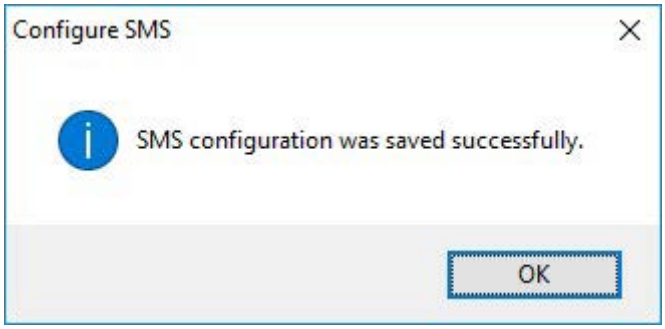


1. A continuación, podrá introducir el SID de su cuenta, el token de autenticación y el **número de prueba** como número de teléfono en la *pestaña Configurar SMS* de TSplus:





Luego, haga clic en Guardar. Se mostrará el siguiente mensaje:



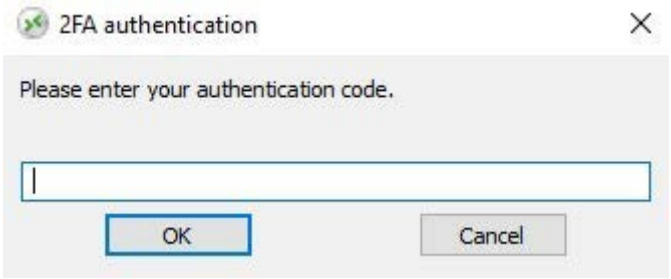
Puede administrar su suscripción a Twilio en la sección Administrar suscripción a Twilio, *en la parte inferior de la* pestaña Configurar SMS. *Administre su cuenta, vea el estado del servicio o comuníquese con el Centro de soporte de Twilio simplemente haciendo clic en los botones correspondientes.*

Iniciar sesión con autenticación de dos factores

Una vez que un usuario haya configurado su cuenta TSplus en su aplicación de autenticación, podrá conectarse utilizando su contraseña y el código proporcionado por su aplicación de autenticación o por SMS.

Desde el portal web de acceso remoto de TSplus:

Desde el cliente generado por TSplus:



Sincronización horaria

Los servidores de aplicaciones y los dispositivos cliente de TSplus deben compartir la misma hora. Esto significa que la hora y la fecha del servidor deben sincronizarse con un servidor horario. Los dispositivos cliente también deben tener sincronización horaria, 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 la hora del servidor no están sincronizadas, esta solicitud puede ser rechazada.

La validación de la información entre el Dispositivo y el servidor se refiere a la hora UTC.
En la sección **Configuración**, el parámetro Discrepency se usa para administrar el período de validez del código, en intervalos de 30 segundos.

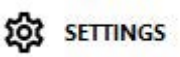
Ejemplo de validación o autenticación válida:

- el servidor está sincronizado con un servidor horario, la zona horaria es UTC + 2, son las 2:30 pm el dispositivo está sincronizado con un servidor horario, la zona horaria es UTC + 1, es 1:30 pm el parámetro Discrepency se configura 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:

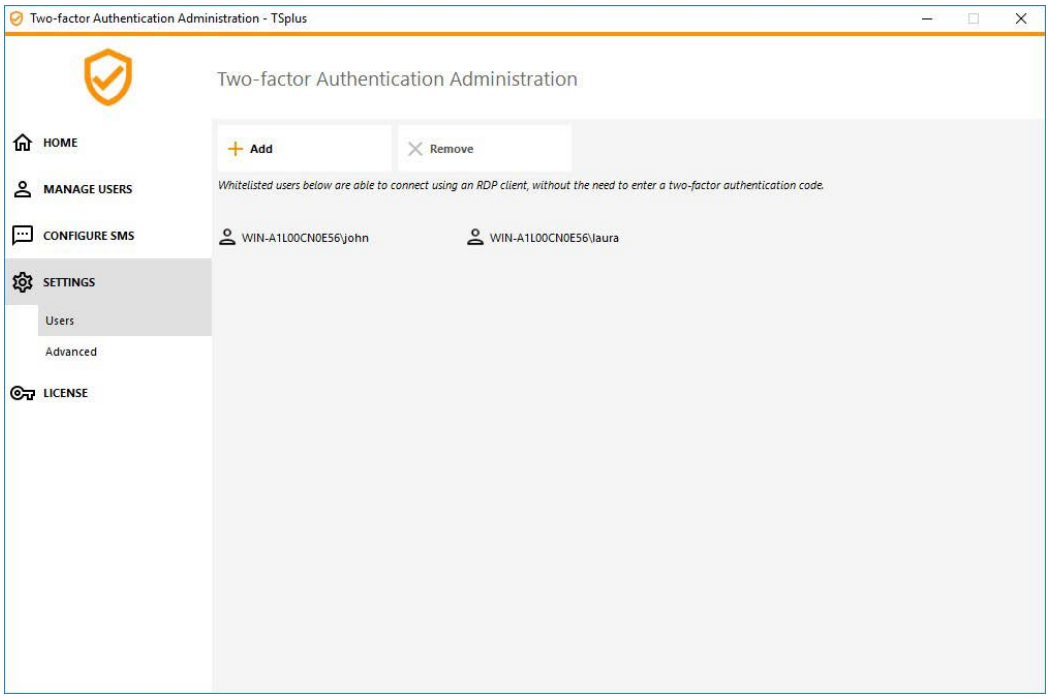
- el servidor está sincronizado con un servidor horario, la zona horaria es UTC + 2, son las 2:30 pm
- el dispositivo no está sincronizado con un servidor horario, la zona horaria es UTC-1, la hora se establece manualmente en 1:30 pm el parámetro Discrepency se configura en 60, es decir, un período de validez del código de 30 minutos la hora del servidor a la que se hace referencia la hora UTC es 12:30 am
- la hora comunicada por el Dispositivo, referida a la hora UTC es 2:30 pm
- la diferencia es de 120 minutos, por lo que se rechaza el código de validación.

Configuración

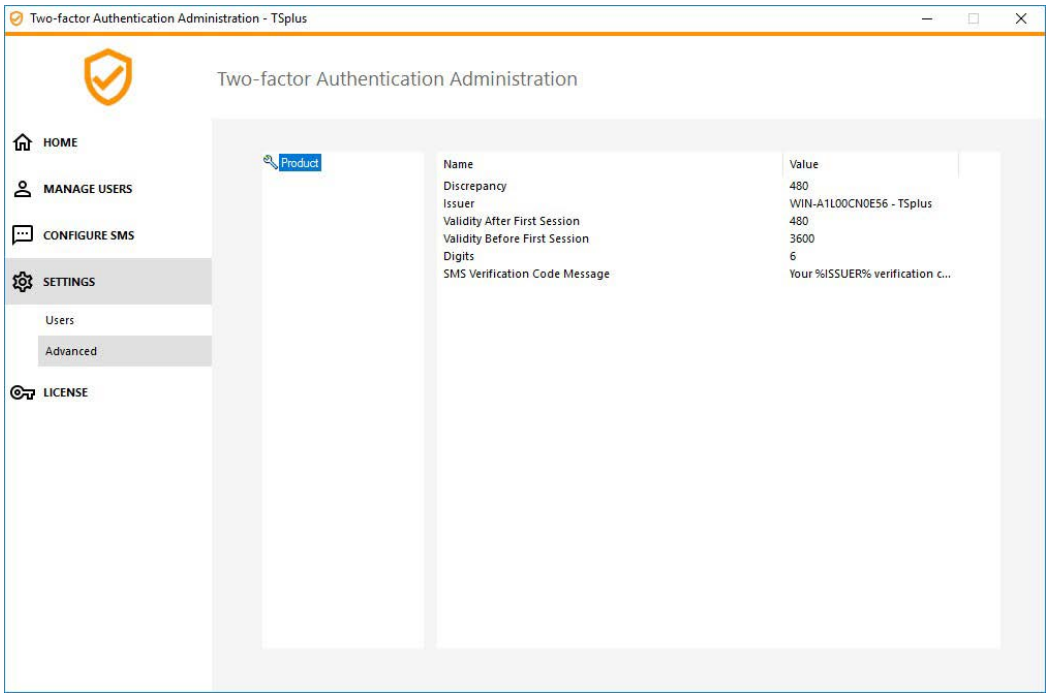


La pestaña Configuración le permite incluir usuarios **en la lista blanca para que se conecten mediante un cliente RDP, sin necesidad de introducir un código de autenticación doble.**

Haga clic en el botón "Agregar" para agregar un usuario y eliminar un usuario seleccionándolo y haciendo clic en el botón "Eliminar".

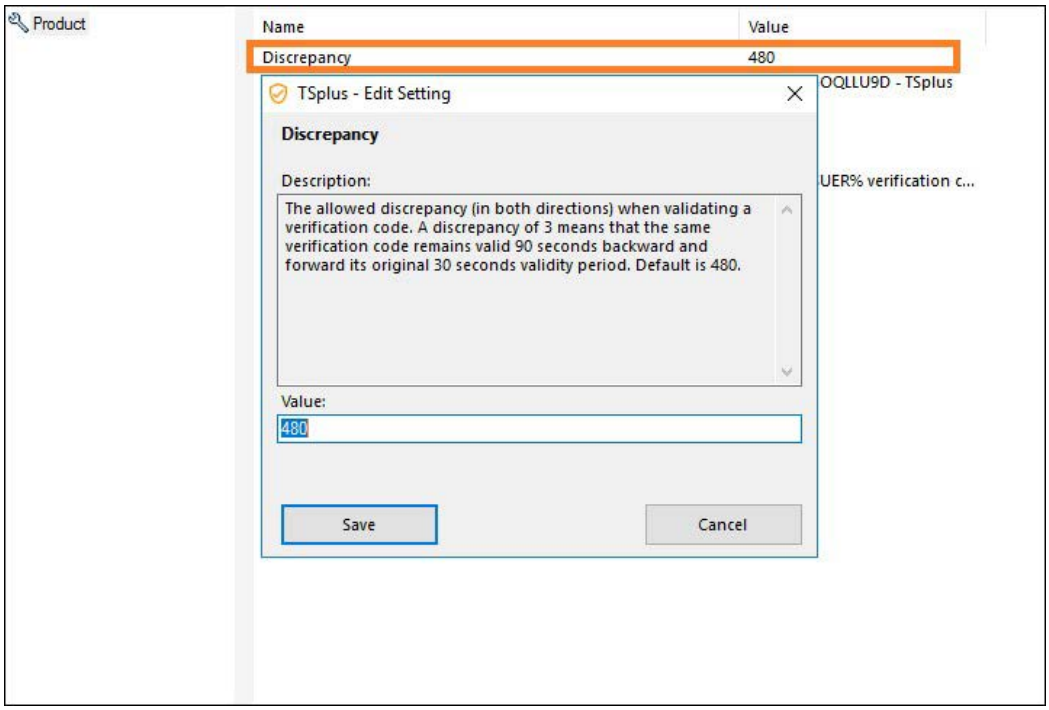


La pestaña Avanzado le permite configurar la autenticación de dos factores en profundidad.



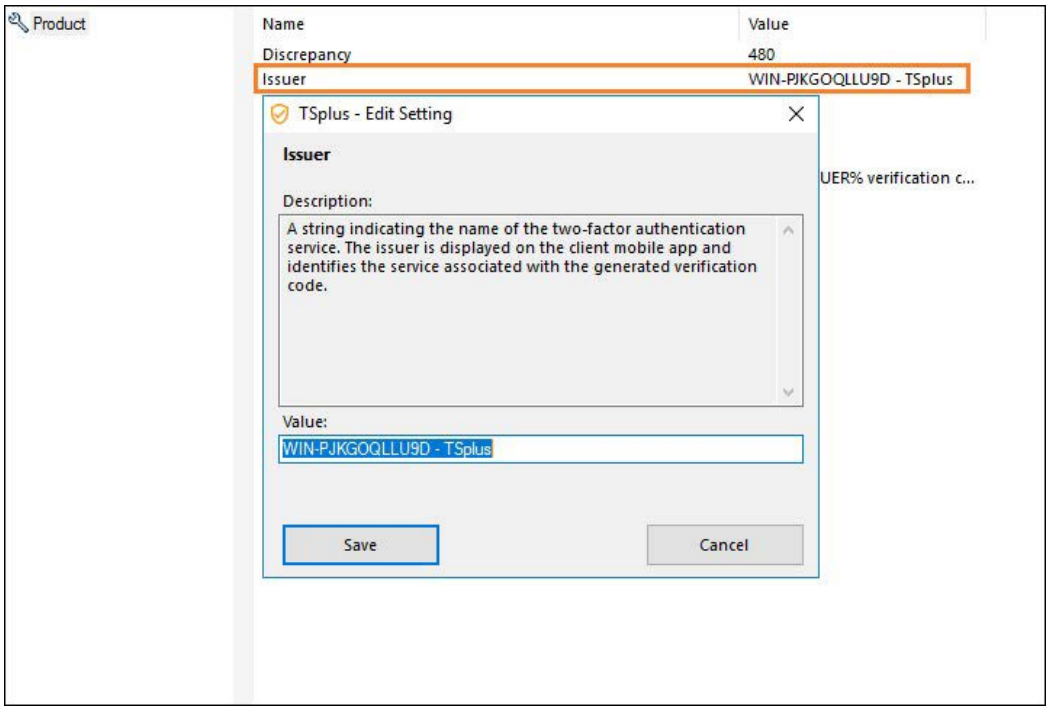
Discrepancia

Puede modificar el valor Discrepancia, que le 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 su período de validez original de 30 segundos. El valor predeterminado es 480, lo que significa 480 x 30 segundos = 4 horas.



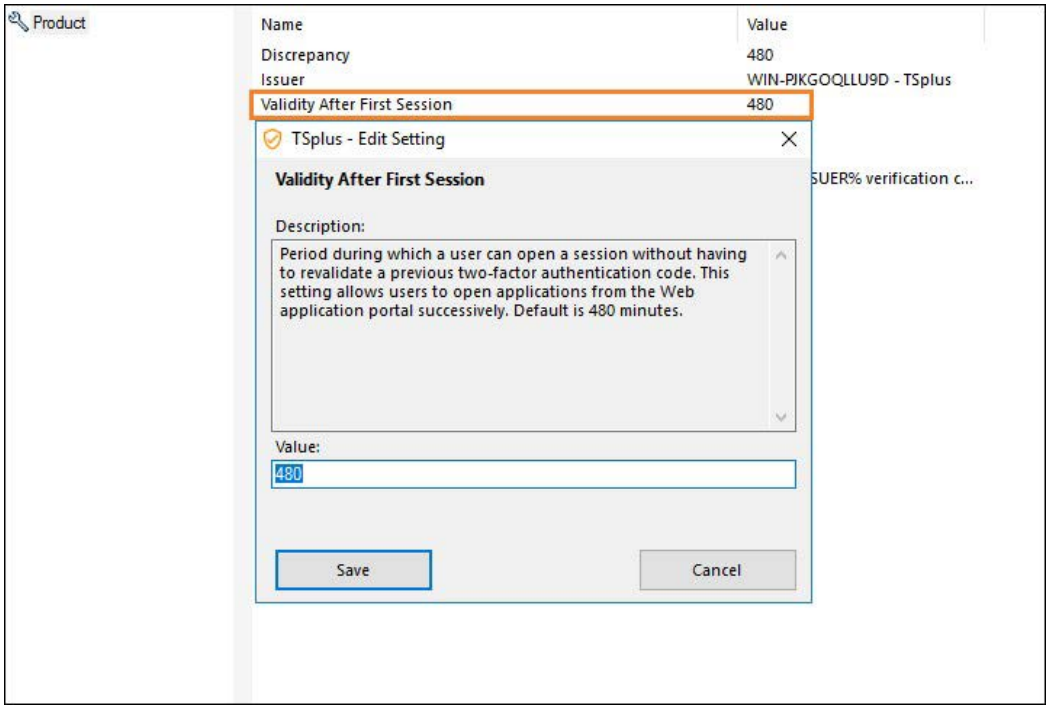
Emisor

Una cadena que indica el nombre del servicio de autenticación de dos factores. El emisor se muestra en la aplicación móvil cliente e identifica el servicio asociado con el código de verificación generado. De forma predeterminada, se compone del nombre del servidor con TSplus.



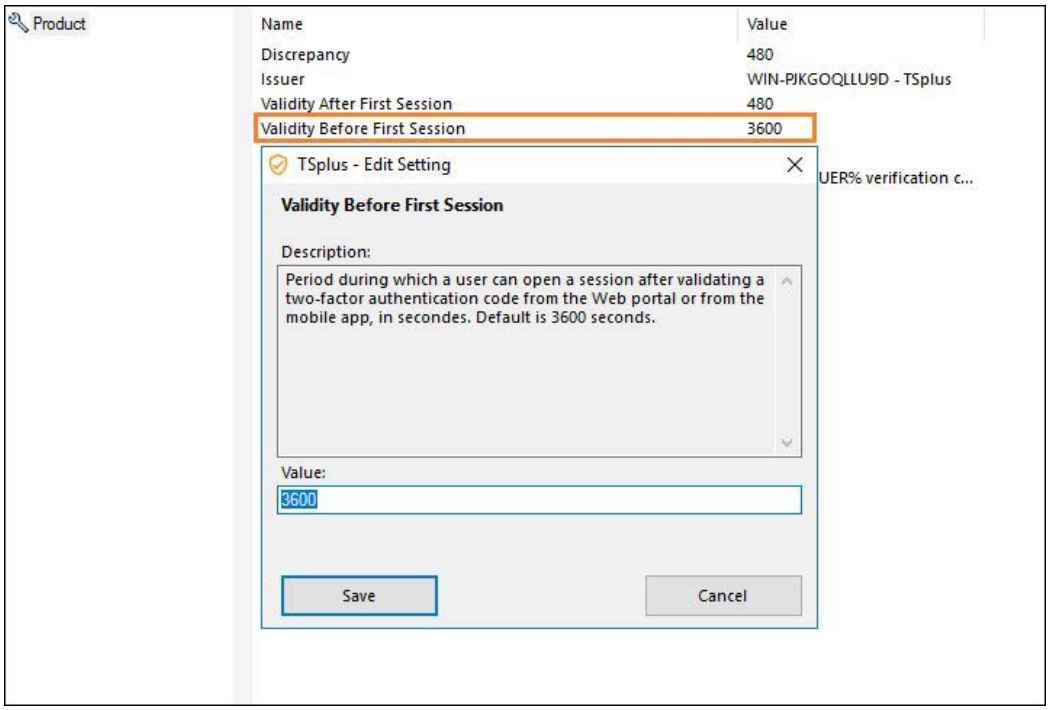
Validez después de la primera sesión

Período durante el cual un usuario puede abrir una sesión sin tener que revalidar un código de autenticación de dos factores anterior. Esta configuración permite a los usuarios abrir aplicaciones desde el portal de aplicaciones web sucesivamente. El valor predeterminado es 480 minutos.



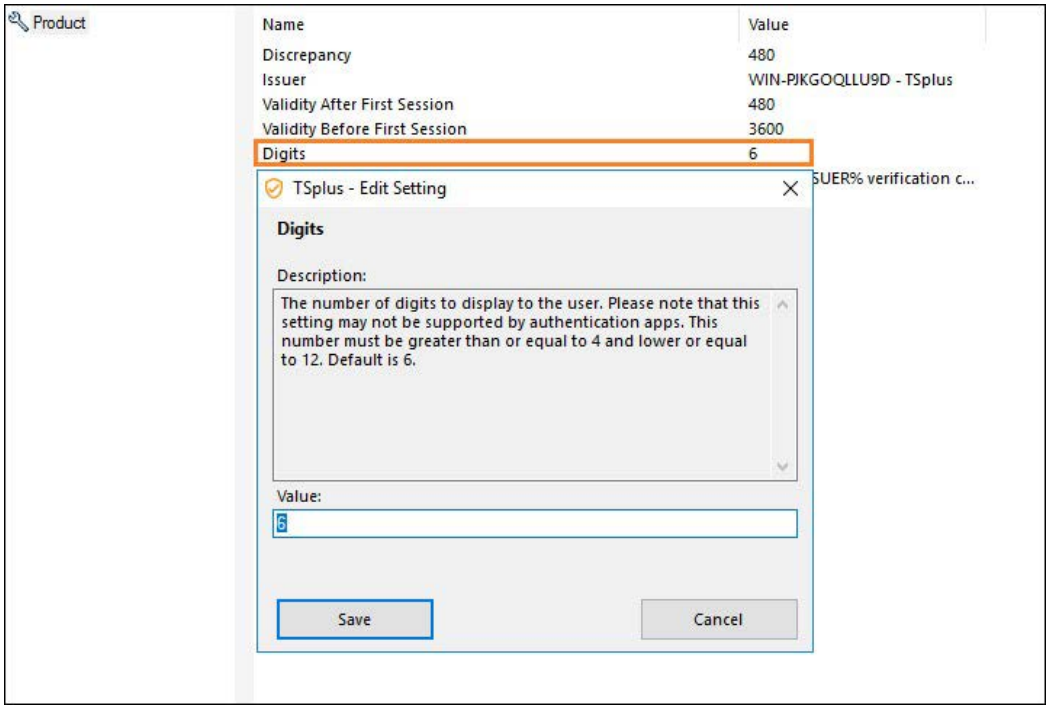
Validez antes de la primera sesión

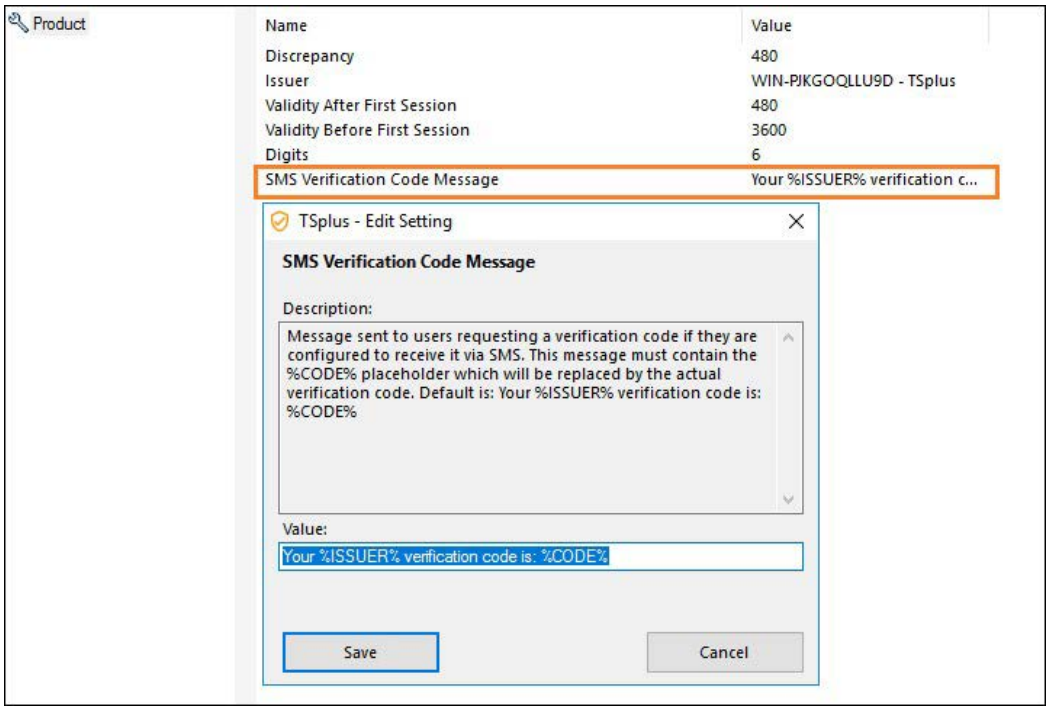
Período durante el cual un usuario puede abrir una sesión después de validar un código de autenticación de dos factores desde el portal web o desde la aplicación móvil, en secondes. El valor predeterminado es 3600 segundos.



Dígitos

Número de dígitos que se van a mostrar al usuario. Tenga en cuenta que es posible que esta configuración no sea compatible con las aplicaciones de autenticación. Este número debe ser mayor o igual a 4 e inferior o igual a 12. El valor predeterminado es 6.



Mensaje de código de verificación por SMS

Mensaje enviado a los usuarios solicitando un código de verificación si están configurados para recibirlo a través de SMS. Este mensaje debe contener el marcador de posición %CODE% que será reemplazado por el código de verificación real. El valor predeterminado es: El código de verificación %ISSUER% es: %CODE%