Two-factor Authentication

Two-factor authentication adds an extra layer of security and **prevents access to your users' session even if someone knows their password**.

A combination of two different factors is used to achieve a greater level of security:

1) something they know, **a password**.
2) something they have, a **device - such as a smartphone - with an authentication app installed.**.

You can use one of the following authenticator apps to proceed. These apps are available across a wide range of platforms:
- Authy
- Google Authenticator
- Microsoft Authenticator

Each time a user sign in to its remote session it will need its password and a verification code available from its mobile phone. Once configured, the authenticator app will display a verification code to allow him or her to log in any time. It works even if its device is offline.

OR you can decide to receive verification codes by **SMS**. In this case, you will have to create a free account on Twilio.

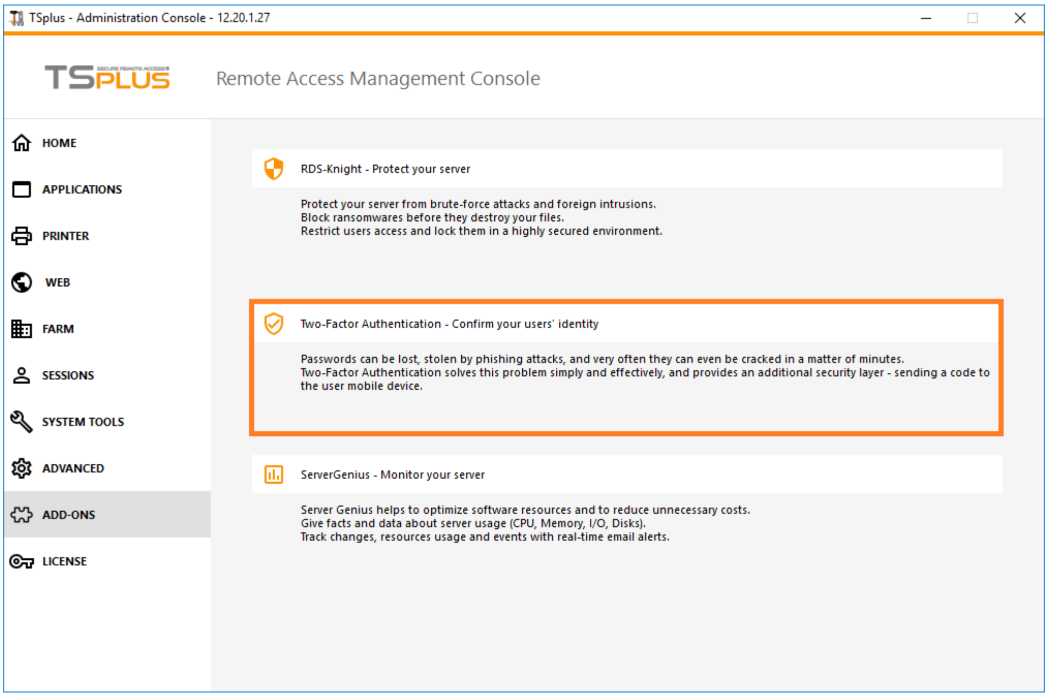
Two-factor authentication is available with **HTML5 and Remoteapp connections on TSplus Web portal only**, on **TSplus Mobile Web and Enterprise Editions**. This authentication mode does not support login through Remote Desktop client.

In order to provide an even safer solution, RDP connections are denied for 2FA enabled users.

As a prerequisite, TSplus server and Devices must be on time. See the Time Synchronization and Settings sections for more configuration information.

Activating the Two-factor Authentication Add-On License

The Two-Factor Authentication feature can be found on the Add-On tab of the AdminTool:



RDS-Knight - Protect your server

Protect your server from brute-force attacks and foreign intrusions.
Block ransomwares before they destroy your files.
Restrict users access and lock them in a highly secured environment.

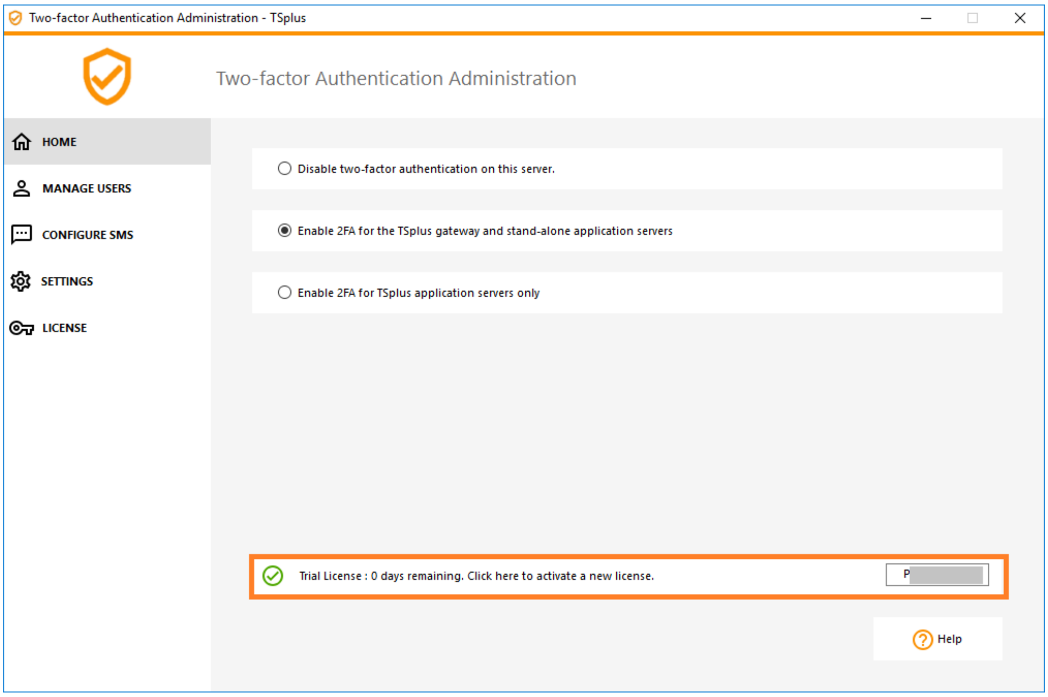
Two-Factor Authentication - Confirm your users' identity

Passwords can be lost, stolen by phishing attacks, and very often they can even be cracked in a matter of minutes.
Two-Factor Authentication solves this problem simply and effectively, and provides an additional security layer - sending a code to the user mobile device.

ServerGenius - Monitor your server

Server Genius helps to optimize software resources and to reduce unnecessary costs.
Give facts and data about server usage (CPU, Memory, I/O, Disks).
Track changes, resources usage and events with real-time email alerts.

It is available as a 30-day trial for 10 users. To activate your license, copy the serial number you can find at the bottom of the Home tile:


Two-factor Authentication Administration - TSplus
Two-factor Authentication Administration
HOME
MANAGE USERS
CONFIGURE SMS
SETTINGS
LICENSE
Help

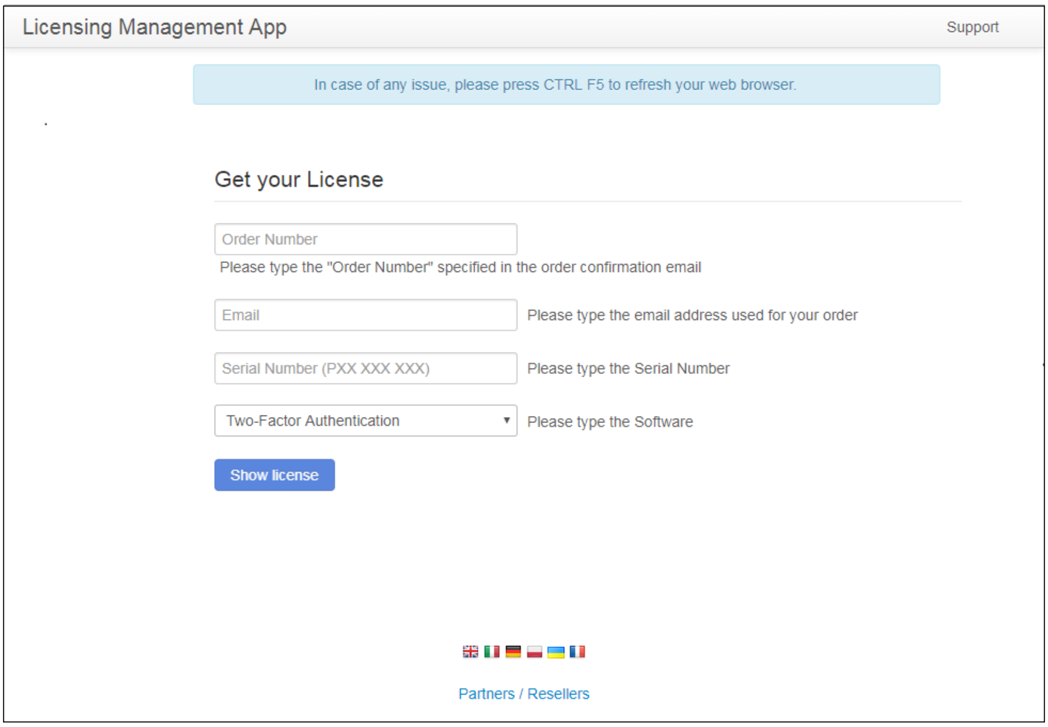
○ Disable two-factor authentication on this server.

● Enable 2FA for the TSplus gateway and stand-alone application servers

○ Enable 2FA for TSplus application servers only

Trial License : 0 days remaining. Click here to activate a new license. P[redacted]

Then, connect to our Licensing Portal and enter your Order Number, your e-mail address, Serial Number and select "Two-Factor Authentication" on the dropdown list below:



Licensing Management App

Support

In case of any issue, please press CTRL F5 to refresh your web browser.

Get your License

Order Number

Please type the "Order Number" specified in the order confirmation email

Email — Please type the email address used for your order

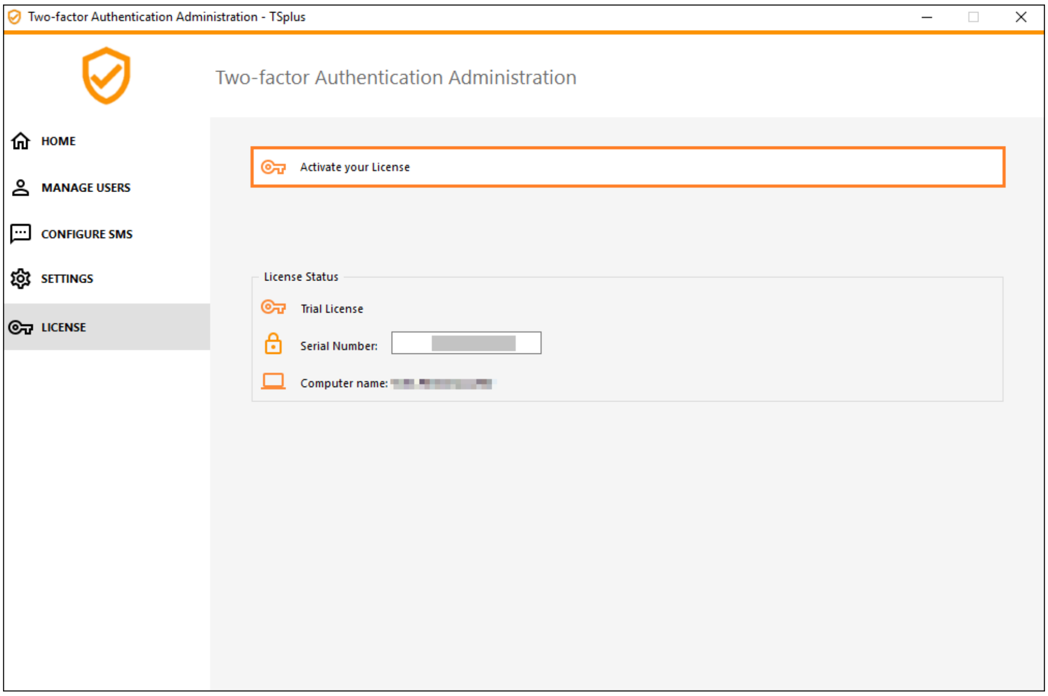
Serial Number (PXX XXX XXX) — Please type the Serial Number

Two-Factor Authentication ▾ — Please type the Software

Show license

Partners / Resellers

You will get your license.lic file. Then, go to the *License* tab and cick on the "Activate your license" button:



Two-factor Authentication Administration - TSplus

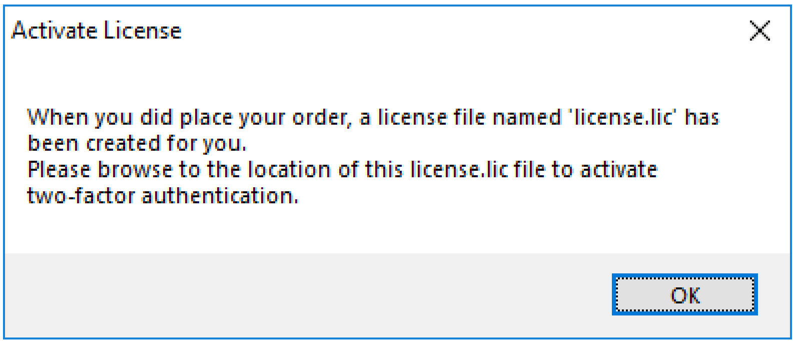
Two-factor Authentication Administration

License Status

Trial License

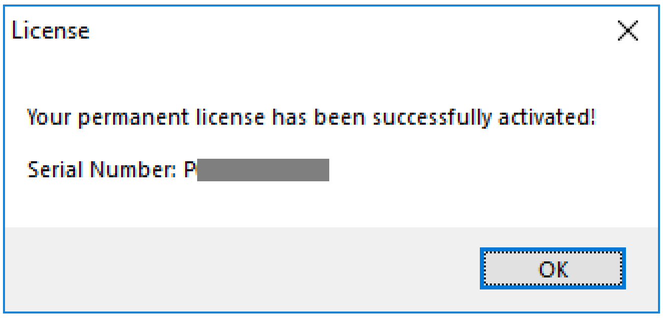
Serial Number: [redacted]

Computer name: [redacted]



Activate License

When you did place your order, a license file named 'license.lic' has been created for you.
Please browse to the location of this license.lic file to activate two-factor authentication.



License

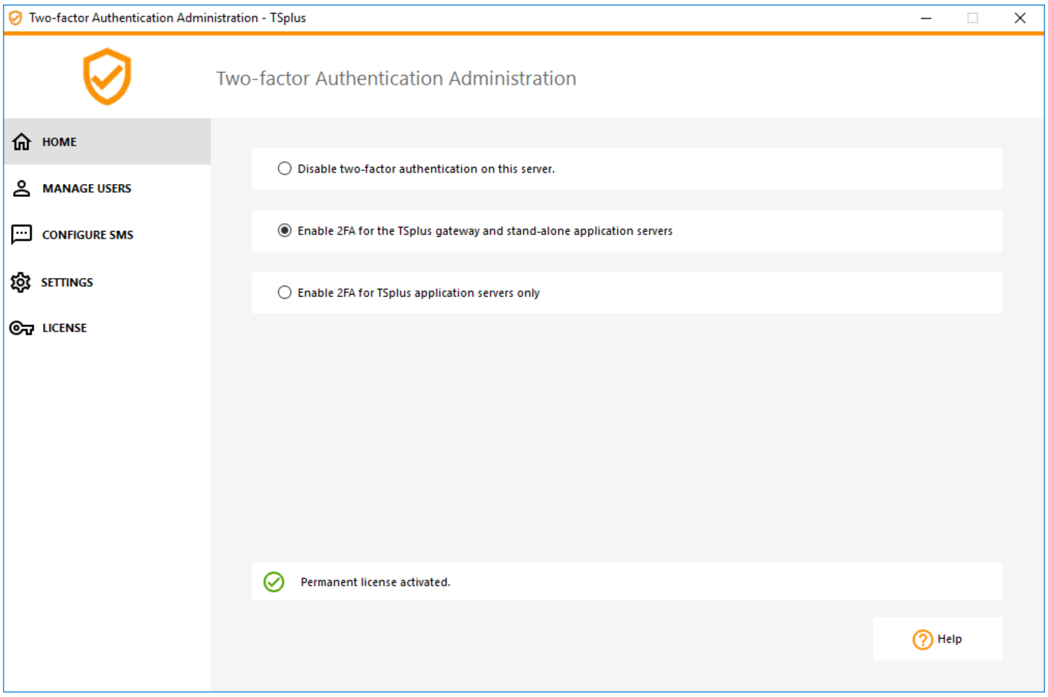
Your permanent license has been successfully activated!

Serial Number: P[redacted]

Enable Two-factor Authentication

Perform the following steps to enable two-factor authentication for your TSplus server or deployment. If your TSplus deployment is configured to use multiple servers, perform this task on the TSplus server exposed as the single point of entry for users or having the reverse proxy role.

1) Open the two-factor authentication administration application. The two-factor authentication status and the license status are displayed:



Two-factor Authentication Administration - TSplus

Two-factor Authentication Administration

○ Disable two-factor authentication on this server.

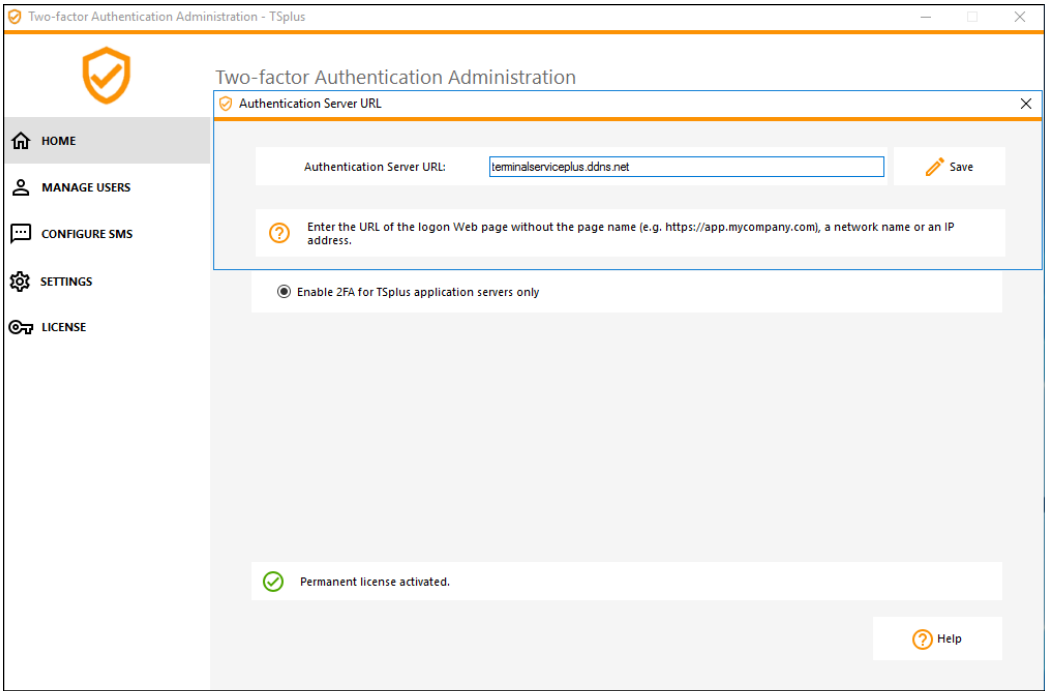
● Enable 2FA for the TSplus gateway and stand-alone application servers

○ Enable 2FA for TSplus application servers only

✓ Permanent license activated.

By default, 2FA is enabled for the TSplus gateway and stand-alone application servers.

You can enable it for TSplus application servers only, by entering the authentication server URL:


Two-factor Authentication Administration - TSplus
Two-factor Authentication Administration
HOME
MANAGE USERS
CONFIGURE SMS
SETTINGS
LICENSE
Authentication Server URL
Save
Help

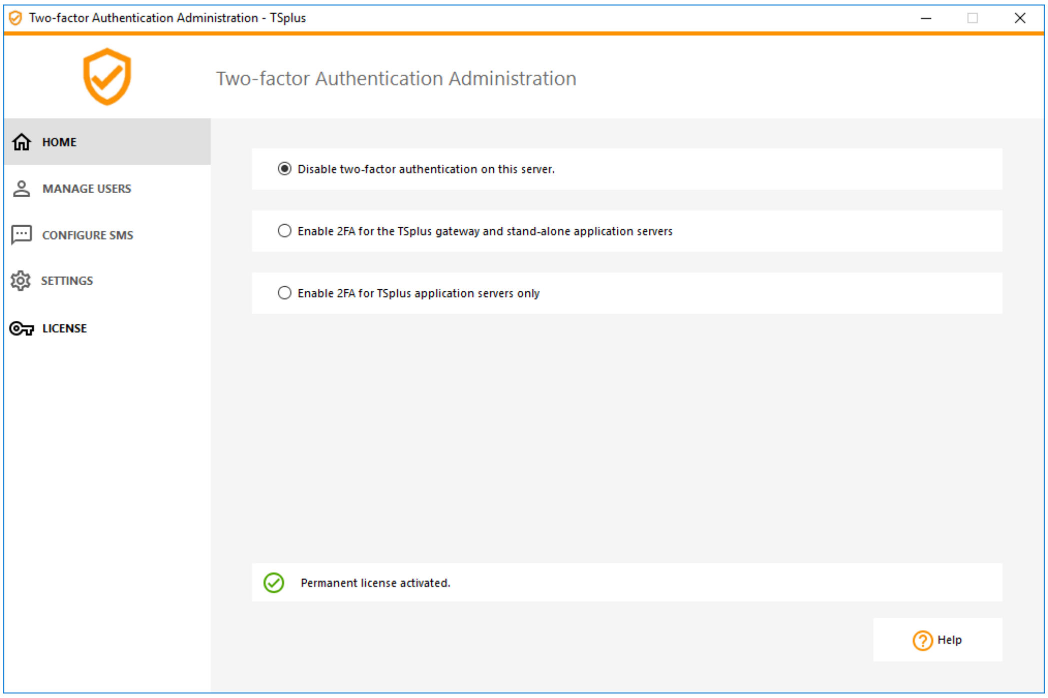
Authentication Server URL: terminalserviceplus.ddns.net

Enter the URL of the logon Web page without the page name (e.g. https://app.mycompany.com), a network name or an IP address.

● Enable 2FA for TSplus application servers only

Permanent license activated.

Or disable it:


Two-factor Authentication Administration - TSplus
Two-factor Authentication Administration
HOME
MANAGE USERS
CONFIGURE SMS
SETTINGS
LICENSE
Help

● Disable two-factor authentication on this server.

○ Enable 2FA for the TSplus gateway and stand-alone application servers

○ Enable 2FA for TSplus application servers only

Permanent license activated.

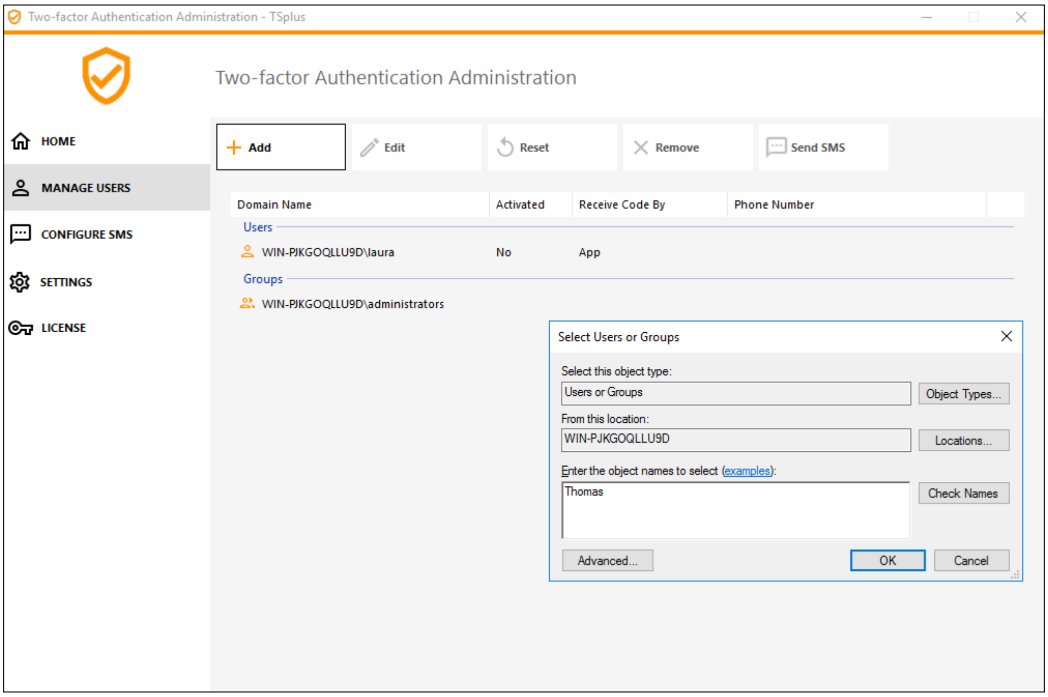
Add Users and Groups

Once two-factor authentication is enabled, you can configure users for two-factor authentication.

1) From the two-factor authentication administration application, click on the *Manage Users* tab.

MANAGE USERS

2) Then, click on *Add* to select users and/or groups of users. The *Select Users or Groups* box opens.



Domain Name	Activated	Receive Code By	Phone Number
Users			
WIN-PJKGOQLLU9D\laura	No	App	
Groups			
WIN-PJKGOQLLU9D\administrators			

Select Users or Groups

Select this object type:
Users or Groups

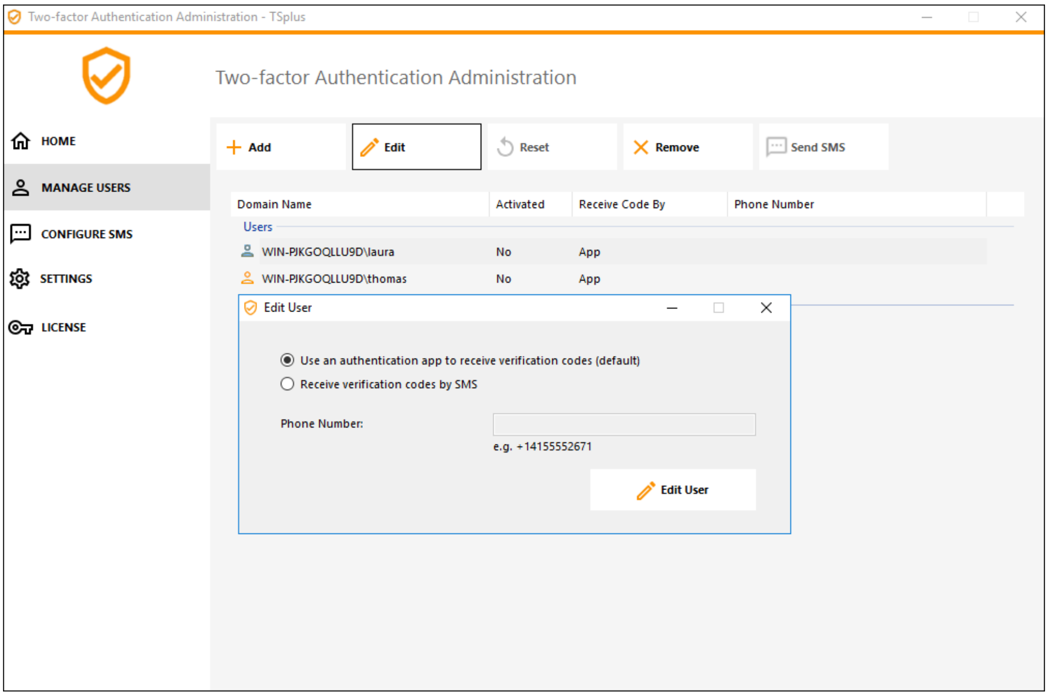
From this location:
WIN-PJKGOQLLU9D

Enter the object names to select (examples):
Thomas

3) Add as many users and groups as required and then click *OK*. The users and groups are added to the list and enabled for two-factor authentication.

Edit Users

On the same tile, you can edit the way users receive verification codes by selecting a user and clicking on the "Edit" button:



Two-factor Authentication Administration - TSplus

Two-factor Authentication Administration

Domain Name	Activated	Receive Code By	Phone Number
Users			
WIN-PJKGOQLLU9D\laura	No	App	
WIN-PJKGOQLLU9D\thomas	No	App	

Edit User

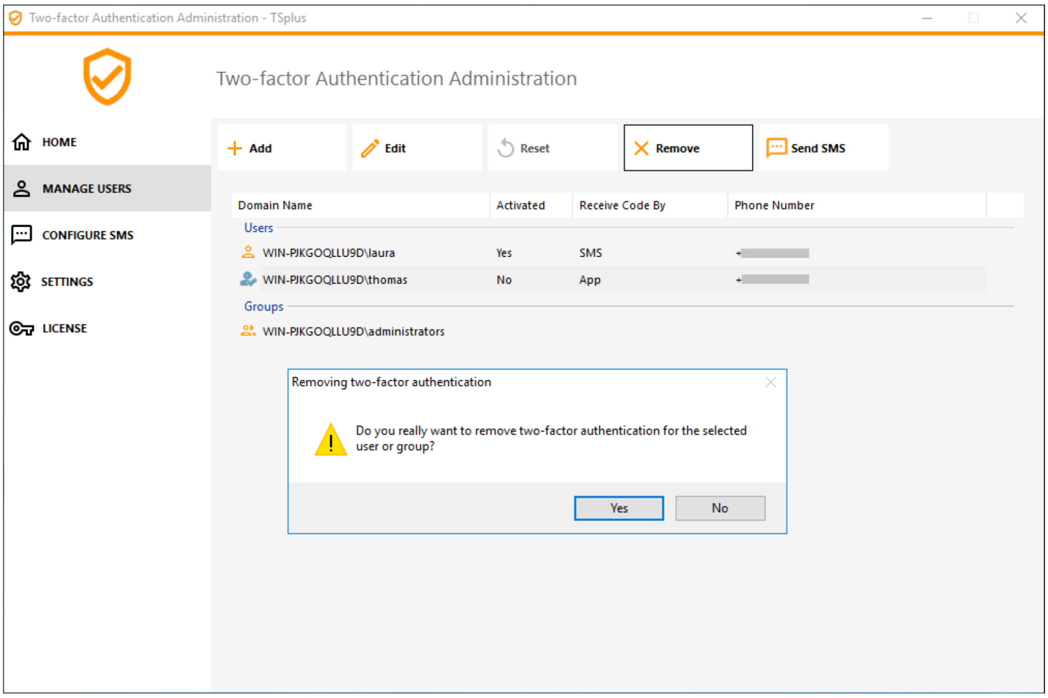
● Use an authentication app to receive verification codes (default)
○ Receive verification codes by SMS

Phone Number:
e.g. +14155552671

The user receives verification codes on the authentication app by default. You can choose that he/she receives it by SMS by selecting the option and adding the user's phone number on the field below.

Remove Users and Groups

In order to remove users or groups, select the user or the group and then click on *Remove*. A confirmation message is displayed.



Two-factor Authentication Administration - TSplus

Two-factor Authentication Administration

Domain Name	Activated	Receive Code By	Phone Number
Users			
WIN-PJKGOQLLU9D\laura	Yes	SMS	+[redacted]
WIN-PJKGOQLLU9D\thomas	No	App	+[redacted]
Groups			
WIN-PJKGOQLLU9D\administrators			

Removing two-factor authentication

Do you really want to remove two-factor authentication for the selected user or group?

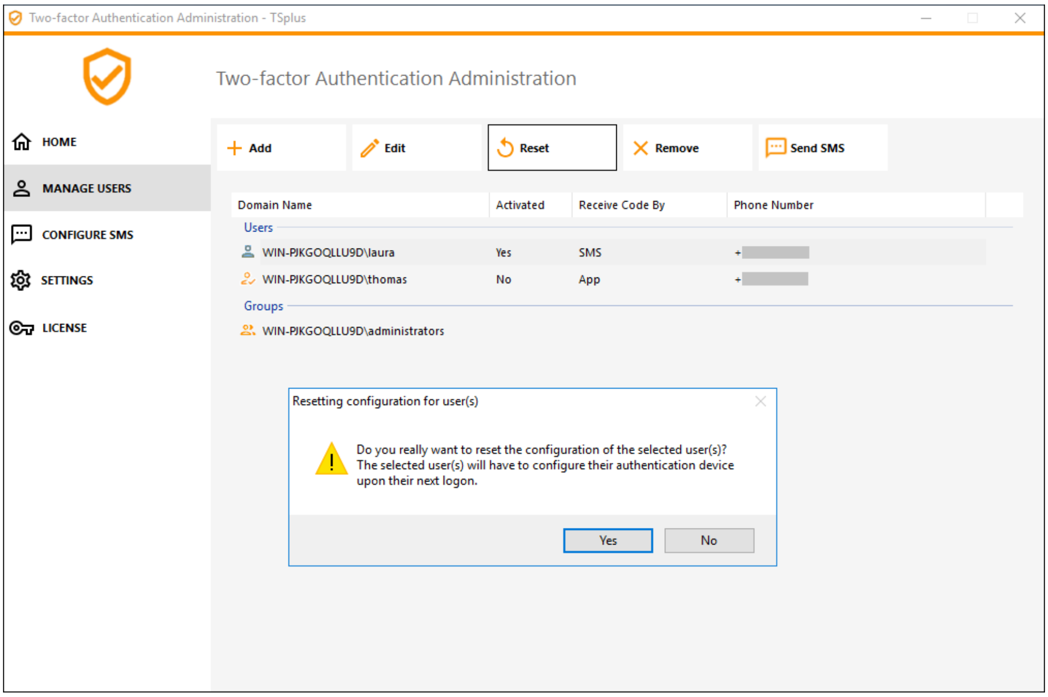
Click *Yes*. The user or the group is removed from its list and won't connect using two-factor authentication anymore.

Reset Configuration for Users

In the event of the loss of the authenticating device for a user, or if the user needs to display the secret QR code again, you must reset the user authentication settings.

1) From the two-factor authentication administration application, click on the *Manage Users* tab.

2) Select one or multiple activated users and then click on *Reset*. A confirmation message is displayed:


Two-factor Authentication Administration - TSplus
Two-factor Authentication Administration
HOME
MANAGE USERS
CONFIGURE SMS
SETTINGS
LICENSE
Add
Edit
Reset
Remove
Send SMS
Yes
No

Domain Name	Activated	Receive Code By	Phone Number
Users			
WIN-PJKGOQLLU9D\laura	Yes	SMS	+[redacted]
WIN-PJKGOQLLU9D\thomas	No	App	+[redacted]
Groups			
WIN-PJKGOQLLU9D\administrators			

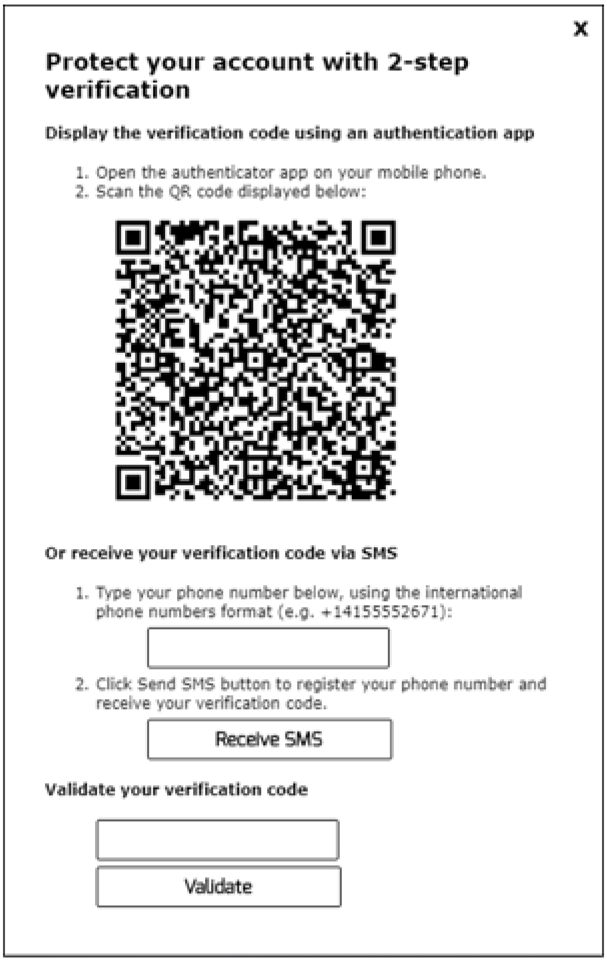
Resetting configuration for user(s)

Do you really want to reset the configuration of the selected user(s)?
The selected user(s) will have to configure their authentication device upon their next logon.

3) Click *Yes*. The selected users will be presented a new QR code at the next login and will have to scan it in their device's authentication app.
You can also modifiy the user's phone number, so that he can receive a verification code on his new device.

Enroll User for Two-factor Authentication

Once a user has been enabled for using two-factor authentication, an activation message will be displayed at his next successful logon from the TSplus Web portal.



x

Protect your account with 2-step verification

Display the verification code using an authentication app

1. Open the authenticator app on your mobile phone.
2. Scan the QR code displayed below:

Or receive your verification code via SMS

1. Type your phone number below, using the international phone numbers format (e.g. +14155552671):
2. Click Send SMS button to register your phone number and receive your verification code.

Validate your verification code

In order to complete the required steps, you have two choices: either generate codes via an authenticator app, either make the user receive codes by SMS.

Receive codes with an Authenticator Application

The user must install an authenticator app on a portable device, such as his smartphone.

You can use one of the following authenticator apps to proceed. These apps are available across a wide range of platforms:
- Authy
- Google Authenticator
- Microsoft Authenticator

Please use each app documentation for more details on how to proceed to add your TSplus account.

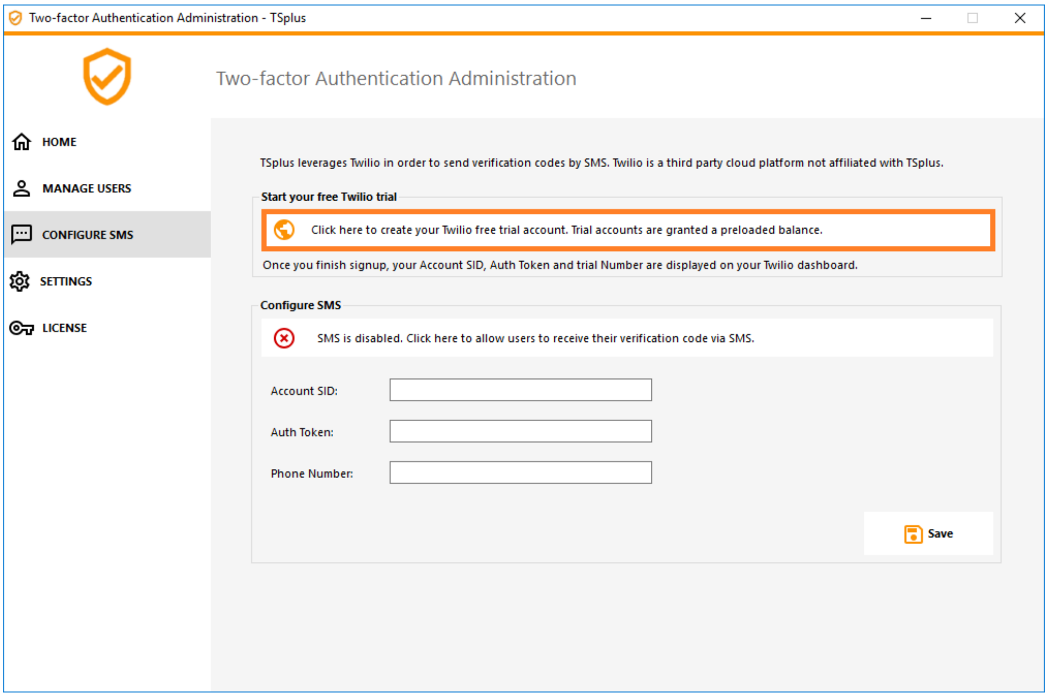
Configure SMS

In order for the user to receive verification codes by SMS, you must first enable it. Click on the *Configure SMS* tab:

Configure SMS Image not found or type unknown

TSplus leverages Twilio in order to send verification codes by SMS. Twilio is a third-party cloud platform, not affiliated with TSplus.

1) Just create a free account on Twilio by clicking on the button below "Start your free trial with Twilio":



Two-factor Authentication Administration

TSplus leverages Twilio in order to send verification codes by SMS. Twilio is a third party cloud platform not affiliated with TSplus.

Start your free Twilio trial

Click here to create your Twilio free trial account. Trial accounts are granted a preloaded balance.

Once you finish signup, your Account SID, Auth Token and trial Number are displayed on your Twilio dashboard.

Configure SMS

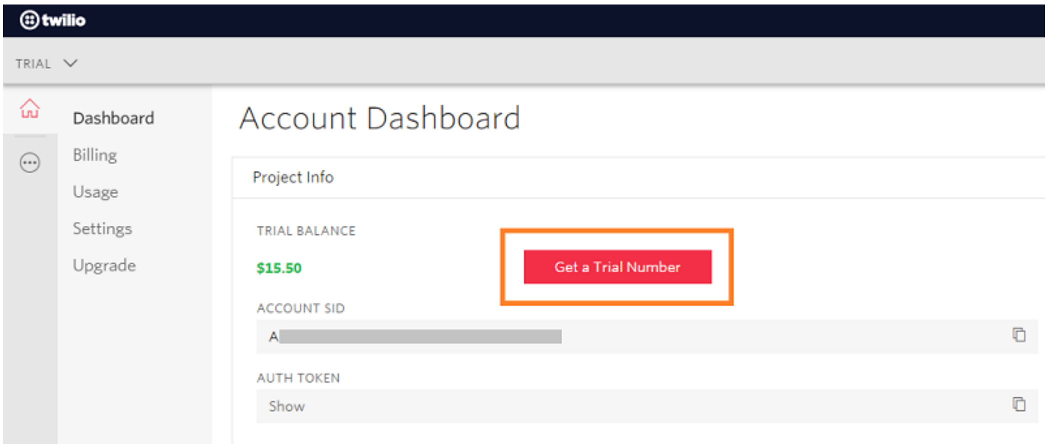
SMS is disabled. Click here to allow users to receive their verification code via SMS.

Account SID:

Auth Token:

Phone Number:

2) On your Twilio account dashboard, you will need to activate your Trial Number:



Account Dashboard

Project Info

TRIAL BALANCE

$15.50

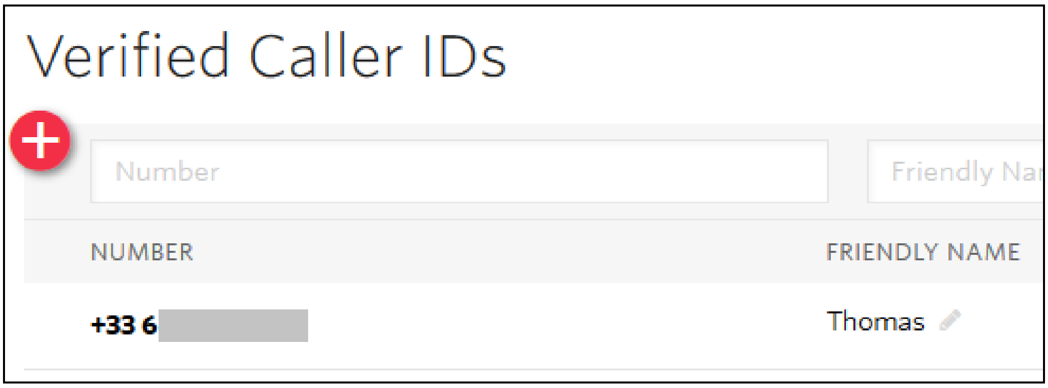
ACCOUNT SID

A[redacted]

AUTH TOKEN

Show

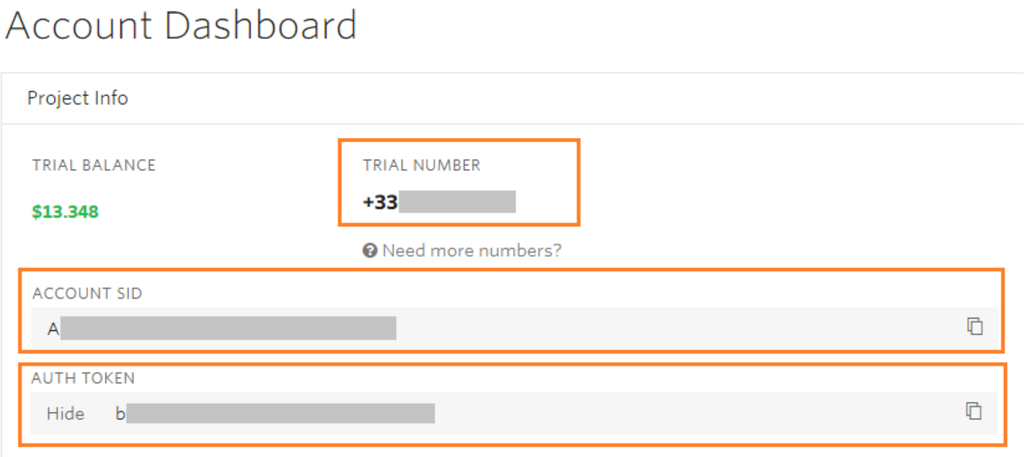
3) The next step is only necessary for Trial versions. It allows Twilio to verify the actual phone number on which SMS will be sent.
Enter this number under the "Phone Numbers" menu - "Verified Caller IDs" tab :



Verified Caller IDs

NUMBER	FRIENDLY NAME
+33 6[redacted]	Thomas

4) You will then be able to enter your account SID, Authentication Token and **Trial Number** as the Phone Number on the *Configure SMS* tab of TSplus:



Account Dashboard

Project Info

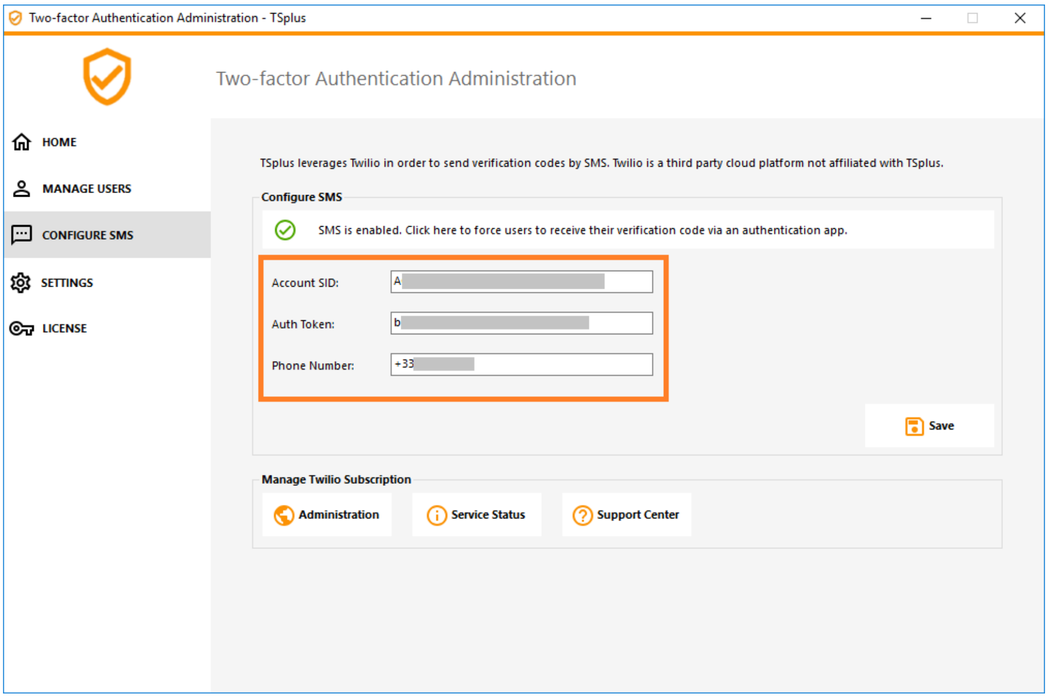
TRIAL BALANCE
$13.348

TRIAL NUMBER
+33[redacted]

Need more numbers?

ACCOUNT SID
A[redacted]

AUTH TOKEN
Hide b[redacted]



Two-factor Authentication Administration - TSplus

Two-factor Authentication Administration

TSplus leverages Twilio in order to send verification codes by SMS. Twilio is a third party cloud platform not affiliated with TSplus.

Configure SMS

SMS is enabled. Click here to force users to receive their verification code via an authentication app.

Account SID: A[redacted]

Auth Token: b[redacted]

Phone Number: +33[redacted]

Manage Twilio Subscription

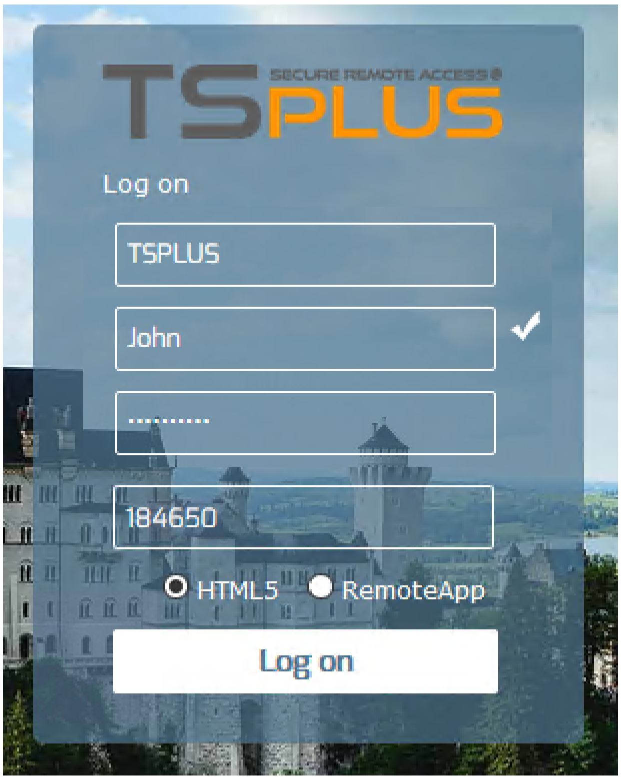
Then, click on Save. The following message will be displayed:

Image not found or type unknown
Configure SMS

You can manage your Twilio subscription on the *Manage Twilio subscription* section, at the bottom of the *Configure SMS* tab. Administrate your account, see the Service Status or reach Twilio Support Center just by clicking on the corresponding buttons.

Login using Two-factor Authentication

Once a user has configured his TSplus account in his authenticator app, he or she will be able to connect using its password and the code provided by its authenticator app or by SMS.



TSPLUS

John ✓

....

184650

Time Synchronization

TSplus server and Devices must be on time. This means that the time and date of the server must be synchronized with a time server. Devices must also have time synchronization, regardless of the time zone on which they are configured.

If an authentication request comes from a Device whose date and time are not synchronized, or if the server's date and time are not synchronized, this request may be rejected.

The validation of information between the Device and the server relates to UTC time.
In the **Settings** section, the Discrepency parameter is used to manage the period of validity of the code, in intervals of 30 seconds.

Example of validation or valid authentication:

- the server is synchronized with a time server, the time zone is UTC + 2, it is 2:30 pm
- the Device is synchronized with a time server, the time zone is UTC + 1, it is 1:30 pm
- the Discrepency parameter is configured at 60, i.e. a code validity period of 30 minutes
- referred to UTC time, the Device time and the server time are identical.

Example of validation or invalid authentication:

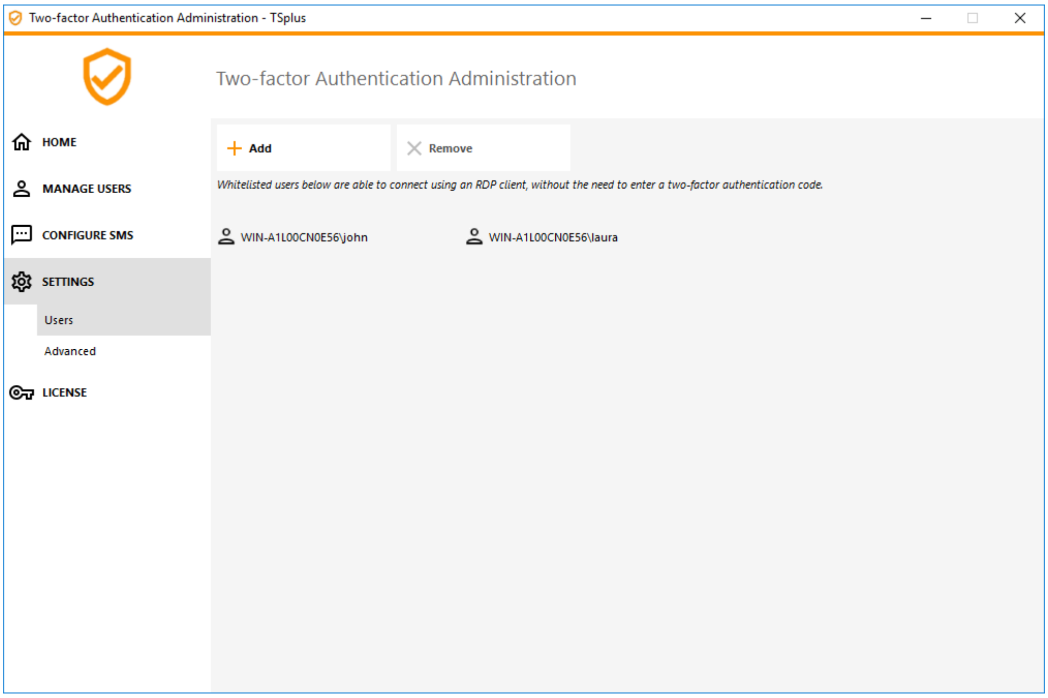
- the server is synchronized with a time server, the time zone is UTC + 2, it is 2:30 pm
- the Device is not synchronized with a time server, the time zone is UTC-1, the time is manually set to 1:30 pm
- the Discrepency parameter is configured at 60, i.e. a code validity period of 30 minutes
- the server time referred to UTC time is 12:30 am
- the time communicated by the Device, referred to UTC time is 2:30 pm
- the difference is 120 minutes, the validation code is therefore refused.

Settings

SETTINGS

The Settings tab allows you to **whitelist users, in order for them to connect using an RDP client, without the need to enter a two-authentication code.**

Click on the "Add" button to add a user and remove a user by selecting it and clicking on the "Remove" button.

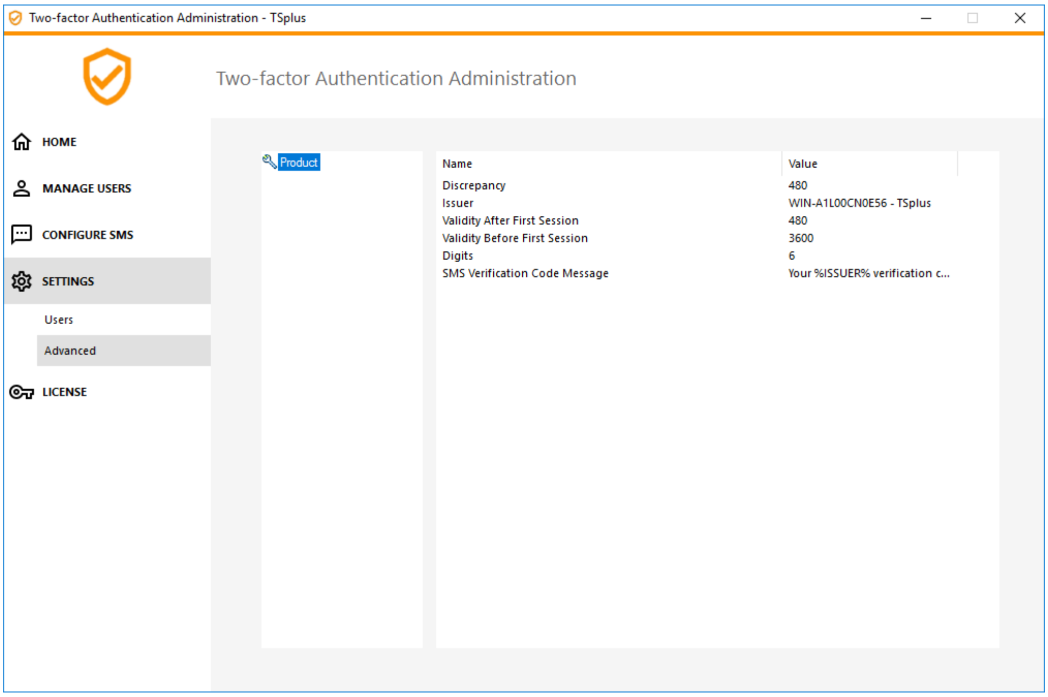

Two-factor Authentication Administration - TSplus
Two-factor Authentication Administration
HOME
MANAGE USERS
CONFIGURE SMS
SETTINGS
Users
Advanced
LICENSE
+ Add
Remove

Whitelisted users below are able to connect using an RDP client, without the need to enter a two-factor authentication code.

WIN-A1L00CN0E56\john

WIN-A1L00CN0E56\laura

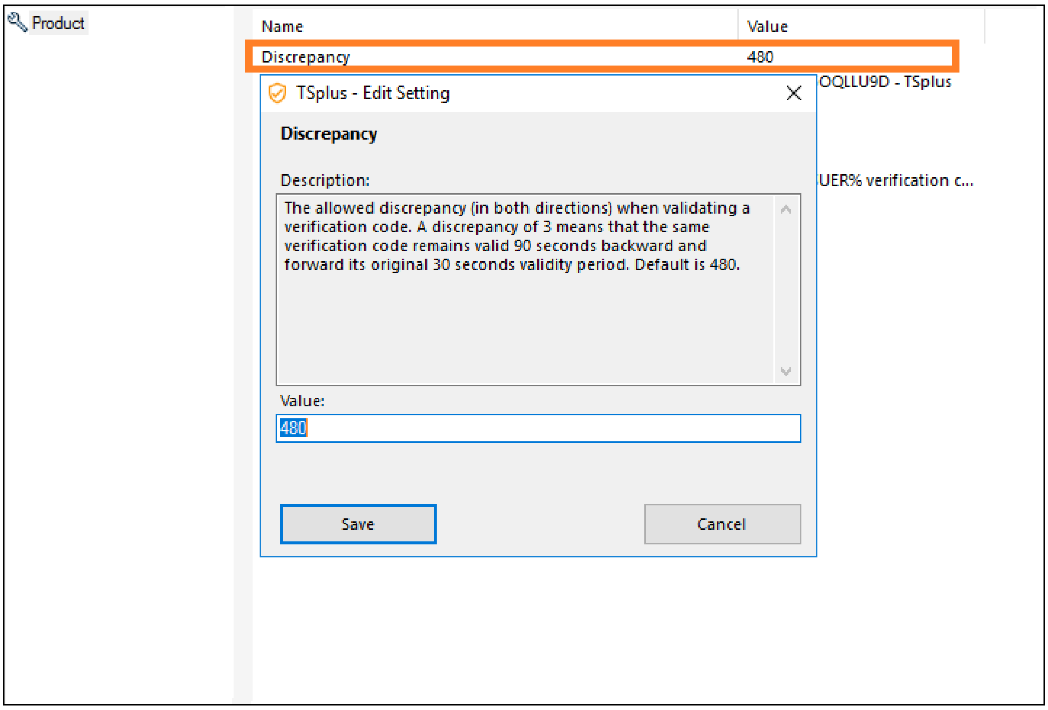
The Advanced tab allows you to configure Two-Factor Authentication in-depth settings.


Two-factor Authentication Administration - TSplus
Two-factor Authentication Administration
HOME
MANAGE USERS
CONFIGURE SMS
SETTINGS
Users
Advanced
LICENSE
Product

Name	Value
Discrepancy	480
Issuer	WIN-A1L00CN0E56 - TSplus
Validity After First Session	480
Validity Before First Session	3600
Digits	6
SMS Verification Code Message	Your %ISSUER% verification c...

Discrepancy

You can modify the Discrepancy value, which allows you to set the validation time of a verification code.
A discrepancy of 3 means that the same verification code remains valid 90 seconds backward and forward its original 30 seconds validity period. Default is 480, which means 480 x 30 seconds= 4 hours.



Name	Value
Discrepancy	480
	OQLLU9D - TSplus
	UER% verification c...

Discrepancy

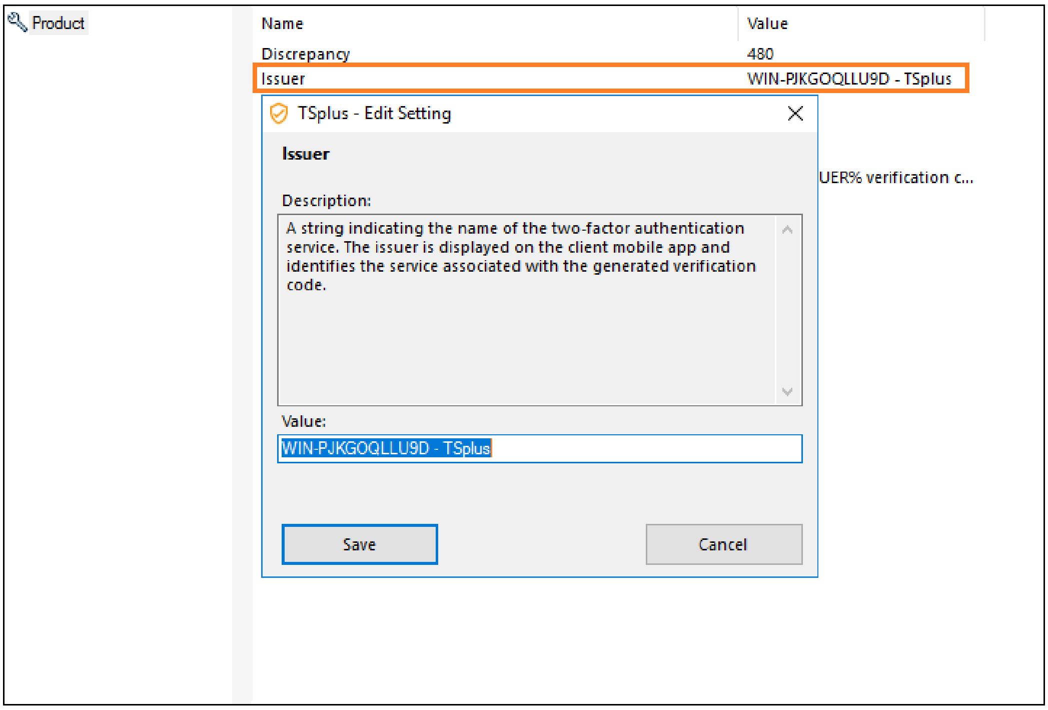
Description:

The allowed discrepancy (in both directions) when validating a verification code. A discrepancy of 3 means that the same verification code remains valid 90 seconds backward and forward its original 30 seconds validity period. Default is 480.

Value: 480

Issuer

A string indicating the name of the two-factor authentication service. The issuer is displayed on the client mobile app and identifies the service associated with the generated verification code. By default, it is composed of the server's name with TSplus.



Name	Value
Discrepancy	480
Issuer	WIN-PJKGOQLLU9D - TSplus

Issuer

Description:

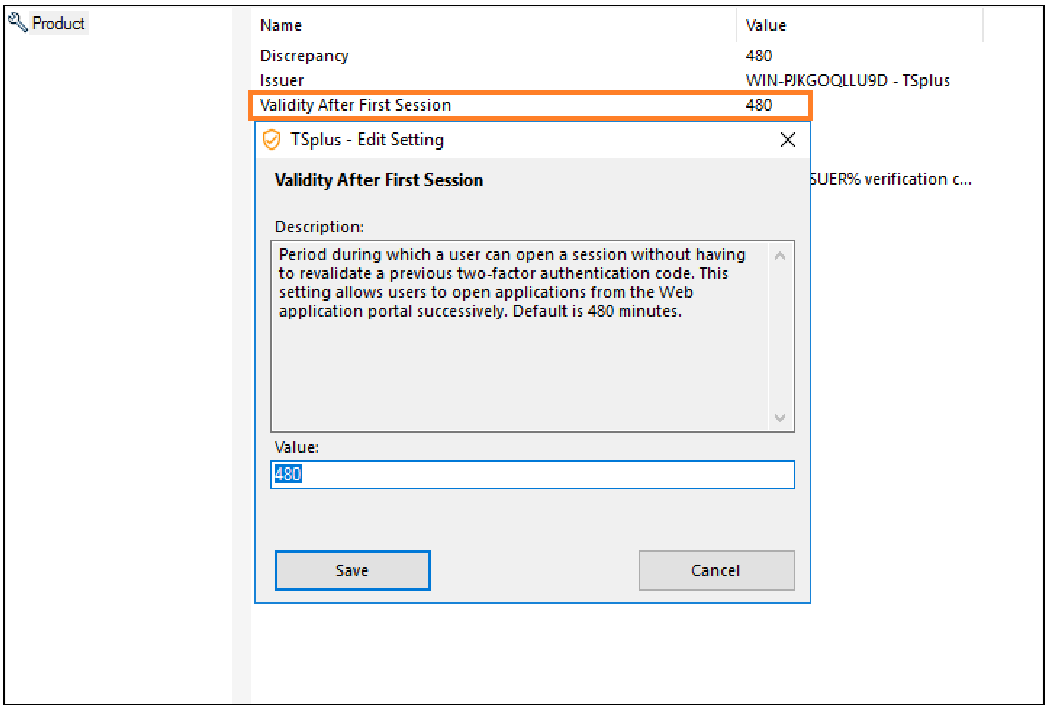
A string indicating the name of the two-factor authentication service. The issuer is displayed on the client mobile app and identifies the service associated with the generated verification code.

Value:

WIN-PJKGOQLLU9D - TSplus

Validity After First Session

Period during which a user can open a session without having to revalidate a previous two-factor authentication code. This setting allows users to open applications from the Web application portal successively. Default is 480 minutes.



Name	Value
Discrepancy	480
Issuer	WIN-PJKGOQLLU9D - TSplus
Validity After First Session	480

Validity After First Session

Description:

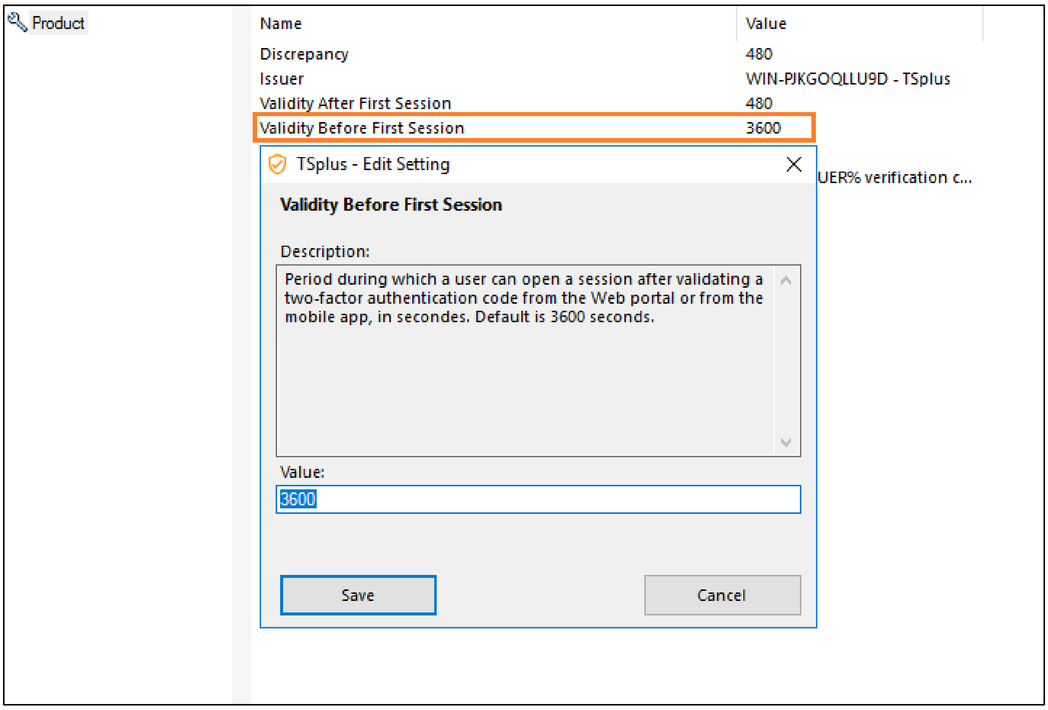
Period during which a user can open a session without having to revalidate a previous two-factor authentication code. This setting allows users to open applications from the Web application portal successively. Default is 480 minutes.

Value:

480

Validity Before First Session

Period during which a user can open a session after validating a two-factor authentication code from the Web portal or from the mobile app, in secondes. Default is 3600 seconds.



Name	Value
Discrepancy	480
Issuer	WIN-PJKGOQLLU9D - TSplus
Validity After First Session	480
Validity Before First Session	3600
	UER% verification c...

TSplus - Edit Setting

Validity Before First Session

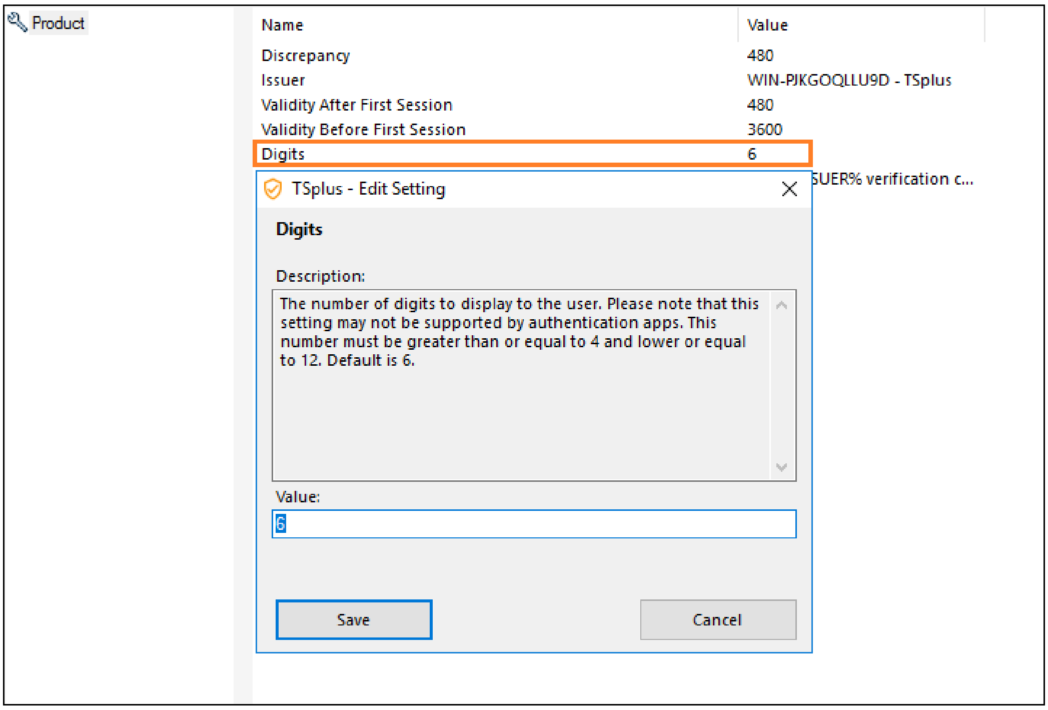
Description:

Period during which a user can open a session after validating a two-factor authentication code from the Web portal or from the mobile app, in secondes. Default is 3600 seconds.

Value: 3600

Digits

The number of digits to display to the user. Please note that this setting may not be supported by authentication apps. This number must be greater than or equal to 4 and lower or equal to 12. Default is 6.



Name	Value
Discrepancy	480
Issuer	WIN-PJKGOQLLU9D - TSplus
Validity After First Session	480
Validity Before First Session	3600
Digits	6
	SUER% verification c...

TSplus - Edit Setting

Digits

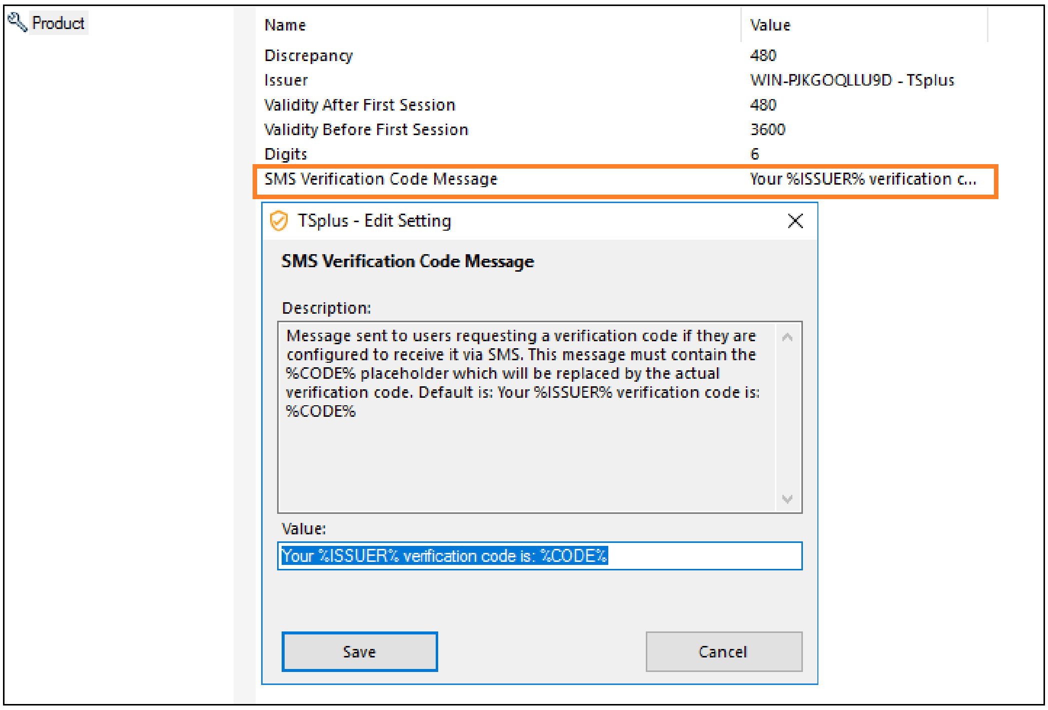
Description:

The number of digits to display to the user. Please note that this setting may not be supported by authentication apps. This number must be greater than or equal to 4 and lower or equal to 12. Default is 6.

Value: 6

SMS Verification Code Message

Message sent to users requesting a verification code if they are configured to receive it via SMS. This message must contain the %CODE% placeholder which will be replaced by the actual verification code. Default is: Your %ISSUER% verification code is: %CODE%



Name	Value
Discrepancy	480
Issuer	WIN-PJKGOQLLU9D - TSplus
Validity After First Session	480
Validity Before First Session	3600
Digits	6
SMS Verification Code Message	Your %ISSUER% verification c...

TSplus - Edit Setting

SMS Verification Code Message

Description:

Message sent to users requesting a verification code if they are configured to receive it via SMS. This message must contain the %CODE% placeholder which will be replaced by the actual verification code. Default is: Your %ISSUER% verification code is: %CODE%

Value:

Your %ISSUER% verification code is: %CODE%