Two-factor Authentication

Table of contents

- <u>Overview</u>
- <u>Requirements</u>
- <u>Activate your license</u>
- Enable two-factor authentication
- Add users and groups
- Edit users
- <u>Remove users and groups</u>
- Reset configuration for users
- Enroll User for two-factor authentication
- Receive codes with an authenticator app
- Configure SMS to receive authentication codes
- Login using two-factor authentication
- Time synchronization
- Settings

Overview

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.

The 2FA codes generated are TOTP (time-based one time password), and therefore are for single use.

Therefore, it is not possible to reuse a 2FA code that has already been used. This prevents the theft and then the use of a 2FA code by observing the user while he enters his code.

Requirements

Two-factor authentication requires TSplus Remote Access Mobile Web or Enterprise Editions.

Two-factor authentication is supported by:

- TSplus Remote Access Web portal, for both HTML5 and Remoteapp connections
- TSplus Connection Client, for clients generated since version 15.30.3.15, with 2FA support explicitly enabled. See Portable Client Generator Support for Two-factor Authentication
- 2FA is related to Windows Users and not Web credentials

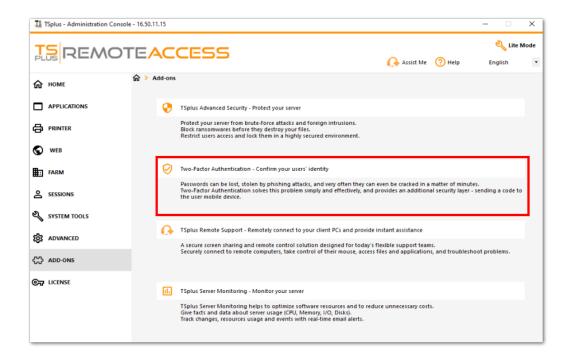
This authentication mode does not support login through standard Microsoft Remote Desktop client (mstsc.exe).

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 <u>Time Synchronization</u> and <u>Settings</u> sections for more configuration information.

Activating Two-factor Authentication Add-On License

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



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 Adm	inistration - 16.50.11.15	-		×
$\overline{\mathbf{O}}$	Two-factor Authentication Administration			
М НОМЕ	O Disable two-factor authentication on this server.			
A MANAGE USERS				
CONFIGURE SMS	Enable 2FA for the TSplus gateway and stand-alone application servers.			
CONFIGURE E-MAIL	Enable 2FA for TSplus application servers only			
S MANAGE 2FA REQUESTS				
ស្ត្រី settings				
ତ୍ମ LICENSE				
	Permanent license activated.			
	Control of Support date: 2026-11-21			
		🥐 Helj	0	

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:

Image: Service of the ser	Two-factor Authentication	in Administration - 16.50.11.15	
Authentication Server URL: iedd/ma.net Save Authentication Server URL: iedd/ma.net Authentication Server Server URL: iedd/ma.net Authentication Server Ser			×
MANAGE USER CONFIGURE SM CONFIGURE SM CONFIGURE E-MAIL MANAGE 2FA REQUESTS SETTINGS TUCENSE Permanent license activated.) номе	Authentication Server (19): Unalidou not	
CONFIGURE E-MAIL CONFIGURE E-MAIL MANAGE ZFA REQUESTS SETTINGS LICENSE Permanent license activated.	MANAGE USER	Autricituduon servei onci iteagunisme	
Enable 2FA for TSplus application servers only MANAGE 2FA REQUESTS SETTINGS LICENSE O Permanent license activated.	CONFIGURE SM	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.	
SETTINGS	CONFIGURE E-MAIL	Enable 2FA for TSplus application servers only	
→ LICENSE	MANAGE 2FA REQUESTS	5	
Permanent license activated.	SETTINGS		
		Bermannet licence activited	
C End of support date: 2026-11-21		Permanenti licertse activated.	
		End of support date: 2026-11-21	
⊘ Неір		0	Help

Or disable it:

0	Two-factor Authentication Admi	nistration - 16.50.11.15	-		×
	$\overline{\mathbf{O}}$	Two-factor Authentication Administration			
ŵ	номе				
8	MANAGE USERS	Disable two-factor authentication on this server.			
	CONFIGURE SMS	O Enable 2FA for the TSplus gateway and stand-alone application servers.			
	CONFIGURE E-MAIL	Enable 2FA for TSplus application servers only			
5	MANAGE 2FA REQUESTS				
鐐	SETTINGS				
©7	LICENSE				
		Permanent license activated.			
		C End of support date: 2026-11-21			
			<u>(</u>) не	lp	

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.

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

0	wo-factor Authentication Admin	nistration - 16.50.11.	15				– 🗆 X
	\oslash	Two-factor A	Authentication Ad	ministratio	n		
ŵ	HOME	+ Add User	+ Add Group	/ Edit	🖑 Reset	× Remove	
ది	MANAGE USERS	Domain Name		Activated	Receive Code By	Phone Number	Email
Ē	CONFIGURE SMS						
	CONFIGURE E-MAIL		♣ Configure 2FA for a use	21	- 0	×	
5	MANAGE 2FA REQUESTS		Find in local user				
鐐	SETTINGS			Sélectionnez un t	-		×
©7	LICENSE		Username	Sélectionnez le typ			
			Enter a username (for exam	un utilisateur			Types d'objets
				A partir de cet emp			
				DESKTOP-VHE8	C1I		Emplacements
					objet à sélectionner (exemp	<u>es)</u> :	
				DESKTOP-VHE8	L II'test		Vérifier les noms
				Avancé]		OK Annuler
		¢					>

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 Adm	inistration - 16.50.11.15	– 🗆 X				
\bigcirc	Two-factor Authentication Administration					
М НОМЕ	+ Add User + Add Group 🧪 Edit 🖄 Reset 🗙 Remove					
	Domain Name Activated Receive Code By Phone Number	Email				
CONFIGURE SMS	Users Construction Description Descripti Description Description Description Description					
CONFIGURE E-MAIL						
3 MANAGE 2FA REQUESTS	Edit User - X How to receive confirmation code ? User defined					
SETTINGS	How to receive confirmation code ? User defined Phone Number: Authentication app SMS					
	Isma Email					
	E-mail					
	/ tort user					
	¢	>				

The user receives verification codes on the authentication app by default. You can choose that he/she receives it by SMS or EMAIL by selecting the option.

Selected SMS and added the user's phone number in the field or selected EMAIL and added the user's email.

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.

0	Two-factor Authentication Adn	ninistration - 16.50.11.15					- 🗆 X
	$\overline{\mathbf{O}}$	Two-factor Aut	Two-factor Authentication Administration				
ŵ	НОМЕ	+ Add User	+ Add Group	🧪 Edit	5 Reset	× Remove	
ది	MANAGE USERS	Domain Name		Activated	Receive Code By	Phone Number	Email
Ē	CONFIGURE SMS	Users A DESKTOP-VHE8	C1I\test	No	User defined		56.0000
	CONFIGURE E-MAIL						
5	MANAGE 2FA REQUESTS		Removing t	wo-factor auther	ntication	×	
鐐	SETTINGS						
©-	LICENSE		<u> </u>	o you really want ie selected user o	to remove two-factor auti r group?	nentication for	
					Oui	Non	
		<					>

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 Ad	ministration - 16.50.11.15	i				- 0
$\overline{\mathbf{O}}$	Two-factor A	uthentication A	dministratio	on		
НОМЕ	+ Add User	+ Add Group	🥖 Edit	S Reset	× Remove	
MANAGE USERS	Domain Name		Activated	Receive Code By	Phone Number	Email
CONFIGURE SMS	Users DESKTOP-VH	E8C1I\test	Yes	E-mail		test@test.fr
CONFIGURE E-MAIL						
MANAGE 2FA REQUESTS		Resetting	configuration for u	user(s)	×	
SETTINGS			Do you really want	to reset the configuration ed user(s) will have to conf	n of the selected	
LICENSE			authentication de	vice upon their next logon		
				Oui	Non	
	<					

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 modifive 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.

Clic	to configure your authentication app
	pen the authenticator app on your mobile phone. can the QR code displayed below:
	Secret key: IMPCKUPCDGJWZOHISPHS32S456W4ERIA
alidat	e your verification code obtained by SMS, e-mail or via your 2FA app
	Validate

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:

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 Action	Iministration - TSplus — 🗌 🗙
\bigotimes	Two-factor Authentication Administration
슈 HOME 온 MANAGE USERS	TSplus leverages Twilio in order to send verification codes by SMS. Twilio is a third party cloud platform not affiliated with TSplus.
CONFIGURE SMS	Click here to create your Twilio free trial account. Trial accounts are granted a preloaded balance.
袋 settings ©귟 license	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:
	Save

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

(i) tw	vilio		
TRIAL	~		
5	Dashboard Billing Usage Settings Upgrade	Account Dashboard Project Info TRIAL BALANCE \$15.50 Get a Trial Number	
		ACCOUNT SID A AUTH TOKEN Show	0 0

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 <u>"Phone Numbers" menu - "Verified Caller IDs"</u> tab :

Verified Caller IDs	
Number	Friendly Na
NUMBER	FRIENDLY NAME
+33 6	Thomas 🥒

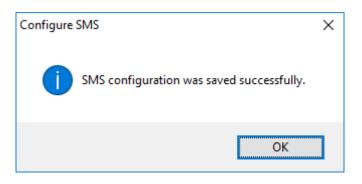
4) You will then be able to enter your account SID, Authentication Token and **Trial Number** as the Phone Number on the *Configure SMS* tab of TSplus:

Account Dashboard

Project Info		
TRIAL BALANCE \$13.348	TRIAL NUMBER	
	• Need more numbers?	
ACCOUNT SID		Ū
AUTH TOKEN Hide b		ū

🤣 Two-factor Authentication Admi	inistration - TSplus —	×
$\overline{\mathbf{O}}$	Two-factor Authentication Administration	
ゆ home 名 manage users	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.	
説 settings ©テテ license	Account SID: A Auth Token: b Phone Number: +33	
	Manage Twilio Subscription Administration Service Status O Support Center	

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



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.

Configure EMAIL

For the user to receive verification codes by EMAIL, you must first configure your SMTP email.

Stwo-factor Authentication Adm	inistration - 16.50.11.7	_	- 🗆	×
\bigcirc	Two-factor Authentication Ad	ministration		
М НОМЕ	Email settings			
	SMTP configurationallows TSplus to send co	onfirmation codes by email, for enabling 2FA		
	SMTP Hostname	smtp.		
	SMTP Port	465		
S MANAGE 2FA REQUESTS	Use SSL			
SETTINGS	SMTP Username	apikey		
ලි LICENSE	SMTP Password			
	Send Email From	admin©		
		Save		
	Send test Email To	test@"		
		Test		

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, by SMS or Email.

From the TSplus Remote Access Web portal:

B		
Protect your a	ccount with 2-step verification	
Validate your verifica	tion code	
Validate		

From the TSplus generated client:

2FA authentication		×
Please enter your authentication c	ode.	
F 1		7
ОК	Cancel	

Time Synchronization

TSplus application servers and client devices must share the same time. This means that the time and date of the server must be synchronized with a time server. Client 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

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.

01	wo-factor Authentication Admi	inistration - 16.50.11.15 —	×
	\oslash	Two-factor Authentication Administration	
ŵ	HOME	+ Add × Remove	
گ	MANAGE USERS	Whitelisted users below are able to connect using an RDP client, without the need to enter a two-factor authentication code.	
Ē	CONFIGURE SMS	C DESKTOP-VHE8C11/test	
	CONFIGURE E-MAIL		
5	MANAGE 2FA REQUESTS		
鐐	SETTINGS		
	Users		
	Advanced		
©7	LICENSE		

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

0	Two-factor Authentication Adm	inistration - 16.50.11.15		- 0	×
	$\overline{\mathbf{O}}$	Two-factor Authenticati	on Administration		
命	НОМЕ	역 _N Product	Name	Value	
8	MANAGE USERS	tigi Security	Discrepancy Issuer	480 DESKTOP-VHE8C1I - TSplus	
Ē	CONFIGURE SMS		Validity After First Session Validity Before First Session Digits	480 3600 6	
	CONFIGURE E-MAIL		SMS Verification Code Message Display Domain in the application	Your %ISSUER% verification c yes	
5	MANAGE 2FA REQUESTS		Allow HTML5 for not configured users	yes	
鐐	SETTINGS				
	Users				
	Advanced				
ଙ୍କ	LICENSE				

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.

Roduct	Name	Value	
	Discrepancy	480	
	⊘ TSplus - Edit Setting	×	OQLLU9D - TSplus
	Discrepancy		
	Description:		UER% verification c
	The allowed discrepancy (in both directions) when validating 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:		
	Save Cano	el	
			1

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.

Noduct	Name	Value		
	Discrepancy	480		
	Issuer	WIN-PJK	GOQLLU9D - TSplus	
	🤣 TSplus - Edit Setting	×		
	Issuer		UER% verification c	
	Description:		UER% Verification c	
	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 verificat code.			
	Value: WIN-PJKGOQLLU9D - TSplus			
	Save Cano	el		

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.

Noduct	Name	Value	
-	Discrepancy	480	
	lssuer		GOQLLU9D - TSplus
	Validity After First Session	480	
	Splus - Edit Setting	×	
	Validity After First Session		SUER% verification c
	Description:		
	Period during which a user can open a session witho to revalidate a previous two-factor authentication co setting allows users to open applications from the W application portal successively. Default is 480 minutes	de. This /eb	
	Value:	~	
	480		
	400		
	Save	Cancel	

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.

Noduct	Name	Value
	Discrepancy	480
	Issuer	WIN-PJKGOQLLU9D - TSplus
	Validity After First Session	480
	Validity Before First Session	3600
	🤣 TSplus - Edit Setting	× UER% verification c
	Validity Before First Session	
	Description:	
	Period during which a user can open a session aft two-factor authentication code from the Web port mobile app, in secondes. Default is 3600 seconds.	tal or from the
	Value:	
	3600	
	Save	Cancel

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.

Noduct	Name	Value	
	Discrepancy	480	
	lssuer		GOQLLU9D - TSplus
	Validity After First Session	480	
	Validity Before First Session	3600	
	Digits	6	
	⊘ TSplus - Edit Setting	×	5UER% verification c
	Digits		
	Description:		
	The number of digits to display to the user. Please note that setting may not be supported by authentication apps. This number must be greater than or equal to 4 and lower or equ to 12. Default is 6.		
		\sim	
	Value:		
	6		
	Save	el	
			-

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%

Noduct	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 coc configured to receive it via SMS. This message must %CODE% placeholder which will be replaced by the verification code. Default is: Your %ISSUER% verifica %CODE%	t contain the e actual
		~
	Value:	
	Your %ISSUER% verification code is: %CODE%	
	Save	Cancel