Financial Services

Security Administration Guide-SaaS

TSoftPlus™

Financial Services

File Security Administration Guide TSoftPlus-SaaS

Date Edited: August 2021

Disclaimer

The contents of this publication, including its appendices, exhibits, and other attachments, as updated or revised, are highly confidential and proprietary to Wolters Kluwer Financial Services, Inc. or its subsidiaries or affiliates (“Wolters Kluwer Financial Services”). This publication is distributed pursuant to a Non-Disclosure Agreement, Evaluation Agreement, License Agreement and/or other similar agreement(s) with Wolters Kluwer Financial Services, Inc. or its subsidiary or affiliate. Unless otherwise specifically provided in such agreement(s), the reproduction of this publication is strictly prohibited. Use and distribution of this publication are also subject to the responsibilities and obligations of such agreement(s), which require confidential treatment of this publication and its contents.

Except only for the warranties (if any) expressly set forth in the agreement(s) under which this publication is provided (i.e., your agreement or license for the described product), this publication is provided “as is”, and Wolters Kluwer Financial Services makes no warranty, express, implied, by description, by sample or otherwise, and in particular and without limitation, makes no implied warranties of merchantability or fitness for purpose. No modifications to this Warranty Disclaimer are authorized unless in writing and signed by the President or a Vice President of the Wolters Kluwer Financial Services entity licensing the product described in this publication.

This publication is intended to provide accurate and authoritative information about the subject matter covered based upon information available at the time of publication. Examples given in this publication are for illustrative purposes only.

Development of this publication and the software (including forms, disclosures, reports, and other documents generated by the software) or other products that it describes was based on Wolters Kluwer Financial Services’ understanding of various laws, regulations and commentaries. Wolters Kluwer Financial Services cannot and does not guarantee that its understanding is correct.

This publication is not intended, and should not be used, as a substitute for legal, accounting, or other professional advice. Wolters Kluwer Financial Services is not engaged in providing legal, accounting or other professional services. If legal or other professional assistance is required, you should seek the services of a competent professional. We encourage you to seek the advice of your own attorney concerning all legal issues involving the use of this publication and any products described in this publication. If your interpretations or your counsel’s interpretations are contrary to those expressed in this publication, you should of course, follow your/your counsel’s interpretations.

The following notice is required by law:

> **WOLTERS KLUWER FINANCIAL SERVICES’S PRODUCTS AND SERVICES ARE NOT A SUBSTITUTE FOR THE ADVICE OF AN ATTORNEY.**

6815 Saukview Drive
St. Cloud, MN 56303

Content

Overview

In Security Administration, you can manage accounts, users, and roles/permissions. IP filtering and client authentication are available if you have access rights to those areas.

- **Accounts**: Wolters Kluwer sets up your initial account and the products your organization has licensed. You can copy this account to set up additional accounts for different areas of your organization. Users, roles, and permissions are managed through an account.
- **Users**: The Users section provides a list of users for the account. You can add, edit, and manage users. Users can be assigned specific roles that include a specific set of permissions. Passwords can be reset and users unlocked
- **Roles**: Users are assigned roles with permissions that determine what they can do in applications. You can add roles and assign specific permissions to the roles. Available permissions are preset by Wolters Kluwer and you can select/deselect permissions as applicable for a role.
- **IP Filtering**: You must have specific permissions to access IP Filtering. This section allows you to enable IP filtering for the account. If filtering is enabled, users will have access to the IP addresses entered in the list.
- **Client Authentication**: You must have specific permissions to access Client Authentication. This section allows you to upload certificates for the account.

Accounts

The Accounts section provides information about your account and the products you have licensed. You can copy the account to set up additional accounts to manage your users and roles by separate accounts.

Copying an Existing Account

To copy an account, select the **Copy** icon next to the account. The account appears in the list with a "Copy of <Account Name>." Select the account. Change the account name and set up users and roles as applicable.

- The copied account will have the same Customer Number and licensed products as the original account
- The person copying the account will be the only user in the User list. Users can be added
- Roles and permissions of the person copying the account will default into Roles and Permissions. Roles/Permissions can be added, and existing Roles/Permissions can be deselected.

Users

Adding a User

Adding a user includes User Information, User Status, and Roles sections.

- Select +User to add a new user. After completing and saving the information, an email is sent to the user with a registration link and product URLs. To register, a user provides a name, password, and challenge questions with answers.
- The Username must be a valid email address and is used for the registration email, the confirmation email that includes product URLs, and password reset emails.
- In the Users List, Not Registered and a mail icon displays to indicate a user was set up and sent an email, but has not completed registration.

User Information

After a user has registered, name and phone number information display.

- The Reset Password link can be used to reset a user's password. Selecting the link sends an email to the user to set up a new password.

  - A user can request a password reset by clicking the Forgot Password? link on the main login screen, contacting an Account administrator, or selecting the Change Password link in the User Information section of their User Profile.
  - If a user has two failed responses to their security questions when changing their password, they will be locked out.
  - An Account Administrator does not have access to a user's password and cannot retrieve it.

Passwords requirements include the following criteria:

- Passwords must be eight characters long.
- Passwords must contain three of the four-character groups:
  - At least one uppercase character (A-Z)
  - At least one lowercase character (a-z)
  - At least one numeric character (0-9)
  - At least one special character, consisting of the following: ! " # $ % ' ( ) * + , - . /: ; = ? @ [\ ] _ ` { | } ~
- Passwords can only be changed once every 48 hours.
- Passwords must be changed every 90 days.

User Status

After a user has completed registration, **Locked** and **Password Reset Pending** options are available.

- Locked indicates a locked account. An account is locked after five failed login attempts, or two failed responses to challenge questions.
- Password Reset Pending indicates an email was sent to a user to reset their password, but the user has not completed the reset. If the user does not reset their password within seven days, they must request a new password reset.

Roles

- Wolters Kluwer provides specific roles for each licensed product. Custom roles can be also added in the Roles section. You can select/deselect roles for the user.
- Multiple accounts may have different roles depending on the roles set up for the account.

Deleting a User

- A user can be deleted from the Users List.
- If a user cannot be deleted because the user has permissions for multiple products, the Account Administrator can remove the product roles for the user.

Roles

A Role is a collection of permissions that is assigned to a user. When a user is assigned a role, the user also is assigned the permissions attached to the role. Permissions allow access to specific functions and actions in a product.

- Wolters Kluwer provides preset roles and permissions for each product.
- You can edit roles by selecting/deselecting permissions for a role. Permissions cannot be added or edited.
- You can add and delete custom roles. You can add as many permissions for a custom role as needed and you can select permissions from multiple products.

TSoftPlus Roles and Permissions

Wolters Kluwer provides four default roles for the TSoftPlus product: Manage Security Administration Account, Manage TSoftPlus, TSoftPlus Administrator, and TSoftPlus Loan Processor. After the January 2018 Deployment, the Manage Security Administration Account and Manage TSoftPlus roles will include new permissions. Please refer to the tables below for more information about the new permissions.

- The Default Roles and Default Permissions grid details what permissions are set in the default role.
- The Available Permissions for the Custom Roles grid details what permissions are available to select from when creating a new role or making edits to existing roles.

TSoftPlus "Manage Security Administration Account" Default Role and Permissions

"Manage Security Administration Account" Default Role for Accounts contained the following permissions prior to the January 2018 Deployment

Default Permission	*Permission Group*	*Description*
Clone Account	Security Administration	Allows an Account Administrator to copy an account to create additional accounts.
Manage Account	Security Administration	Allows an Account Administrator to manage account information.
Manage Account Users	Security Administration	Allows an Account Administrator to manage other users.

"Manage Security Administration Account" Default Role for Accounts will migrate to contain the following permissions after the January 2018 Deployment

Default Permission	*Permission Group*	*Description*
Add User to Account	Security Administration	Allows an Account Administrator to add users to an account. This is a new permission as of the January 2018 Deployment.
Assign or Remove Permissions for Security Administration	Security Administration	Allows an Account Administrator to assign or remove permissions in Security Administration. This is a new permission as of the January 2018 Deployment.
Basic Access for Security Administration	Security Administration	Allows a user to have basic access to Security Administration. This is a new permission as of the January 2018 Deployment.
Clone Account	Security Administration	Allows an Account Administrator to copy an account to create additional accounts.
Edit Account (Prior to the January 2018 Deployment, was Manage Account permission)	Security Administration	Allows an Account Administrator to manage account information. This was the previous Manage Account permission.
Edit Account Roles	Security Administration	Allows an Account Administrator to edit account roles in an account. This is a new permission as of the January 2018 Deployment.
Edit Account Users (Prior to the January 2018 Deployment, was Manage Account Users permission)	Security Administration	Allows an Account Administrator to edit account users in an account. This was the previous Manage Account Users permission.
Remove User from Account	Security Administration	Allows an Account Administrator to remove users in an account. This is a new permission as of the January 2018 Deployment.
Reset Account User Password	Security Administration	Allows an Account Administrator to reset an Account User password in an account. This is a new permission as of the January 2018 Deployment.
Unlock Account User	Security Administration	Allows an Account Administrator to unlock a user in an account. This is a new permission as of the January 2018 Deployment.

Default Permission	*Permission Group*	*Description*
View Account Roles	Security Administration	Allows an Account Administrator to view account roles in an account. This is a new permission as of the January 2018 Deployment.
View Account Users	Security Administration	Allows an Account Administrator to view account users in an account. This is a new permission as of the January 2018 Deployment.

TSoftPlus "Manage TSoftPlus" Default Role and Permissions

(For accounts created after you began using Security Administration)

"Manage Account Recordkeeping Services" Default Role for Accounts created after the November 2017 deployment will migrate to contain the following permissions (in **Bold)** after the January 2018 deployment.

Default Permission	*Permission Group*	*Description*
Basic Access for TSoftPlus	TSoftPlus	Allows a user to access TSoftPlus.
Manage Administration for TSoftPlus	TSoftPlus	Allows an Account Administrator to access Administration.
Assign or Remove Permissions for TSoftPlus	TSoftPlus	Allows an Account Administrator to assign or remove permissions for TSoftPlus. This permission works in combination with other Security Administration permissions (i.e. remove user from an account). It was created to prevent collisions for Accounts with more than one product. Example: An account is licensed for Product A and Product B. There are users in the Account for Product A and Product B. An Account Administrator for Product A needs to remove a user. There are users in the list for both Product A and Product B. If the Account Administrator has the Assign or Remove Permissions for Product A and Assign or Remove Permissions for Product B, the Administrator can remove a user that has permissions for Product A and/or Product B. If the Account Administrator has the Assign or Remove Permissions for Product A only, the Administrator can only remove the users that have permission for Product A, and they are not allowed to remove a user that has Product B permissions.

TSoftPlus "Manage TSoftPlus" Default Role and Permissions

(For accounts created in Administration before you began using Security Administration)

"Manage Account Recordkeeping Services" Default Role for Accounts created prior to the November 2017 deployment will migrate to contain the following permissions (in **Bold**) after the January 2018 deployment.

Default Permission	*Permission Group*	*Description*
Add User to Account	Security Administration	Allows an Account Administrator to add users to an account. This is a new permission as of the January 2018 Deployment.

Default Permission	*Permission Group*	*Description*
Assign or Remove Permissions for Security Administration	Security Administration	Allows an Account Administrator to assign or remove permissions in Security Administration. This is a new permission as of the January 2018 Deployment.
Basic Access for Security Administration	Security Administration	Allows a user to have basic access to Security Administration. This is a new permission as of the January 2018 Deployment.
Clone Account	Security Administration	Allows an Account Administrator to copy an account to create additional accounts.
Edit Account (Prior to the January 2018 Deployment, was Manage Account permission)	Security Administration	Allows an Account Administrator to manage account information. This was the previous Manage Account permission.
Edit Account Roles	Security Administration	Allows an Account Administrator to edit account roles in an account. This is a new permission as of the January 2018 Deployment.
Edit Account Users (Prior to the January 2018 Deployment, was Manage Account Users permission)	Security Administration	Allows an Account Administrator to edit account users in an account. This was the previous Manage Account Users permission.
Remove User from Account	Security Administration	Allows an Account Administrator to remove users in an account. This is a new permission as of the January 2018 Deployment.
Reset Account User Password	Security Administration	Allows an Account Administrator to reset an Account User password in an account. This is a new permission as of the January 2018 Deployment.
Unlock Account User	Security Administration	Allows an Account Administrator to unlock a user in an account. This is a new permission as of the January 2018 Deployment.
View Account Roles	Security Administration	Allows an Account Administrator to view account roles in an account. This is a new permission as of the January 2018 Deployment.
View Account Users	Security Administration	Allows an Account Administrator to view account users in an account. This is a new permission as of the January 2018 Deployment.
Basic Access for TSoftPlus	TSoftPlus	Allows a user to access TSoftPlus.
Manage Administration for TSoftPlus	TSoftPlus	Allows an Account Administrator to access Administration.
Assign or Remove Permissions for TSoftPlus	TSoftPlus	Allows an Account Administrator to assign or remove permissions for TSoftPlus. This permission works in combination with other Security Administration permissions (i.e. remove user from an account). It was created to prevent collisions for Accounts with more than one product. Example: An account is licensed for Product A and Product B. There are users in the Account for Product A and Product B. An Account Administrator for Product A needs to remove a user. There are users in the list for both Product A and Product B.

Default Permission	Permission Group	Description
		If the Account Administrator has the Assign or Remove Permissions for Product A and Assign or Remove Permissions for Product B, the Administrator can remove a user that has permissions for Product A and/or Product B. If the Account Administrator has the Assign or Remove Permissions for Product A only, the Administrator can only remove the users that have permission for Product A, and they are not allowed to remove a user that has Product B permissions.

TSoftPlus "Administrator" Default Role and Permissions

Default Permission	Permission Group	Description
Basic Access for TSoftPlus	TSoftPlus	Allows a user to access TSoftPlus.
Credit Memo - Open	TSoftPlus	Allows a user to open and edit the Credit Memo.
ETran Submission	TSoftPlus	Allows a user to submit a loan application electronically from TSoftPlus™ and receive an immediate response from SBA.
Financial Analysis - Open, Import	TSoftPlus	Allows a user to upload a Financial Analysis spreadsheet that has already had financial work either partially or totally completed. Allows a user to open or create a new Financial Analysis.
Import FormMaster+	TSoftPlus	Allows a user to import existing TSoft FormMaster loan information into TSoftPlus™. Requires the Loan - Create, View, Modify permission.
Loan Authorization - Open, Remove	TSoftPlus	Allows a user to open the Loan Authorization Wizard in Word 2007 or 2010 and delete the Loan Authorization.
Loan - Create, View, Modify	TSoftPlus	Allows a user to create, view, or modify loans in TSoftPlus™.
Loan-Copy	TSoftPlus	Allows a user to copy a loan. Requires the Loan - Create, View, Modify permission.
Loan-Remove	TSoftPlus	Allows a user to remove a loan.
Loan-Change Type or Organization	TSoftPlus	Allows a user to change a jurisdiction, organization, or loan type. Requires the Loan - Create, View, Modify permission.
Loan-Import XML	TSoftPlus	Allows a user to import transaction information (including ETran results and SBA number if applicable) that you received from another user of TSoftPlus.
Quick Quote-Create, View, Modify	TSoftPlus	Allows a user to create, view, or modify a quote on the Quick Quote page. Requires the Loan - Create, View, Modify permission.
Quick Quote-Remove	TSoftPlus	Allows a user to remove a quote from the Quick Quote screen.
System Setup	TSoftPlus (Installed Version only)	Allows a user to access System Settings to set session timeouts, set maximum concurrent document generation requests, and update content.
Remove PDFs	TSoftPlus	Allows a user to remove any .PDF files that have been uploaded to the loan.

Default Permission	*Permission Group*	*Description*
Upload PDFs	TSoftPlus	Allows a user to upload additional .PDF files into TSoftPlus.

TSoftPlus "Loan Processor" Default Role and Permissions

Default Permission	*Permission Group*	*Description*
Basic Access for TSoftPlus	TSoftPlus	Allows a user to access TSoftPlus.
Credit Memo - Open	TSoftPlus	Allows a user to open and edit the Credit Memo.
ETran Submission	TSoftPlus	Allows a user to submit a loan application electronically from TSoftPlus™ and receive an immediate response from SBA.
Financial Analysis - Open, Import	TSoftPlus	Allows a user to upload a Financial Analysis spreadsheet that has already had financial work either partially or totally completed. Allows a user to open or create a new Financial Analysis.
Loan Authorization - Open, Remove	TSoftPlus	Allows a user to open the Loan Authorization Wizard in Word 2007 or 2010 and delete the Loan Authorization.
Loan - Create, View, Modify	TSoftPlus	Allows a user to create, view, or modify loans in TSoftPlus™.
Loan-Copy	TSoftPlus	Allows a user to copy a loan. Requires the Loan - Create, View, Modify permission.
Loan-Remove	TSoftPlus	Allows a user to remove a loan.
Loan-Change Type or Organization	TSoftPlus	Allows a user to change a jurisdiction, organization, or loan type. Requires the Loan - Create, View, Modify permission.
Loan-Import XML	TSoftPlus	Allows a user to import transaction information (including ETran results and SBA number if applicable) that you received from another user of TSoftPlus™.
Quick Quote-Create, View, Modify	TSoftPlus	Allows a user to create, view, or modify a quote on the Quick Quote page. Requires the Loan - Create, View, Modify permission.
Quick Quote-Remove	TSoftPlus	Allows a user to remove a quote from the Quick Quote screen.
Remove PDFs	TSoftPlus	Allows a user to remove any .PDF files that have been uploaded to the loan.
Upload PDFs	TSoftPlus	Allows a user to upload additional .PDF files into TSoftPlus™.

TSoftPlus Available Permissions for Custom Roles

Default Permission	*Permission Group*	*Description*
Add User to Account	Security Administration	Allows an Account Administrator to add users to an account. This is a new permission as of the January 2018 Deployment.
Assign or Remove Permissions for Security Administration	Security Administration	Allows an Account Administrator to assign or remove permissions in Security Administration. This is a new permission as of the January 2018 Deployment.

Default Permission	*Permission Group*	*Description*
Basic Access for Security Administration	Security Administration	Allows a user to have basic access to Security Administration. This is a new permission as of the January 2018 Deployment.
Clone Account	Security Administration	Allows an Account Administrator to copy an account to create additional accounts.
Download Certificates	Security Administration	Allows an Account Administrator to view the Client Authentication Page and download a certificate for configuring the integrations between products.
Edit Account (Prior to the January 2018 Deployment, was Manage Account permission)	Security Administration	Allows an Account Administrator to manage account information. This was the previous Manage Account permission.
Edit Account Roles	Security Administration	Allows an Account Administrator to edit account roles in an account. This is a new permission as of the January 2018 Deployment.
Edit Account Users (Prior to the January 2018 Deployment, was Manage Account Users permission)	Security Administration	Allows an Account Administrator to edit account users in an account. This was the previous Manage Account Users permission.
Manage IP Filtering	Security Administration	Allows an Account Administrator to add or remove IP Addresses in the IP Address list in IP Filtering.
Remove User from Account	Security Administration	Allows an Account Administrator to remove users in an account. This is a new permission as of the January 2018 Deployment.
Reset Account User Password	Security Administration	Allows an Account Administrator to reset an Account User password in an account. This is a new permission as of the January 2018 Deployment.
Unlock Account User	Security Administration	Allows an Account Administrator to unlock a user in an account. This is a new permission as of the January 2018 Deployment.
View Account Roles	Security Administration	Allows an Account Administrator to view account roles in an account. This is a new permission as of the January 2018 Deployment.
View Account Users	Security Administration	Allows an Account Administrator to view account users in an account. This is a new permission as of the January 2018 Deployment.
Basic Access for TSoftPlus	TSoftPlus	Allows a user to access TSoftPlus.
Credit Memo - Open	TSoftPlus	Allows a user to open and edit the Credit Memo.
Download Manage Transactions Report	TSoftPlus	Allows a user to create a CSV-based report that is downloaded from the Manage Transactions page. The report contains transactional data.
ETran Submission	TSoftPlus	Allows a user to submit a loan application electronically from TSoftPlus™ and receive an immediate response from SBA.
Financial Analysis - Open, Import	TSoftPlus	Allows a user to upload a Financial Analysis spreadsheet that has already had financial work either partially or totally completed. Allows a user to open or create a new Financial Analysis.
Loan Authorization - Open, Remove	TSoftPlus	Allows a user to open the Loan Authorization Wizard in Word 2007 or 2010 and delete the Loan Authorization.

Default Permission	*Permission Group*	*Description*
Loan - Create, View, Modify	TSoftPlus	Allows a user to create, view, or modify loans in TSoftPlus™.
Loan-Copy	TSoftPlus	Allows a user to copy a loan. Requires the Loan - Create, View, Modify permission.
Loan-Remove	TSoftPlus	Allows a user to remove a loan.
Loan-Change Type or Organization	TSoftPlus	Allows a user to change a jurisdiction, organization, or loan type. Requires the Loan - Create, View, Modify permission.
Loan-Import XML	TSoftPlus	Allows a user to import transaction information (including ETran results and SBA number if applicable) that you received from another user of TSoftPlus™.
Manage Administration for TSoftPlus	TSoftPlus	Allows an Account Administrator to access Administration.
Quick Quote-Create, View, Modify	TSoftPlus	Allows a user to create, view, or modify a quote on the Quick Quote page. Requires the Loan - Create, View, Modify permission.
Quick Quote-Remove	TSoftPlus	Allows a user to remove a quote from the Quick Quote screen.
Remove PDFs	TSoftPlus	Allows a user to remove any .PDF files that have been uploaded to the loan.
System Setup	TSoftPlus (Installed Version only)	Allows a user to access System Settings to set session timeouts, set maximum concurrent document generation requests, and update content.
Upload PDFs	TSoftPlus	Allows a user to upload additional .PDF files into TSoftPlus™.

IP Filtering

Wolters Kluwer SaaS products allow access from any location so you can access our products from various events and allow employees to work from home. If you prefer to limit access to the product(s) to your physical location, the IP (Internet Protocol) Address Whitelist feature gives you this control. IP addresses that aren't on the Whitelist will be blocked from accessing your licensed products. Your licensed products for an account are located in Account Details.

- The IP Filtering section only displays if you are assigned the Manage Security Administration Role with the Manage IP Filtering permission selected.
- IP Filtering allows you to limit access to IP addresses that you enter in Security Administration. Select **Enable IP Filtering** to activate filtering for the addresses you enter.
- IP Filtering applies to all products listed on the Account Details page.

Adding an IP Address to the IP Address Whitelist

- An IP address is a unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.
- In general, the IP address for this feature needs to be the "public facing" IP address which may be different than an individual computer's IP address.
- You can search for "What is my IP address" in your browser if you want to determine or confirm your public facing IP address.

- If a network is using Dynamic Host Configuration Protocol (DHCP), note that the administrator will need to be prepared ahead of time for this change and update IP Filtering accordingly.

Note
If this feature is configured incorrectly, you can completely block access for all of your users. It is important to have someone with network configuration knowledge involved in the setup of this feature. Modifying the IP Address Whitelist is not recommended during regular business hours. Users may be negatively affected if changes are made while using the application.

---

1. On the IP Address Whitelist page, select **+IP Address** to add an IP address to the IP Address Whitelist.
2. Enter an address and description.

- Select **Current IP Address** to add the current address. Enter a description.

3. Select **+** to add another address.
4. Select **Save** when finished.

- If you select **Enable IP Filtering** on the IP Address Whitelist page, IP addresses that aren't on the Whitelist will be blocked from accessing your licensed products. Your licensed products for an account are located in Account Details.

Multifactor Authentication (TOTP)(New Help Tile)

Overview

Multifactor Authentication (TOTP) is now supported and offers additional security for users logging into an application. TOTP uses a time-based, one-time password generated by an algorithm that uses the current time of day as one of its authentication factors. TOTP is enabled through Security Administration.

After multifactor authentication (TOTP) is enabled, a user must use a third-party authenticator application to generate a secondary passcode. During the login in process, a user will be required to enter the secondary passcode to access the application.

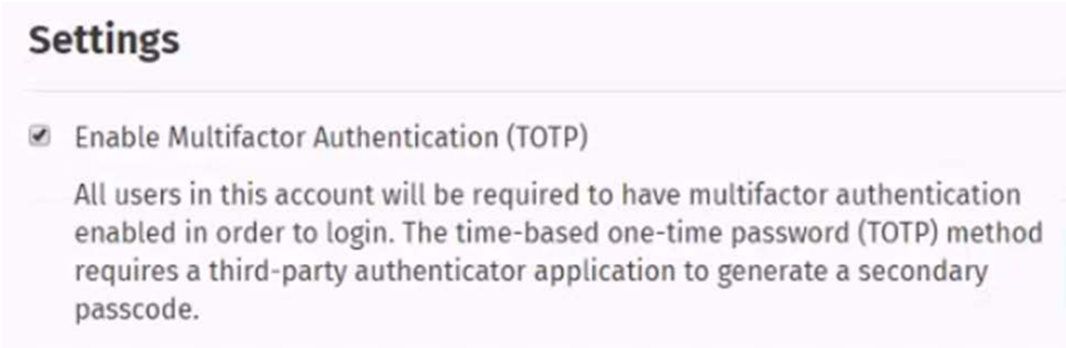
Note: Multifactor authentication (TOTP) is enabled on the account level. All users in the account must use multifactor authentication to access the applications in the account.

Setup

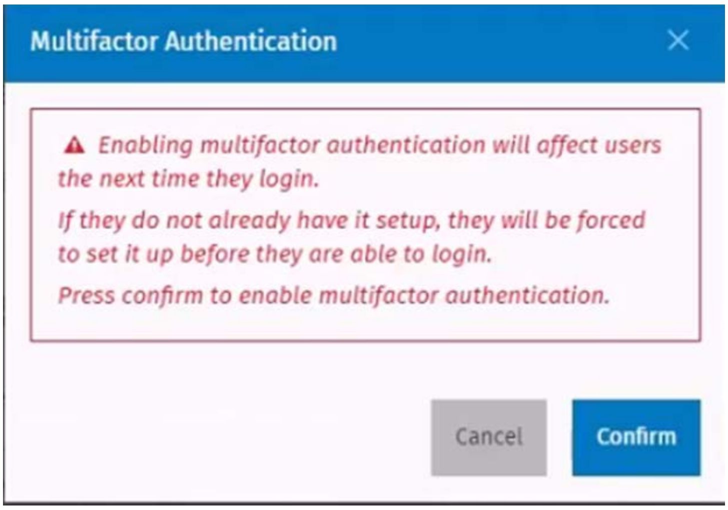
Multifactor Authentication (TOTP) (Security Administration Administrators)

To enable multifactor authentication:

1. In Security Administration, open the account that will use multifactor authentication.
2. Scroll to the bottom of the Account Details page.
3. Under settings, select **Enable Multifactor Authentication (TOTP)** and select **Save**.



4. Select **Confirm** on the confirmation message that displays.



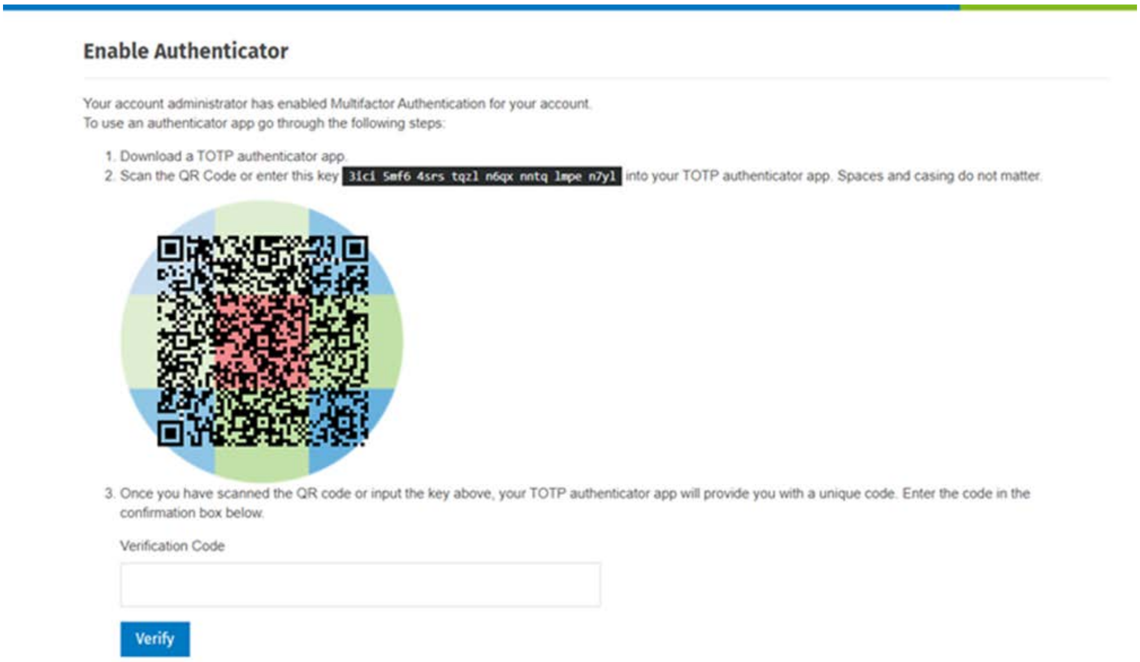
Multifactor Authentication (TOTP) (Users)

After the multifactor authentication is enabled, a user must use a third-party authenticator application to generate a secondary passcode used during authentication. An IT administrator can provide information and recommend a third-party authenticator to use.

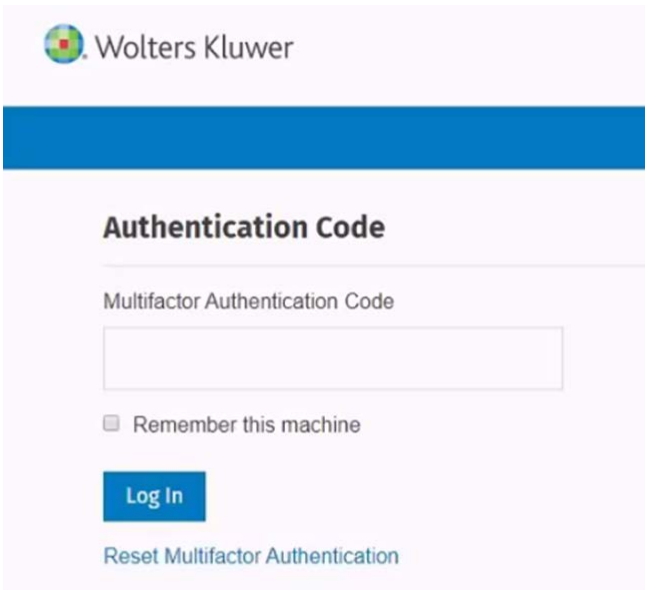
To use multifactor authentication

After multifactor authentication has been enabled in Security Administration, the Enable Authenticator page displays the first time a user enters a user name and password for a Wolters Kluwer application. The Enable Authenticator page will not display after the first time unless multifactor authentication is reset.

1. Enter the TOTP code that displays in the authenticator app in the Verification Code box on the Enable Authenticator page and select **Verify**.



2. Enter the code from your third-party multifactor authentication application and select **Login** on the Authentication Code page.



Note

If a user selects **Remember this machine**, the Authentication Code page does not display for fourteen days unless:

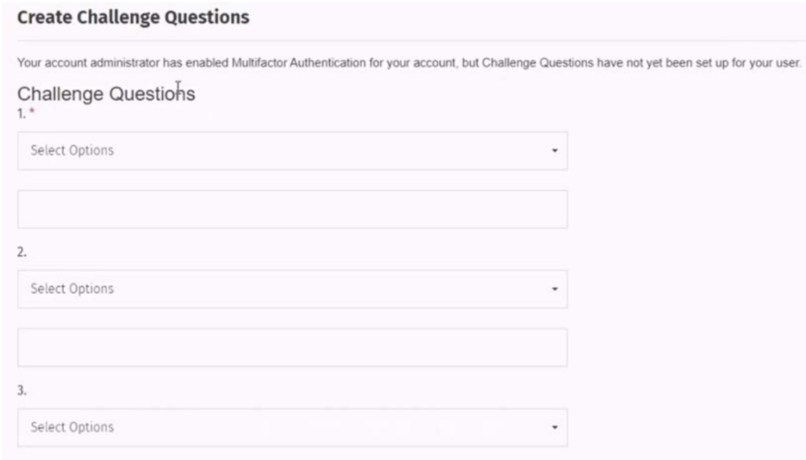
- The user logs in using a different browser.
- The user clears their cookies.
- Another user logs into the computer used by the previous user and selects Remember this machine. (The computer remembers the last person who selects Remember this machine.)

Note

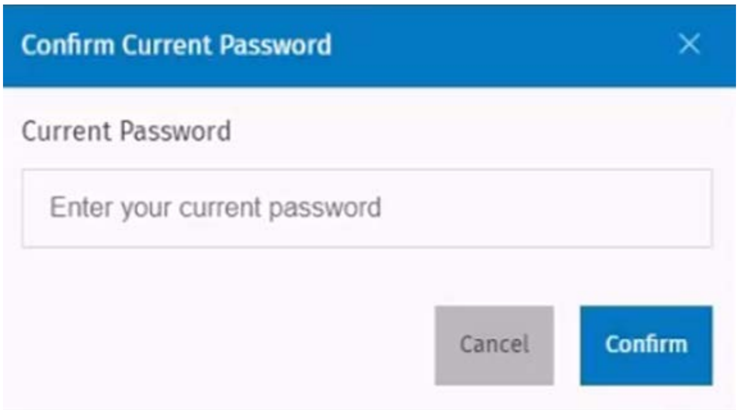
If a user has not set up challenge questions in their User Profile, the Create Challenge Questions page displays before the Enable Authenticator page. A user is required to set up challenge questions to proceed with multifactor authentication. Select **Challenge Questions** for Help Information.

Challenge Questions

- To set up challenge questions, select challenge questions and enter answers. Select **Save**.



- Enter a current password and select **Confirm**.



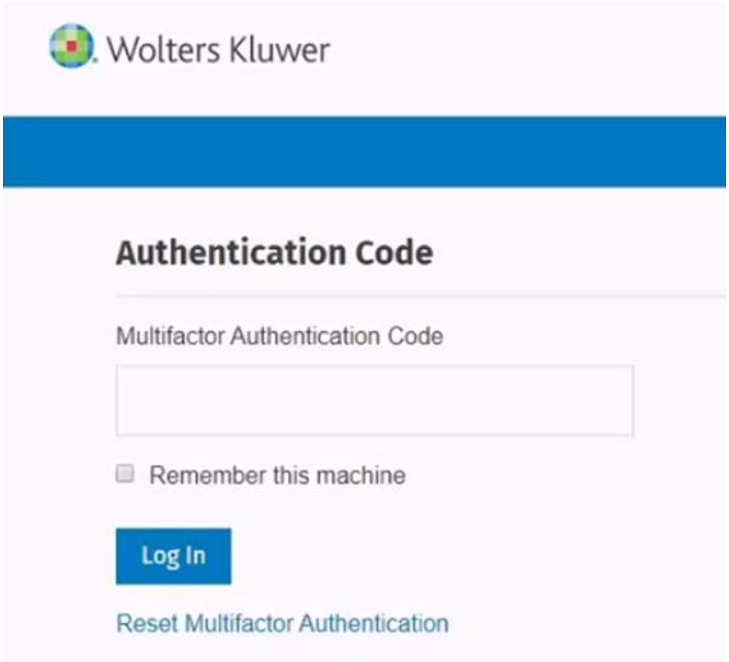
Resetting Multifactor (TOTP) Authentication

Note
Resetting multifactor authentication will require reconfiguring the third-party authenticator application. Select **To use multifactor authentication** for Help Information.

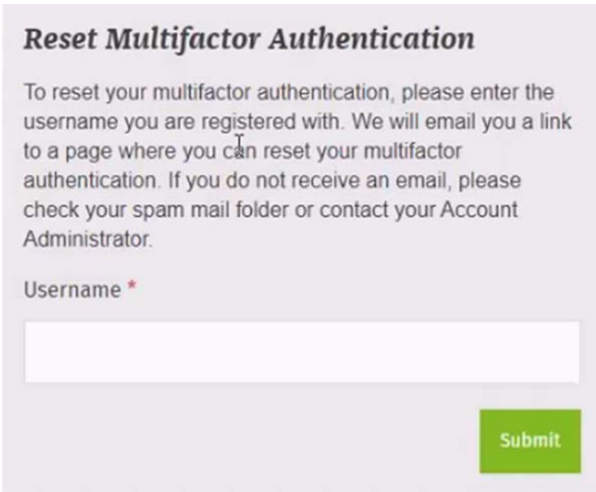
Resetting multifactor authentication (TOTP) on the Authentication Code page

To reset multifactor authentication as a user

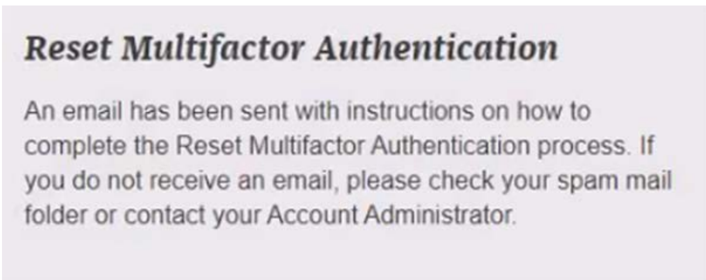
1. Select the **Reset the Multifactor Authentication** link on the Authentication Code page.



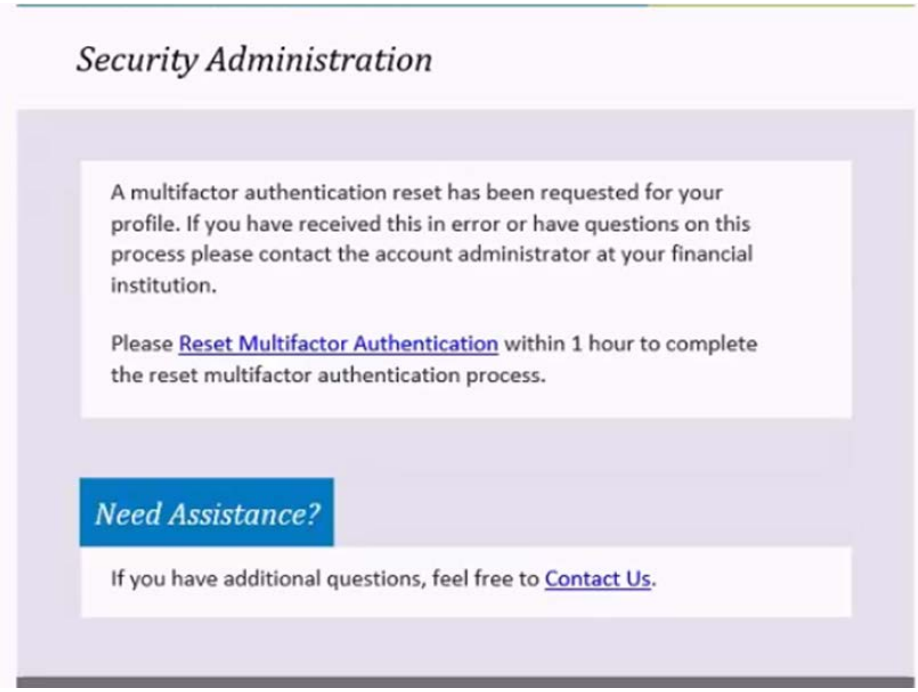
2. Enter the username used to log in to the Wolters Kluwer application.



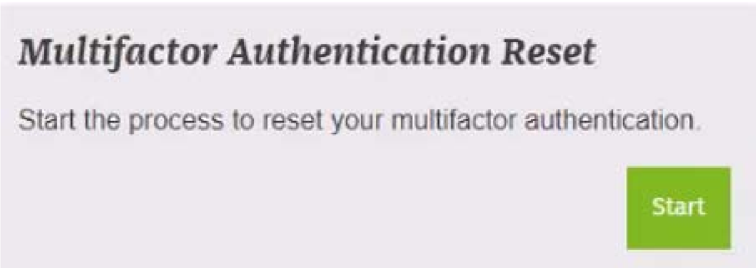
Note: A confirmation message displays after you enter the username.



3. Select the **Reset Multifactor Authentication** link in the email sent by Wolters Kluwer.

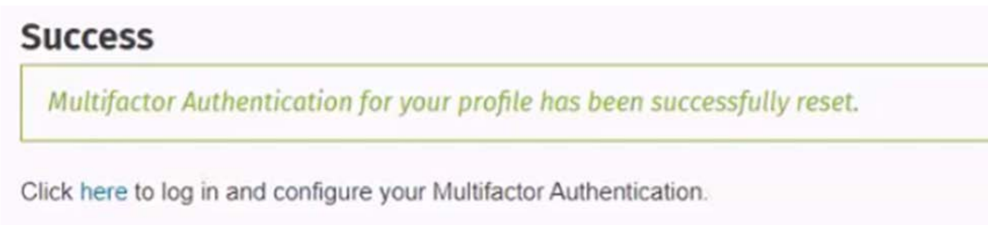


4. Select **Start** on the Multifactor Authentication Reset message.



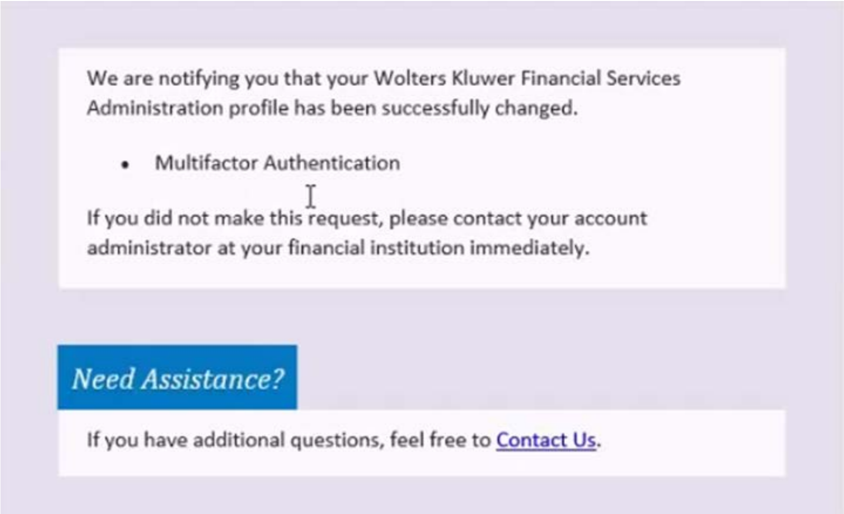
5. Answer the two challenge questions correctly on the pages that display.

6. Select the **here** link to log in and configure your multifactor authentication on the Success page that displays. Select **To use multifactor authentication** for Help information about configuring multifactor authentication.



Note

You will receive an email confirming the multifactor authentication reset.

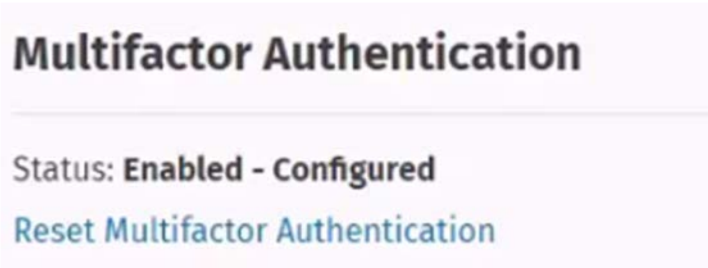


Resetting multifactor authentication (TOTP) in Security Administration

An administrator assigned the Reset Account User Multifactor Authentication permission in Security Administration can reset multifactor authentication for a user.

1. In Security Administration, select the account. Select the Users tab and select the user.

2. Select the **Reset Multifactor Authentication** link under Multifactor Authentication section.



Note
The status changes to Enabled-Not Configured under Multifactor Authentication after resetting multifactor authentication.

Note
The user will be required to reconfigure multifactor authentication the next time they log in.

Client Authentication

Client Authentication only displays if you are assigned the Manage Security Administration Role with the Download Certificates permission selected. This section displays a list of certificates for your account. You can download the certificates provided by Wolters Kluwer.

Frequently Asked Questions

What is the Time Out limit before a user is logged out?

A user is logged out:

- After 20 minutes of inactivity.
- When remaining on the same page for more than 20 minutes.

How does a user change/review their user information?

A user can select their name at the top of the page. Selecting Edit Profile, Edit Questions, or Change Password allows a user to make changes to those areas. The products and accounts where the user has access are also displayed.

What browsers are supported for Security Administration?

Security Administration is built on a responsive platform that allows the application to adjust to your browser's resolution. Security Administration is compatible with:

- Internet Explorer 11 (compatibility mode must be disabled)
- Google Chrome

How do I contact Support?

Access the Solutions Support website at http://www.wolterskluwerfs.com/support/ and select **Contact Us**.