

GUIDE

Kerio Two-Factor Authentication



GFI Software™

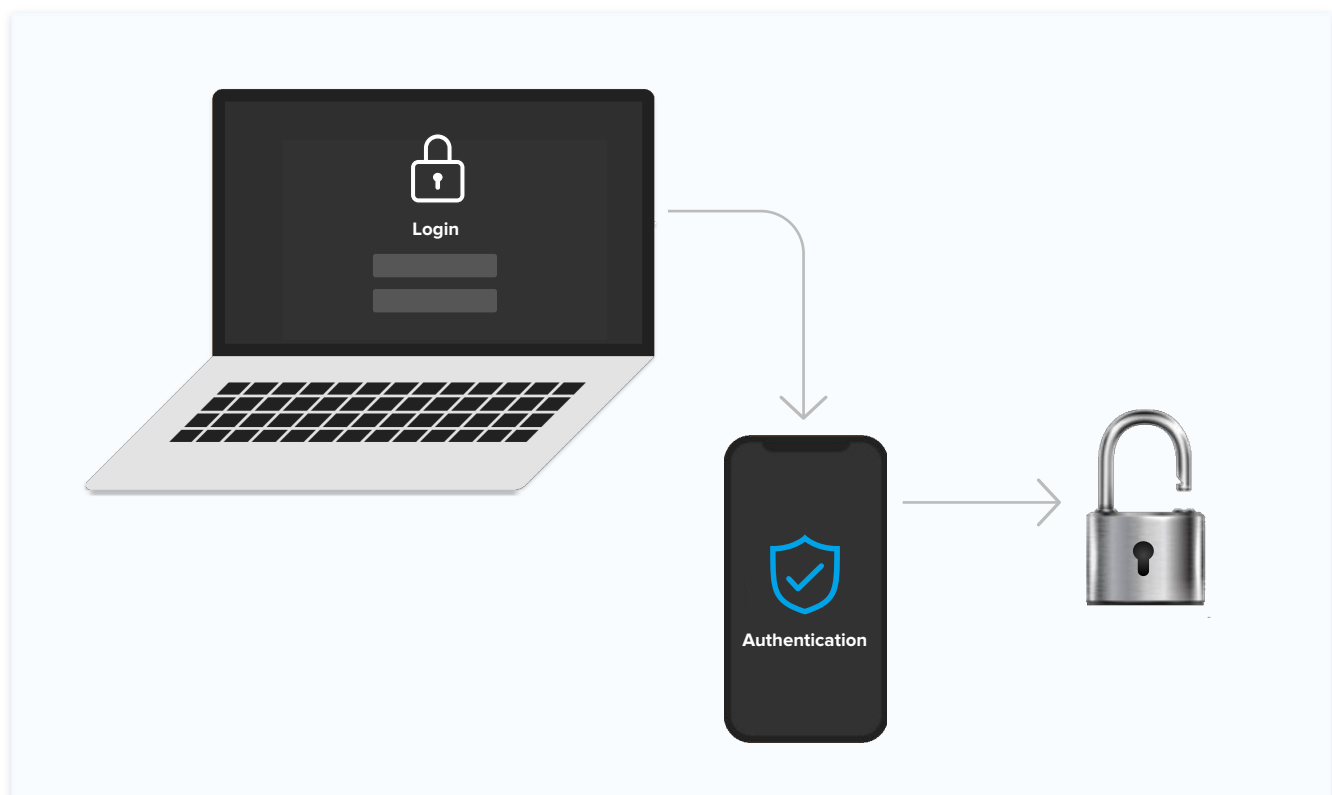
Table of Contents

Kerio Two-Factor Authentication	3
Configuring 2-step verification	4
Enabling the 2-step verification	5
Scenario One - When 2-step verification is optional for all users within the domain	6
Scenario Two - When 2-step verification is enforced for all users within the domain	12
Using recovery email	14
Resetting and turning off 2-step verification	15
Enabling the 2-step verification for the administrator	16
Logs for 2-step verification	17
Application passwords	18
Let's Encrypt integration	19

Kerio Two-Factor Authentication

Kerio Connect Version 9.4 integrates Two-Factor Authentication (2FA) for additional access security. It uses Google and Microsoft mobile device authenticators to supply a real-time token so that administrators have control over the needed level of security. It can also be enabled for Kerio Connect admin console access.

Two-Factor Authentication complements the Kerio Connect Secure Email system. It provides an additional layer of security if usernames or passwords are compromised by phishing or other malicious attacks.





Configuring 2-step verification

This 2-step verification adds an extra layer of security to your account by using an application on the user's smartphone to confirm their identity. By using 2-step verification, even if standard credentials are not compromised, access is not granted unless the second step is verified.

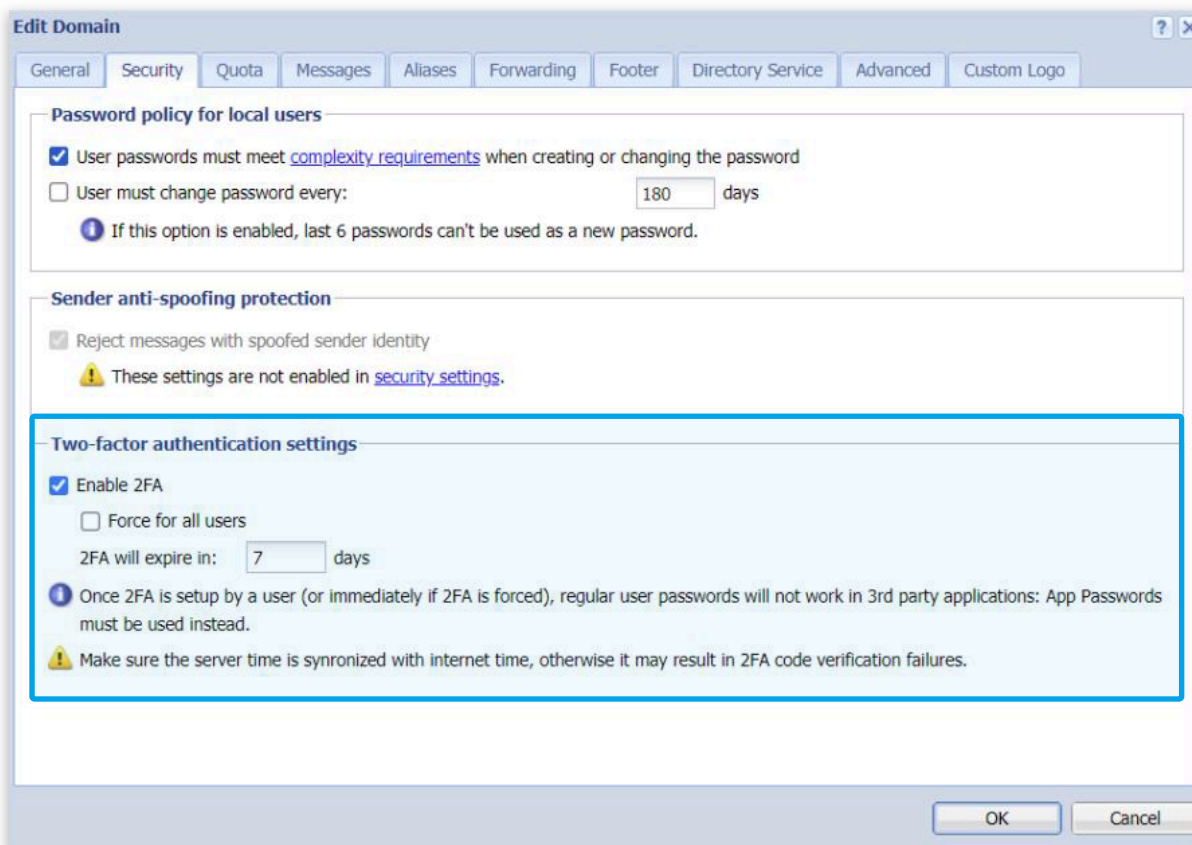
For access, users must first use their credentials to authenticate. Additionally, they must type in a special time-limited code generated by an authentication application on their phones or computers. The authentication must be supported by the Internet Engineering Task Force (IETF) standard RFC 6238. Examples include Google authenticator (available for iOS, Android, Windows phone) and FreeOTP authenticator (available for iOS and Android), though there can be other authentication applications.

The 2-step verification protects these parts of the product:

- ✓ Admin web interface
- ✓ Kerio Connect webmail
- ✓ Kerio Connect client

Enabling the 2-step verification

The administrator can configure 2-step verification per domain. The setting can be found on the Security tab when editing a specific domain.



Edit Domain

General Security Quota Messages Aliases Forwarding Footer Directory Service Advanced Custom Logo

Password policy for local users

☒ User passwords must meet [complexity requirements](#) when creating or changing the password

☐ User must change password every: days

Sender anti-spoofing protection

☒ Reject messages with spoofed sender identity

Two-factor authentication settings

☒ Enable 2FA

☐ Force for all users

2FA will expire in: days

Once 2FA is setup by a user (or immediately if 2FA is forced), regular user passwords will not work in 3rd party applications: App Passwords must be used instead.

Make sure the server time is synchronized with internet time, otherwise it may result in 2FA code verification failures.

OK Cancel

The administrator can choose to set up 2-step verification as optional for all users in the domain or they can enforce this security setting on all users.

NOTE

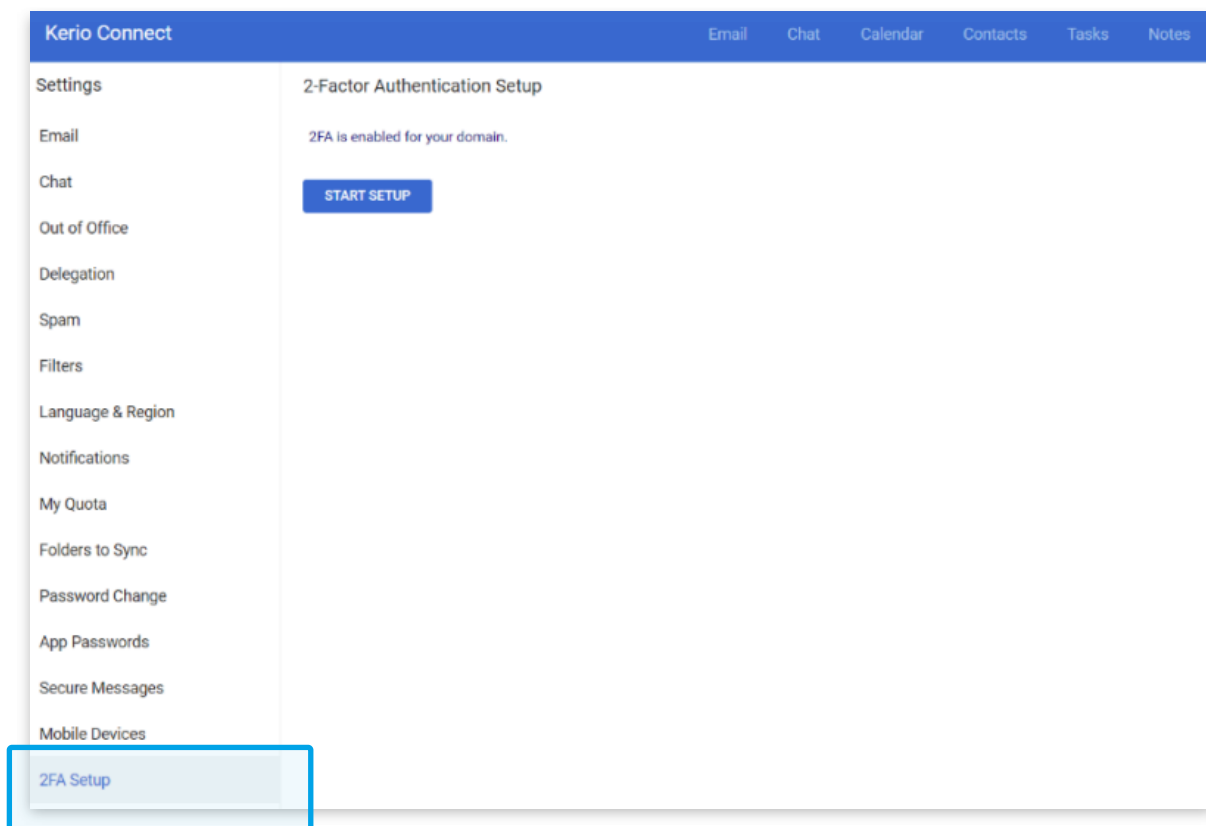
Since 2 step verification code is time based, it is important to check the OS time on the server where Kerio Connect mail server is deployed. The OS time should be in sync with the internet time otherwise it may result in verification failures.

Scenario One

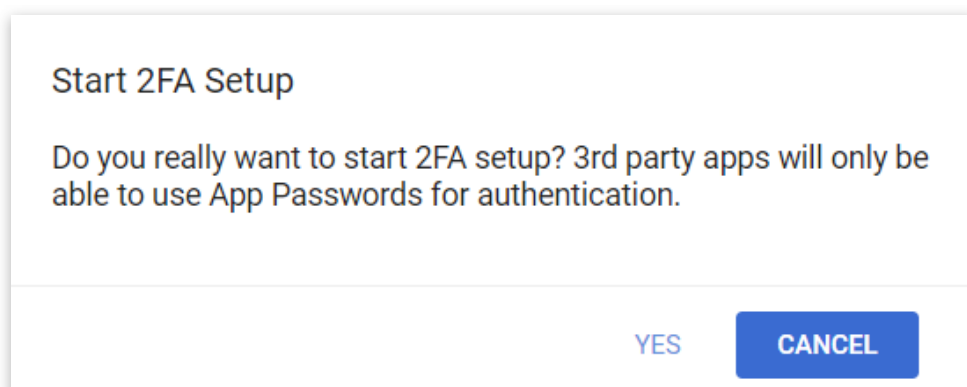
When 2-step verification is optional for all users within the domain

Process for enabling 2-step verification in Kerio Connect webmail

- Enter webmail the standard way on <https://<yourIP>/webmail>
- Authenticate using standard credentials
- Within the user interface, navigate to Settings menu
- At the bottom of the menu is “2FA Setup”:



- Click on the “Start 2FA Setup” button
- In the following dialog box, confirm that you want to start the 2-step verification setup:



Then on the following screen:

- 1 Type in the recovery email address that you want to use to receive the reset code for 2-step verification. Note that the recovery email address must be different from the current email address.
- 2 Scan the QR code with your preferred authentication application.
- 3 The Authentication application will generate a six digit code. Write down the code in the Authentication token column.

2-Factor Authentication Setup

2FA is enabled for your domain.

Secret Key
DSU6XQQIUI5ZRHYXGOLBA7LBSGW2SR06

Recovery e-mail address

 1

Authentication token

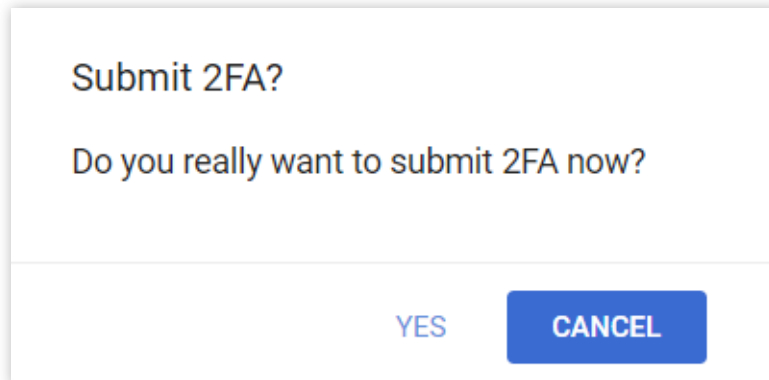
 3

 2

i NOTE

It is recommended that the recovery email be an email address outside the domain to which you have access.

Once all the information has been submitted correctly, the system will ask for the last verification:

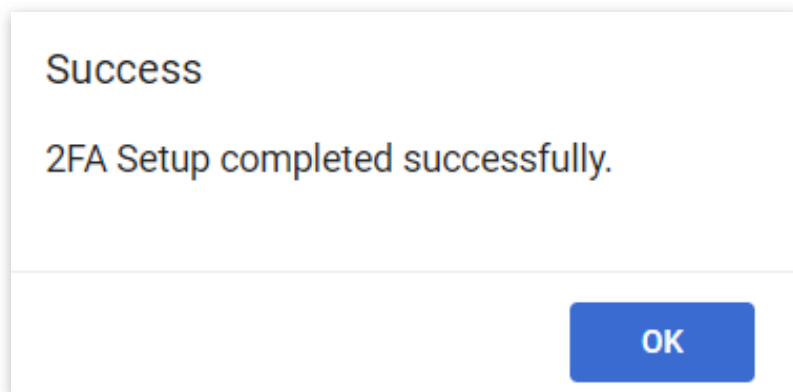
A dialog box with a white background and a thin gray border. It contains the text "Submit 2FA?" in bold, followed by "Do you really want to submit 2FA now?". At the bottom, there are two buttons: "YES" in blue text and "CANCEL" in white text on a blue background.

Submit 2FA?

Do you really want to submit 2FA now?

YES CANCEL

Once verified, the system will inform you whether the 2-step verification was configured successfully. You may be asked to submit a 2-step verification code depending on domain settings.

A dialog box with a white background and a thin gray border. It contains the text "Success" in bold, followed by "2FA Setup completed successfully.". At the bottom right, there is a button with the text "OK" in white on a blue background.

Success

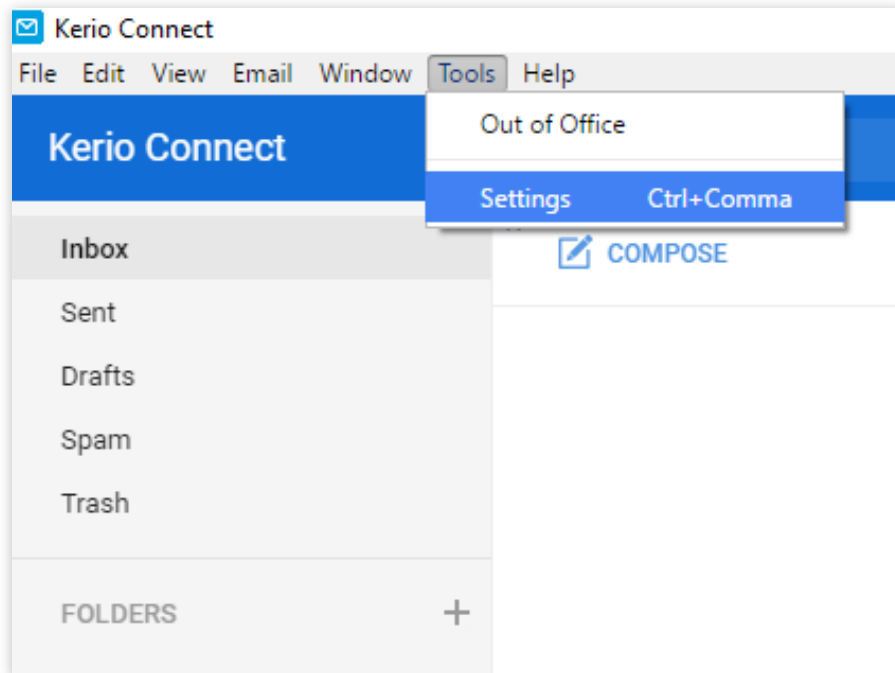
2FA Setup completed successfully.

OK

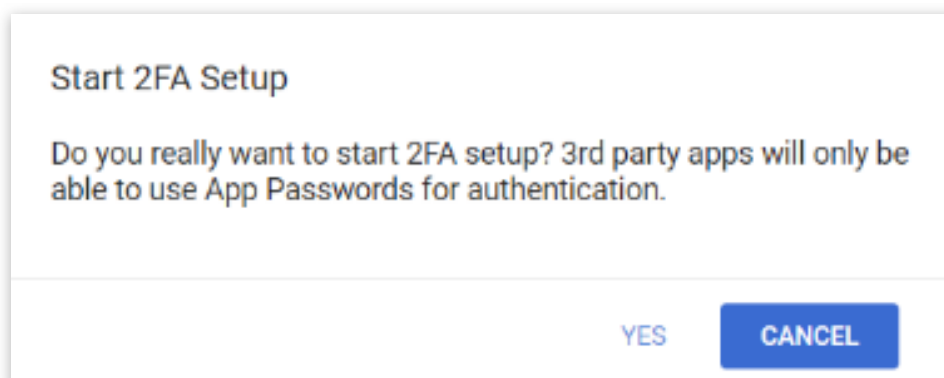
Process for enabling 2-step verification in Kerio Connect client mail

- Open Kerio Connect client the standard way
- Authenticate using standard credentials

Navigate to the 2-step verification setup which is found under: Tools / Settings / 2FA setup



- Click on the “Start 2FA Setup” button
- In the following dialog box, confirm that you want to start the 2-step verification setup:



Then on the following screen:

- 1 Type in the recovery email address that you want to use to receive the reset code for 2-step verification. Note that the recovery email address must be different from the current email address.
- 2 Scan the QR code with your preferred authentication application.
- 3 The Authentication application will generate a six digit code. Write down the code in the Authentication token column.

2-Factor Authentication Setup

2FA is enabled for your domain.

Secret Key
DSU6XQQIUI5ZRHYXGOLBA7LBSGW2SR06

Recovery e-mail address

 1

Authentication token

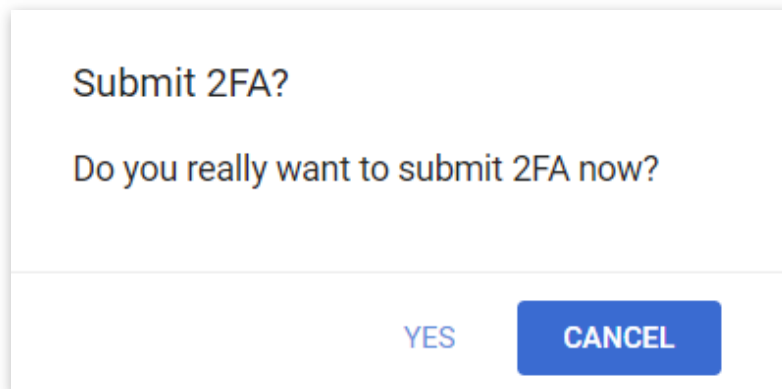
 3

 2

i NOTE

It is recommended that the recovery email be an email address outside the domain to which you have access.

Once all the information has been submitted correctly, the system will ask for the last verification:

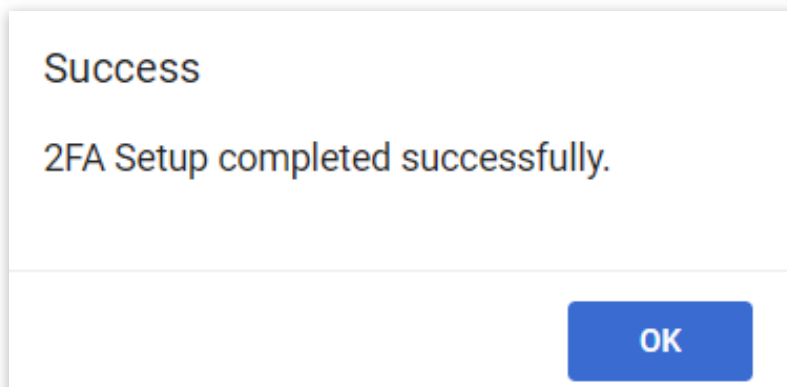
A white dialog box with a light gray border. The title is "Submit 2FA?". The main text is "Do you really want to submit 2FA now?". At the bottom, there are two buttons: "YES" in blue text and "CANCEL" in white text on a blue background.

Submit 2FA?

Do you really want to submit 2FA now?

YES CANCEL

Once verified, the system will inform you whether the 2-step verification was configured successfully. You may be asked to submit a 2-step verification code depending on domain settings.

A white dialog box with a light gray border. The title is "Success". The main text is "2FA Setup completed successfully.". At the bottom right, there is a blue button with the text "OK" in white.

Success

2FA Setup completed successfully.

OK

i NOTE

Older KerioConnect clients are not compatible with the new Kerio Connect server 9.4 because of the lack of 2 step verification support.

Scenario Two

When 2-step verification is enforced for all users within the domain

Process for enabling 2-step verification in Kerio Connect webmail

- Enter webmail the standard way on <https://<yourIP>/webmail>
- Authenticate using standard credentials
- After successful authentication, a 2-step verification setup screen will appear
- Complete the configuration by following the steps described in previous section



The image shows a webmail interface for KerioConnect. At the top, there is a blue envelope icon and the text "KerioConnect". Below this, a white box contains the "Secret Key" "UZ6ATGU27VHYOL7G33QTXEINSZ56JSLP" and a QR code. Under the QR code, there are two input fields: the first contains "yourRecoveryEmail@domain.com" and the second is labeled "2FA Code". A blue button labeled "Submit 2FA Code" is positioned below the input fields. At the bottom of the white box, a note reads: "Please enter 2FA Code using Google or Microsoft Authenticator Apps".

Process for enabling 2-step verification in Kerio Connect client mail

- Open Kerio Connect client the standard way
- Authenticate using standard credentials
- After successful authentication, a 2-step verification setup screen will appear
- Complete the configuration by following the steps described in previous section

The image shows a mobile application interface for KerioConnect. At the top, there is a blue square icon with a white envelope and the text "KerioConnect" in blue. Below this, a white box contains the text "2FA setup required!" in red. Underneath is a large QR code. Below the QR code is a unique alphanumeric code: "UZ6ATGU27VHYOL7G33QTXEINSZ56JSLP". There are two input fields: the first is labeled "2FA Code" and the second contains the placeholder text "yourRecoveryEmail@domain.com". Below these fields is a blue "Login" button and a "Relogin" link. At the bottom of the white box, the text "Version 9.4.0.16696" is displayed.

KerioConnect

2FA setup required!



UZ6ATGU27VHYOL7G33QTXEINSZ56JSLP

2FA Code

yourRecoveryEmail@domain.com

Login

[Relogin](#)

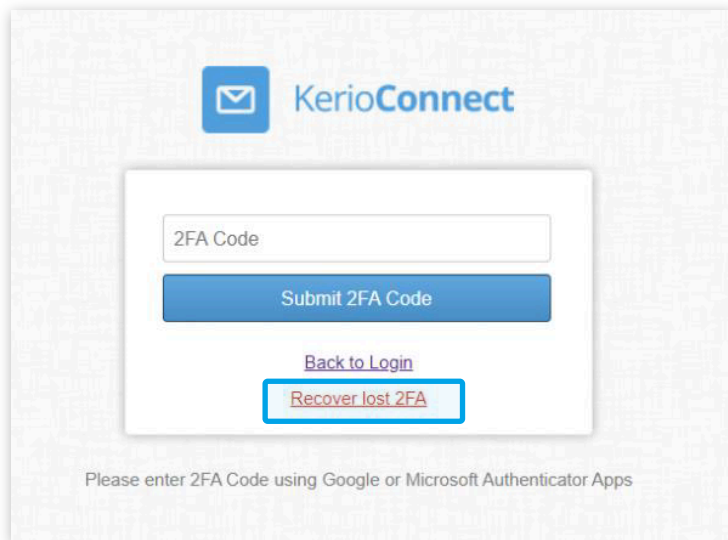
Version 9.4.0.16696

NOTE

Older KerioConnect clients are not compatible with the new Kerio Connect server 9.4 because of the lack of 2 step verification support.

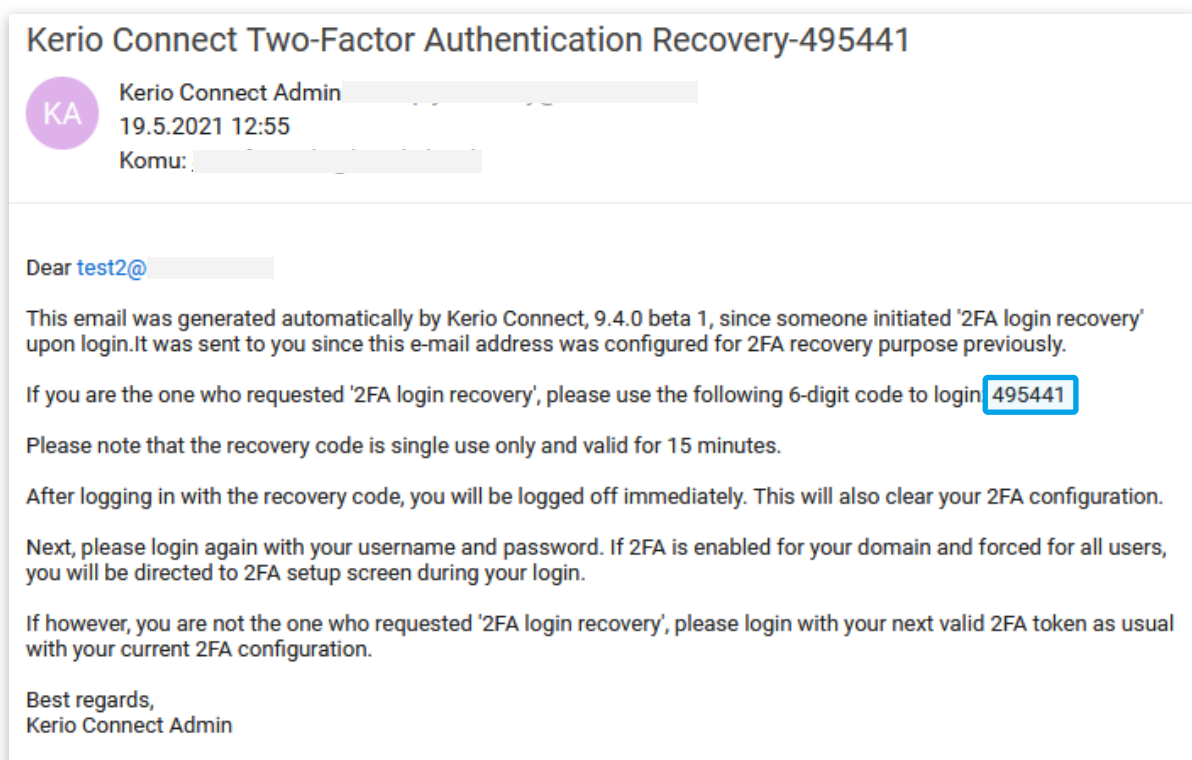
Using recovery email

If you lose access to your 2-step verification code, you can recover or reset these settings with the recovery email submitted during the initial 2-step verification configuration. To use this function, click on the “Recover lost 2FA” button during the 2-step verification.



The image shows the KerioConnect login interface. At the top is the KerioConnect logo. Below it is a form with a text input field labeled '2FA Code', a blue 'Submit 2FA Code' button, a blue link 'Back to Login', and a red-outlined button 'Recover lost 2FA'. At the bottom, a note says 'Please enter 2FA Code using Google or Microsoft Authenticator Apps'.

Once the “Recover lost 2FA” button has been pushed, the Kerio Connect mail server will send an email to the specified recovery email address:

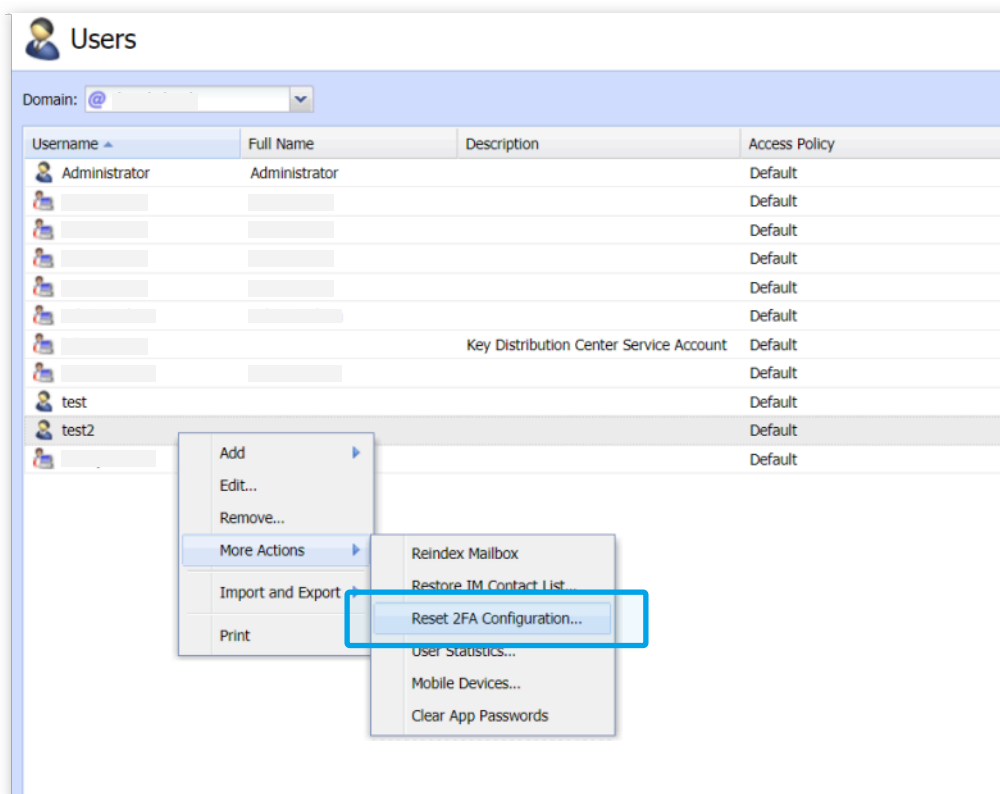


The email will include the recovery six digit code which needs to be submitted into the “2FA code” column. Once the code has been submitted, the 2-step verification settings will be reset and you will be redirected to the initial login screen to submit your credentials. Once authenticated, you will need to re-do the 2-step verification process.

Resetting and turning off 2-step verification

If the 2-step verification has been switched off, you won't need to use your 2-step verification codes any more. However, the system will retain existing settings for 2-step verification users. After switching the 2-step verification back on, you will not be required to repeat the 2-step verification process again, but you will be asked to submit your codes when logging on.

In a scenario where you do not have your 2-step verification code and you also do not have access to your recovery email, an Administrator can still reset it for specific users in the User Section of the chosen domain.



Once the 2-step verification is reset, you will need to re-do the 2-step verification process.

☑ Enabling the 2-step verification for the administrator

In Kerio Connect, there are two types of administrators:

- Built in admin
- Domain administrator with full access rights to admin interface

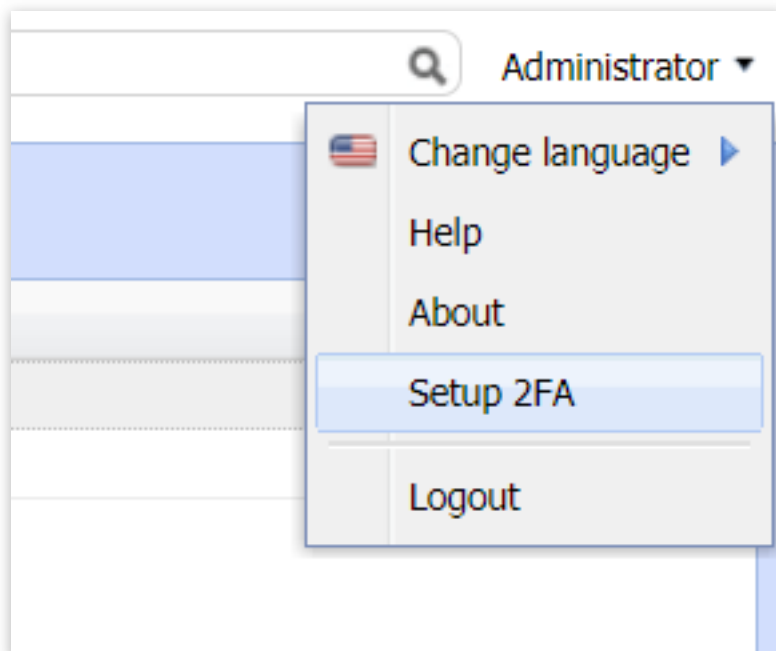
Both of these accounts can enable the 2-step verification.

i NOTE

It is critical that the existing administrator does not use their associated administrator email as the recovery email address. Doing so will prevent the administrator from receiving their recovery access code and trigger a lock out.

Process for enabling 2-step verification for the Kerio Connect Administrator

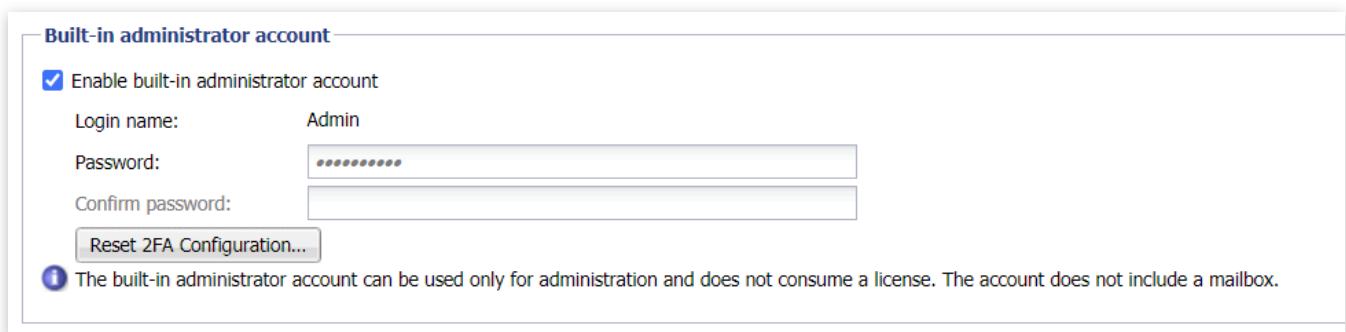
As the administrator, turn on the 2-step verification for the domain and go to Setup. You will find the “Setup 2FA” button in the top right corner drop down menu.



The following steps are identical to standard user steps described in previous sections

Process for enabling 2-step verification for the Kerio Connect built in admin

Once the built in admin account is enabled, you can turn on 2-step verification to enhance security. There needs to be at least one domain within Kerio Connect that has 2-step verification enabled. The setup of 2-step verification is exactly the same as described in previous sections. The only difference is how the 2-step verification can be reset. Since built in admin is not part of any domain, it has a separate reset button located in the Administration settings section:



Built-in administrator account

☒ Enable built-in administrator account

Login name: Admin

Password:

Confirm password:

[Reset 2FA Configuration...](#)

i The built-in administrator account can be used only for administration and does not consume a license. The account does not include a mailbox.



Logs for 2-step verification

All log messages regarding 2-step verification errors can be found in the *Logs/Error* section under the “TwoFAPolicyManSwitch.cpp” key.

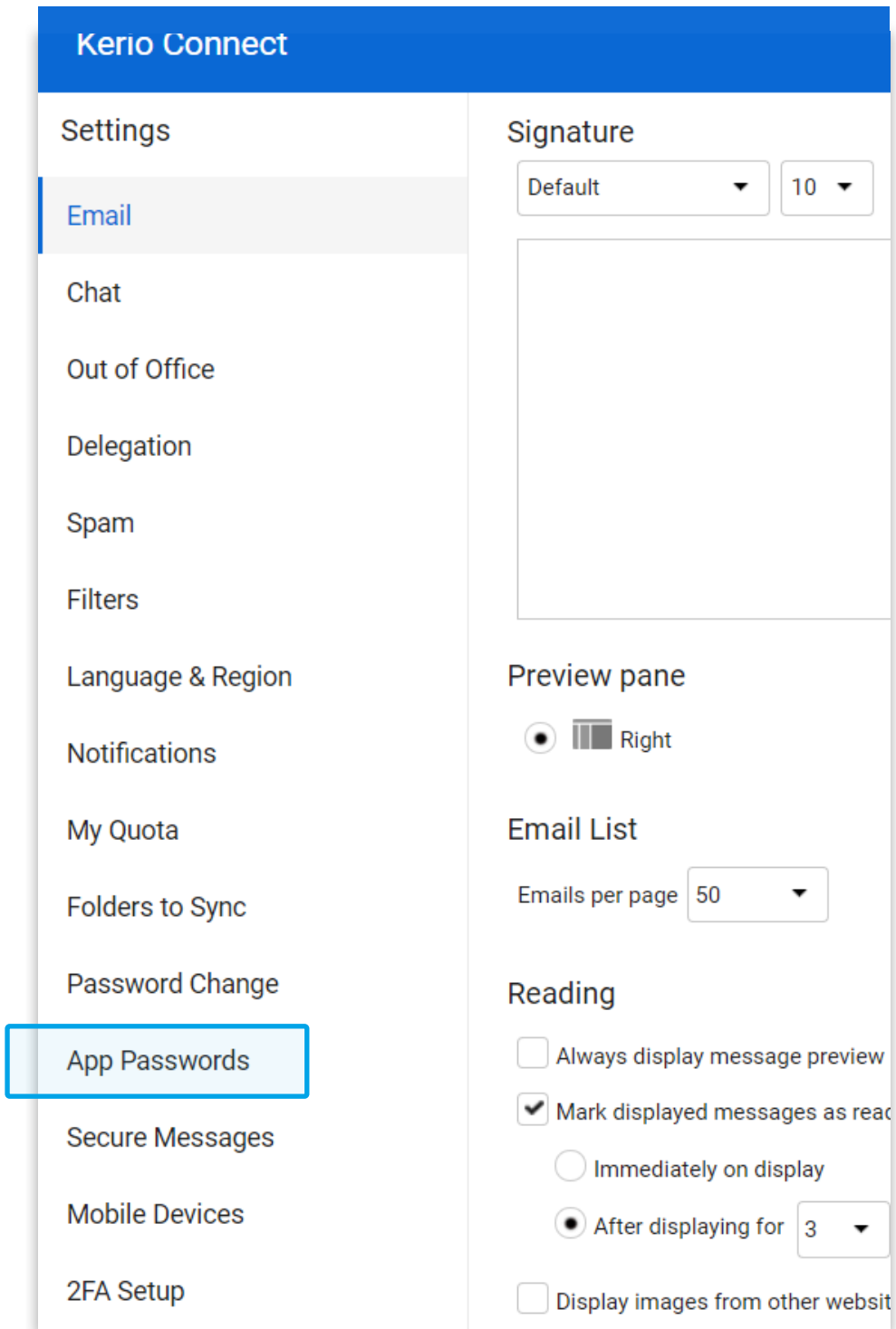
Example:

[17/May/2021 12:18:30] TwoFAPolicyManSwitch.cpp: 2FA cookie token verification error for user: 'Joe.Doe@gfi.com', error: Invalid cookie token.

An error like this means that the user has submitted an incorrect 2-step verification six digit code.

Application passwords

If 2FA is turned on and users are not using Kerio Client WebMail or Kerio Connect Client (but are using KOFF, IMAP or something similar), users will need to set up application passwords.



Kerio Connect

Settings

- Email
- Chat
- Out of Office
- Delegation
- Spam
- Filters
- Language & Region
- Notifications
- My Quota
- Folders to Sync
- Password Change
- App Passwords**
- Secure Messages
- Mobile Devices
- 2FA Setup

Signature

Default 10

Preview pane

☒ Right

Email List

Emails per page 50

Reading

☐ Always display message preview

☒ Mark displayed messages as read

☐ Immediately on display

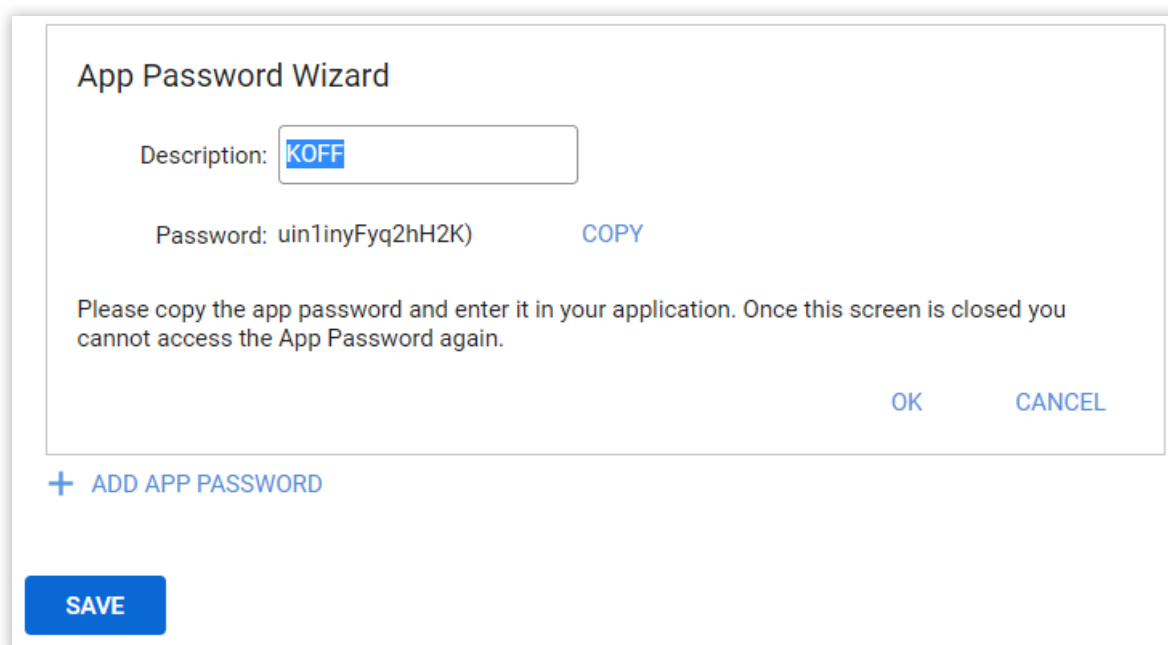
☒ After displaying for 3

☐ Display images from other websites

Once 2FA is turned on, standard account passwords will not work anymore when using KOFF, IMAP or similar. These passwords will be replaced by application passwords which can be created by a user within Kerio Connect WebMail or within Kerio Connect Client after submitting a 2FA code or after successfully setting up 2FA.

Once the application password is configured, the password can not be changed or reviewed. It is strongly suggested that users save their passwords in the password vault.

If the application password is lost, users can easily delete previous passwords and create a new one.



The screenshot shows a dialog box titled "App Password Wizard". It contains a "Description:" label followed by a text input field containing the word "KOFF". Below this, it displays "Password: uin1inyFyq2hH2K)" with a blue "COPY" link to its right. A warning message states: "Please copy the app password and enter it in your application. Once this screen is closed you cannot access the App Password again." At the bottom right of the dialog are "OK" and "CANCEL" buttons. Below the dialog box, there is a blue link that says "+ ADD APP PASSWORD". At the bottom left of the entire form area is a blue "SAVE" button.

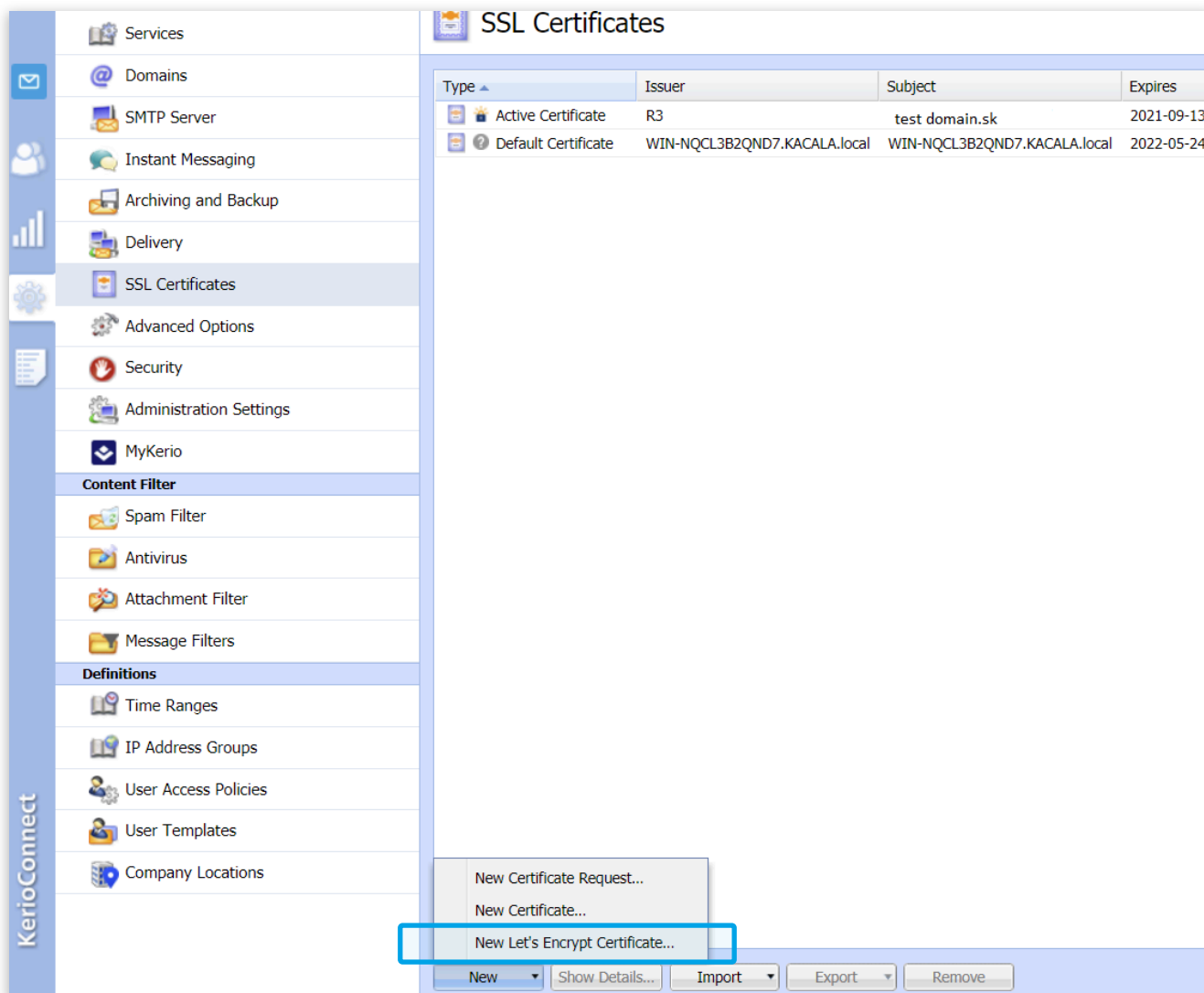


Let's Encrypt integration

Kerio Connect Version 9.4 adds better integration directly into the product for the Let's Encrypt not-for-profit SSL certification author -- including auto-renewal of their 90-day certificates. This makes it easier for businesses to stay secure without adding additional costs. Let's Encrypt is a free, automated and open certificate authority. SSL certificates in Kerio Connect play a huge role in security of the product and its communication mechanism.

Setting up the Let's Encrypt SSL certificate

Let's Encrypt integration is easy. You can find it in the SSL certificate tab “New” as shown here:



The next dialog box will ask you to submit the domain name where you want to generate the SSL certificate. To generate SSL certificates successfully, it is mandatory to have the Kerio Connect mail server reachable on port 80 / HTTP. The Let's Encrypt API will search for the submitted domain name and will verify all the needed information via HTTP.



Opening port 80 might be seen as a security risk for the server and users. It is therefore recommended to only use an encrypted connection with Kerio Connect. It will force users to use webmail over port 443 / HTTPS instead of an unsecured HTTP.

For more information, please refer to the manual:

<https://manuals.gfi.com/en/kerio/connect/content/server-configuration/security/securing-kerio-connect-1239.html#sect-securitypolicy>

Another option is to use an HTTP to HTTPS redirection function on the gateway firewall.

