



ADMINISTRATOR GUIDE

Find out how to set up and use MyKerio to centralize and unify your Kerio software administration.



The information and content in this document is provided for informational purposes only and is provided "as is" with no warranties of any kind, either express or implied, including without limitation any warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software disclaims and in no event shall be liable for any losses or damages of any kind, including any consequential or incidental damages in connection with the furnishing, performance or use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no warranty, promise or guarantee about the completeness, accuracy, recency or adequacy of information contained in this document and is not responsible for misprints, out-of-date information, or errors. GFI reserves the right to revise or update its products, software or documentation without notice. You must take full responsibility for your use and application of any GFI product or service. No part of this documentation may be reproduced in any form by any means without prior written authorization of GFI Software.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

GFI and MyKerio are trademarks or registered trademarks of GFI Software or its affiliates in the US and other countries. Any other trademarks contained herein are the property of their respective owners.

MyKerio is copyright of Kerio. - 1999-2018 Kerio. All rights reserved.

Document Version: 1.2.0

Last updated (month/day/year): 10/01/2018

Contents

1 Introduction to MyKerio	5
2 Using	6
2.1 Getting Started with MyKerio	6
2.2 Using MyKerio dashboard	8
2.3 Adding Kerio Connect to MyKerio	8
2.3.1 Adding Kerio Connect to MyKerio through Kerio Connect Administration	9
2.4 Adding Kerio Control to MyKerio	10
2.4.1 Adding Kerio Control to MyKerio through Kerio Control Administration	10
2.4.2 Adding Kerio Control to MyKerio during the Kerio Control installation	12
2.5 Adding Kerio Operator to MyKerio	13
2.5.1 Adding Kerio Operator to MyKerio through Kerio Operator Administration	13
2.5.2 Adding Kerio Operator to MyKerio during the Kerio Operator installation	15
2.6 Backups in MyKerio	16
2.6.1 Configuring automatic backups to MyKerio	16
2.6.2 Downloading and importing configuration backups from MyKerio	17
2.7 Installing Kerio Control Hardware Box through MyKerio	18
2.8 Managing appliances in MyKerio	21
2.8.1 Displaying the appliance status	22
2.9 Removing appliances from MyKerio	22
2.9.1 Removing appliances through products' administration interfaces	23
3 Monitoring	25
3.1 MyKerio app for mobile devices	25
3.1.1 Using the MyKerio app on Apple Watch	25
3.1.2 Displaying the appliance status	26
3.2 Receiving email notifications from MyKerio	27
3.2.1 Disabling email notifications	27
3.3 Sending alerts and notifications via MyKerio	28
3.3.1 Configuring MyKerio notification service	28
4 Settings	29
4.1 Adding and managing organizations	29
4.1.1 Adding new organizations to MyKerio	29
4.1.2 Managing organizations in MyKerio	30
4.1.3 Switching between organizations	30
4.1.4 Managing users in organizations	31
4.2 Managing users in organizations	31
4.2.1 Adding users to MyKerio	31
4.2.2 Deleting users from organizations	33
4.2.3 Adding and managing organizations	33
4.3 Sharing definitions across Kerio Control appliances with MyKerio	33
4.4 Configuring 2-step verification in MyKerio	40
4.4.1 Enabling 2-step verification	41
4.4.2 Generating backup codes	42
4.4.3 Verifying your identity with SMS codes	43
4.4.4 Cannot access your authenticator?	44
4.4.5 Disabling 2-step verification	45
4.5 Access auditing	45
4.6 Change or reset your password	46
4.6.1 Changing your password	46
4.6.2 Resetting your password	47

5 Troubleshooting and support	48
5.1 Receiving emails via MyKerio notification service does not work	48

1 Introduction to MyKerio

MyKerio simplifies the management of multiple Kerio Connect, Kerio Control and Kerio Operator deployments through a centralized web interface. It provides consolidated system information, automatic configuration backup, status monitoring, system notifications and complete remote configuration.

With a single sign on capability, MyKerio establishes an encrypted communication channel to your deployments, allowing you to apply and share configuration settings remotely and securely without any prior configuration.

MyKerio is able to send email notifications, or reach you via MyKerio app for Android and iOS devices.

Further reading:

- » [Managing appliances](#)
- » [Managing organizations](#)

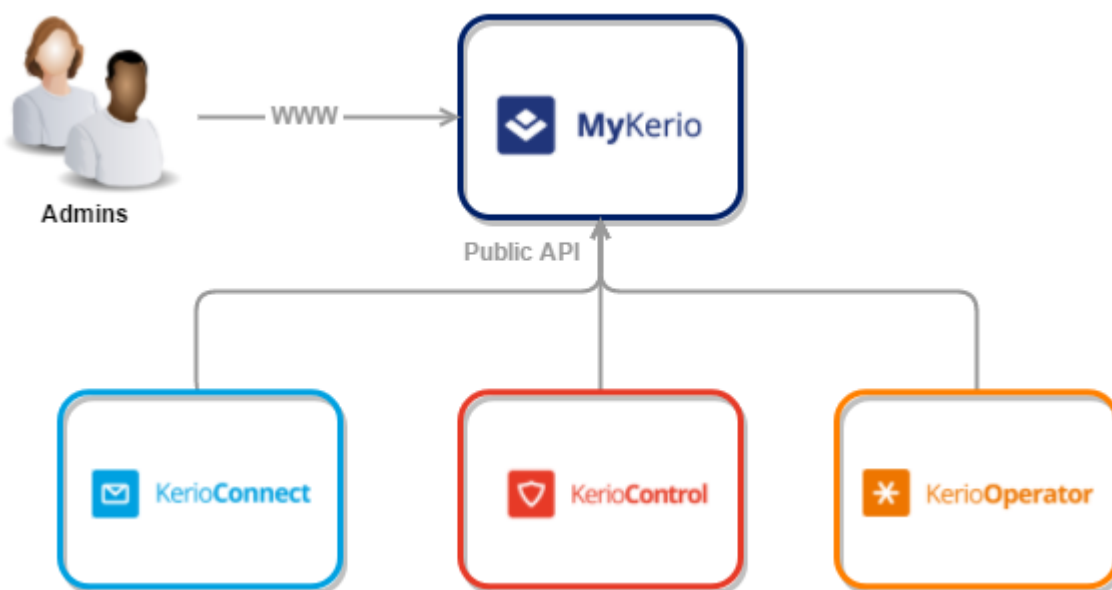
2 Using

This section contains detailed information about following topics:

2.1 Getting Started with MyKerio	6
2.2 Using MyKerio dashboard	8
2.3 Adding Kerio Connect to MyKerio	8
2.4 Adding Kerio Control to MyKerio	10
2.5 Adding Kerio Operator to MyKerio	13
2.6 Backups in MyKerio	16
2.7 Installing Kerio Control Hardware Box through MyKerio	18
2.8 Managing appliances in MyKerio	21
2.9 Removing appliances from MyKerio	22

2.1 Getting Started with MyKerio

MyKerio is a free cloud service that enables you to monitor and manage multiple Kerio appliances from a single dashboard. You can register for a free account at my.kerio.com



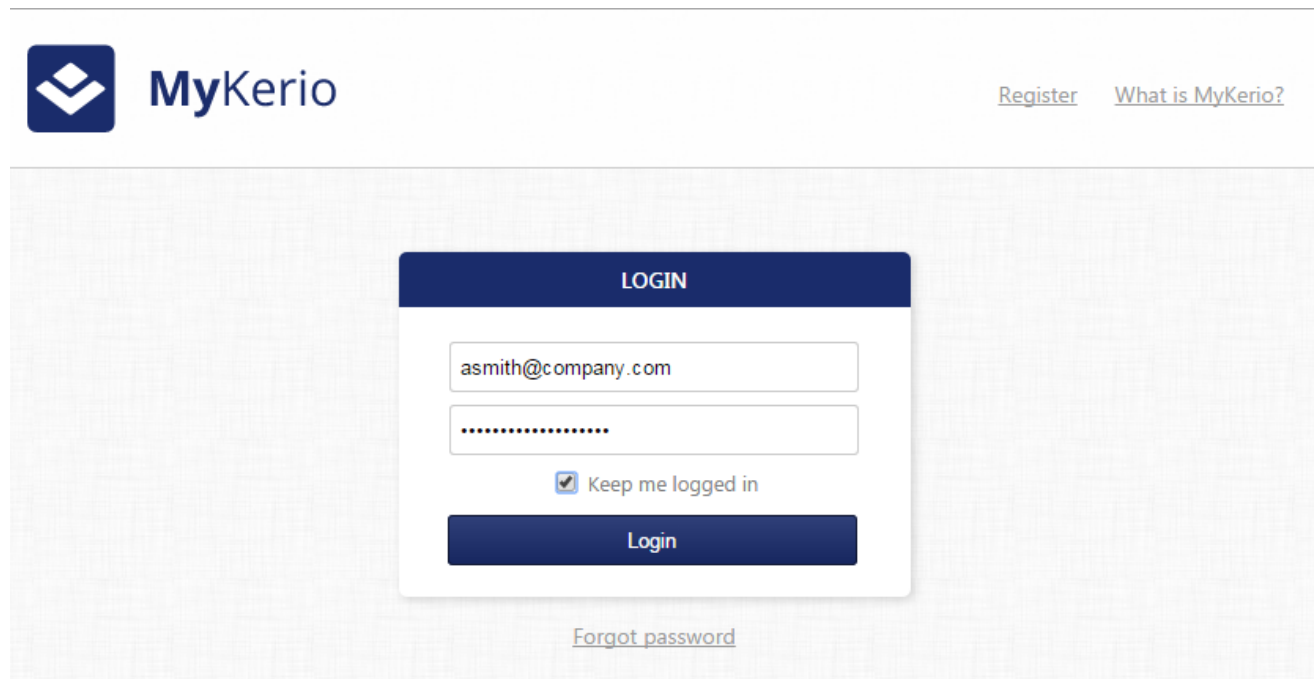
Screenshot 1: Centralized monitoring and management of Kerio appliances

To begin using MyKerio:

1. Go to <https://my.kerio.com/>. If you are not registered yet, click **Register** and go through the registration process.
2. Click **Login**.
3. Type your MyKerio username and password.

4. Optionally, check **Keep me logged in** to avoid getting automatically logged out of MyKerio in case of inactivity.

5. Click **Login**.



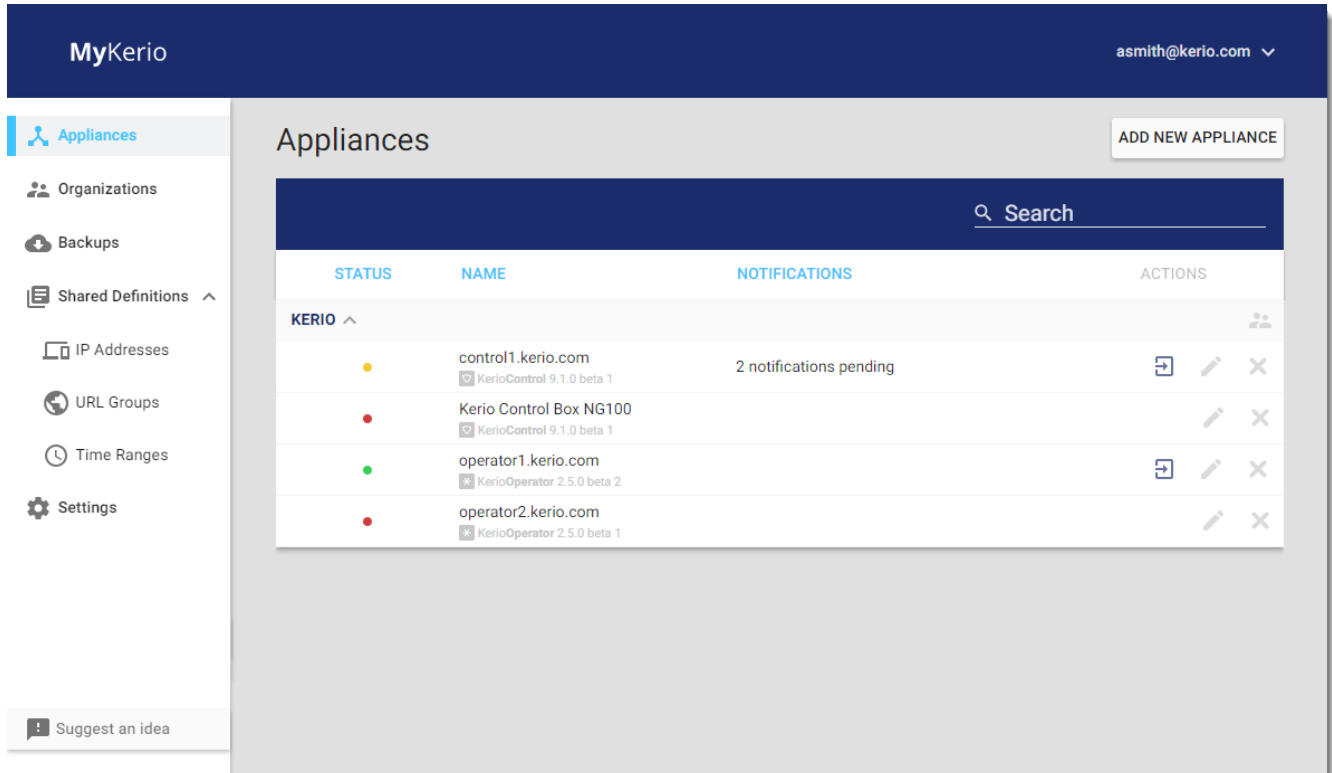
MyKerio supports:

Feature	Description
Remote administration	You can monitor and manage your Kerio products remotely from anywhere. Add Kerio Connect , Kerio Control and, Kerio Operator to MyKerio to start managing and monitoring them.
Unified login	You don't need login credentials for each appliance. You only need to only remember your MyKerio credentials to access your respective appliance's administration.
Secured interaction	MyKerio saves only the product names, versions and IP addresses of the appliances. No credentials from appliances are transferred to or saved in MyKerio. You are also not required to open any service or port on your firewall, because your appliances always establish the connection. MyKerio just forwards commands to your appliances.
Peer administration	You can invite other users as administrators to manage and monitor appliances along with you. For more information, refer to Managing users in organizations (page 31).
Sending notifications	You can set up MyKerio notification service to send alerts and notifications from your appliance. For more information, refer to Sending alerts and notifications via MyKerio (page 28).
2-step verification	You can add an extra layer of security to your account by setting up 2-step verification, which uses an application on your smartphone or computer to confirm your identity. For more information, refer to Configuring 2-step verification in MyKerio (page 40).
Encrypted communication	All communication between your appliances and MyKerio is encrypted.
Activity timeout	MyKerio offers an administration shell that has an inactivity session invalidation in effect, which means that if no activity happens in the browser window for 15 minutes, then the user gets logged out of MyKerio automatically. This feature is only active when a user logs into MyKerio with Keep me logged in option as disabled.

2.2 Using MyKerio dashboard

The MyKerio dashboard displays all the appliances within each organization you have access to.

Before you start, decide on how many organizations and administrators you need for each appliance. See [Adding and managing organizations](#) and [Managing users in organizations](#) for more details.




The screenshot shows the MyKerio dashboard interface. On the left is a sidebar with navigation links: Appliances (selected), Organizations, Backups, Shared Definitions, IP Addresses, URL Groups, Time Ranges, and Settings. At the bottom of the sidebar is a 'Suggest an idea' button. The main content area is titled 'Appliances' and includes an 'ADD NEW APPLIANCE' button in the top right. Below the title is a search bar. A table lists appliances with columns for STATUS, NAME, NOTIFICATIONS, and ACTIONS. The table is filtered by 'KERIO'. The appliances listed are: control1.kerio.com (yellow status dot, 2 notifications pending), Kerio Control Box NG100 (red status dot), operator1.kerio.com (green status dot), and operator2.kerio.com (red status dot). Each row has icons for opening the administration interface, editing, and deleting.


STATUS	NAME	NOTIFICATIONS	ACTIONS
KERIO ^			
●	control1.kerio.com KerioControl 9.1.0 beta 1	2 notifications pending	[Open] [Edit] [Delete]
●	Kerio Control Box NG100 KerioControl 9.1.0 beta 1		[Edit] [Delete]
●	operator1.kerio.com KerioOperator 2.5.0 beta 2		[Open] [Edit] [Delete]
●	operator2.kerio.com KerioOperator 2.5.0 beta 1		[Edit] [Delete]

» The first column in each row displays the status of each appliance. See [Displaying Appliance Status](#) for more information.

» To open the administration interface for the appliance, click .

» If an appliance is not connected, the **Open administration** button disappears.

» To rename an appliance, click  in the appliance's row in the dashboard and type the new name.

» To remove a appliance from the **MyKerio** dashboard, click  in the appliance's row. The removed appliance is still running, but it is no longer connected to MyKerio.

2.3 Adding Kerio Connect to MyKerio

MyKerio is a cloud service that enables you to administer multiple instances of Kerio Connect appliances through a centralized web interface. This topic describes a process for adding Kerio Connect to MyKerio. There are two ways how to accomplish it:

- » [Adding Kerio Connect to MyKerio through Kerio Connect Administration](#)
- » [Adding Kerio Connect to MyKerio through the initial configuration](#)

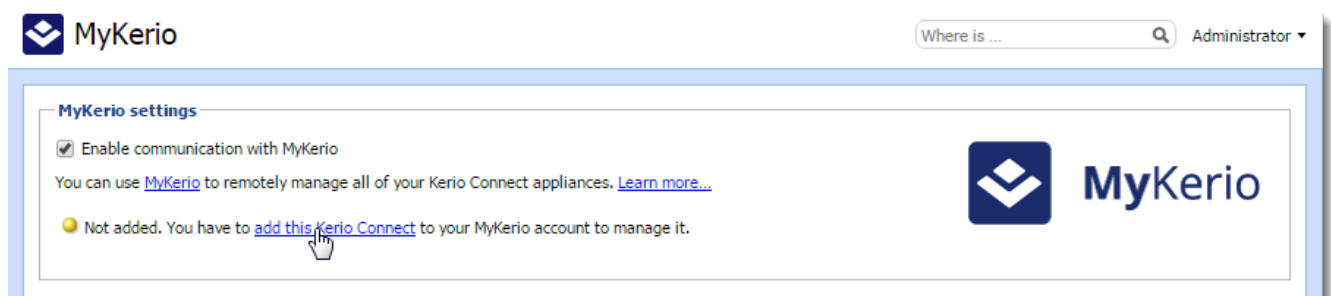
NOTE

You can add only on-prem Kerio Connect appliances to MyKerio. Kerio Connect Multi-Server is not supported.

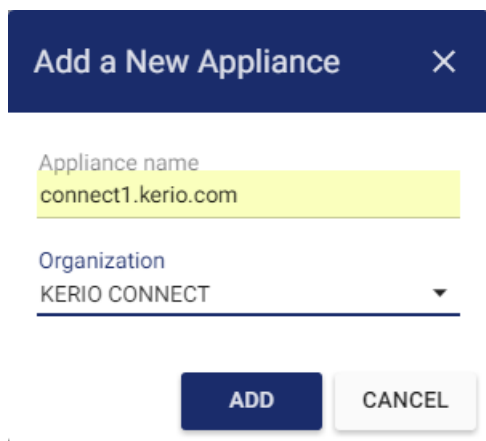
2.3.1 Adding Kerio Connect to MyKerio through Kerio Connect Administration

To link Kerio Connect to MyKerio you must enable access to MyKerio in Kerio Connect and sign up for MyKerio.

1. In the Kerio Connect administration interface, go to **Configuration > MyKerio**.
2. Select **Enable communication with MyKerio**.
3. Click **Apply**.
4. Click the link **add this Kerio Connect**.

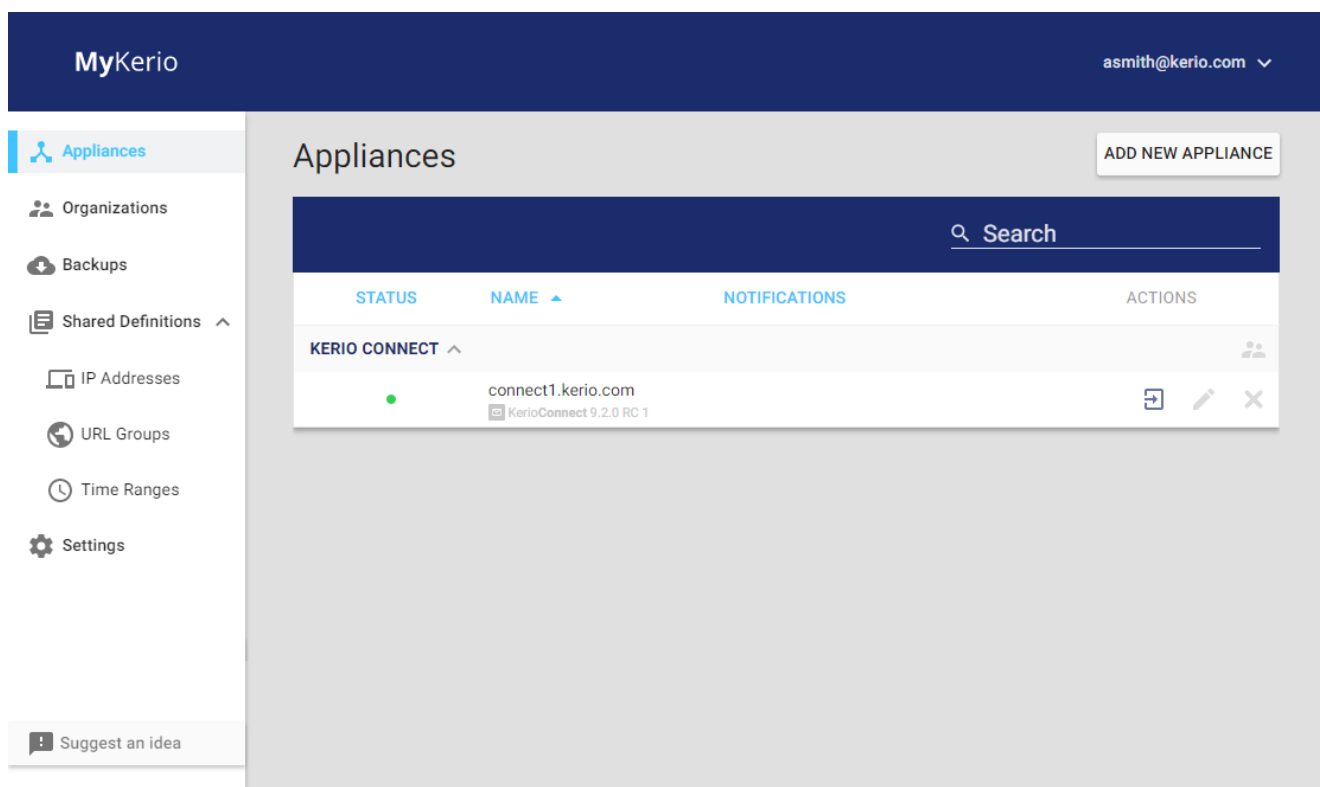


5. Your web browser opens <https://my.kerio.com/login>, where you can register or log in if you are already registered. After successful login, MyKerio displays the **Add a New Appliance** dialog box.
6. Type the name of the Kerio Connect appliance (for example, your company name). If you have more organizations created in MyKerio, select also the organization. For more information, refer to [Managing users in organizations](#) (page 31).



7. Click **Add**.

You are now connected to MyKerio and you can see the Kerio Connect appliance in the MyKerio dashboard.



2.4 Adding Kerio Control to MyKerio

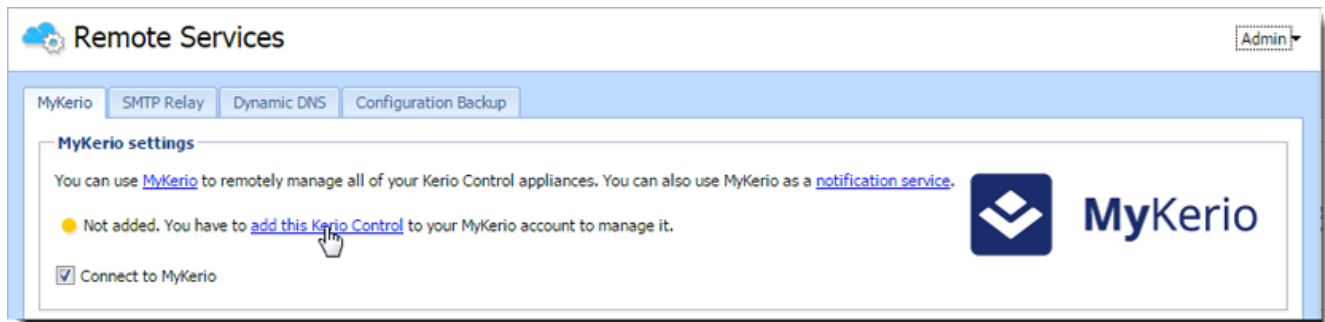
MyKerio is a cloud service that enables you to administer multiple instances of Kerio Control appliances through a centralized web interface. This topic describes a process for adding Kerio Control to MyKerio. There are two ways how to accomplish it:

- » [Adding Kerio Control to MyKerio through Kerio Control Administration](#)
- » [Adding Kerio Control to MyKerio during the Kerio Control installation](#)

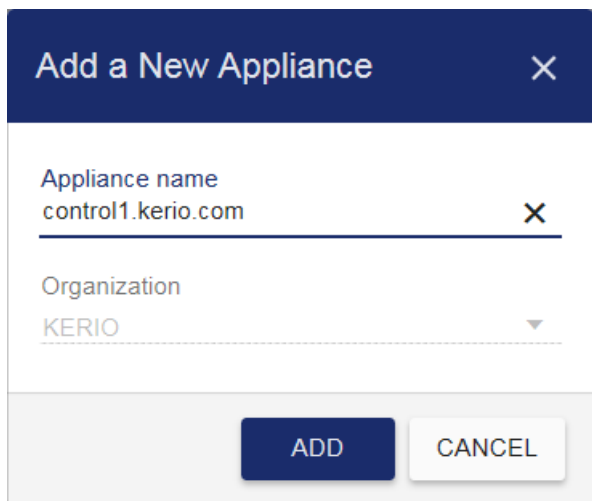
2.4.1 Adding Kerio Control to MyKerio through Kerio Control Administration

To link Kerio Control to MyKerio you must enable access to MyKerio in Kerio Control and sign up for MyKerio.

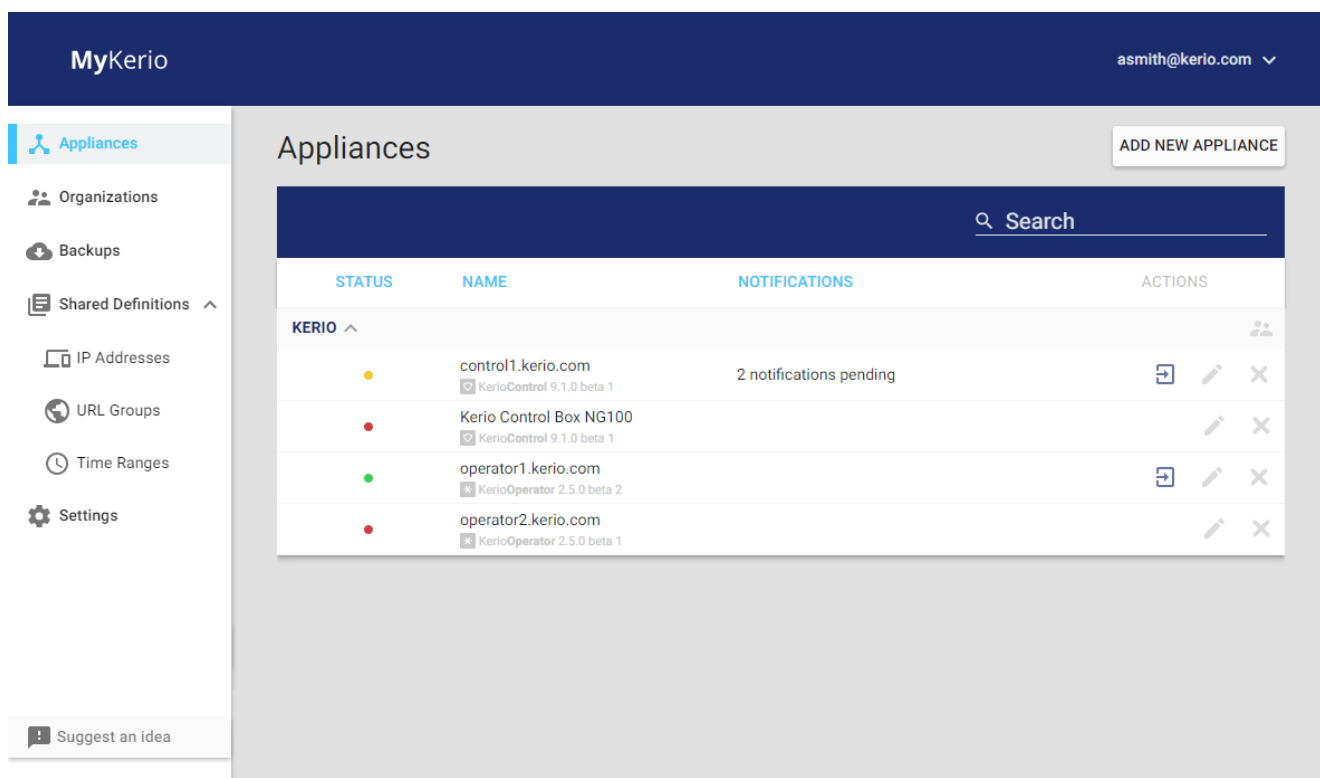
1. In the Kerio Control administration interface, go to **Remote Services**.



2. Ensure that **Connect to MyKerio** is checked.
3. Click the link **add this Kerio Control**. Your web browser opens <https://my.kerio.com/>, where you can register or log in if you are already registered.
4. After successful login, MyKerio displays the **Add a New Appliance** dialog box.
5. Type the name of the Kerio Control appliance (for example, your company name). If you have more organizations created in MyKerio, select also the organization. For more information, refer to [Adding and managing organizations](#) (page 29).



6. Click **Add**.
- You are now connected to MyKerio and you can see the Kerio Control appliance in the MyKerio dashboard.

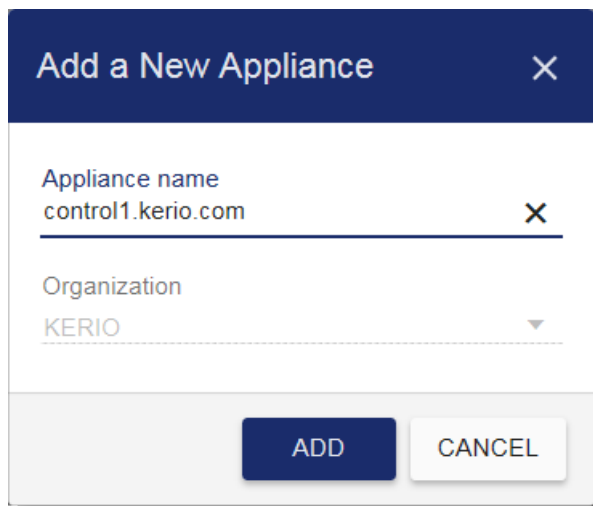


2.4.2 Adding Kerio Control to MyKerio during the Kerio Control installation

When you install a new Kerio Control appliance, you can add it to MyKerio during the installation process. In the last installation dialog in the Kerio Control console, you can find a link to MyKerio (see figure below):



1. Type the link to your browser. Your web browser opens <https://my.kerio.com/login>, where you can register or log in if you are already registered. MyKerio with the **Add a New Appliance** dialog box opens.



2. Type the name of the newly installed appliance.

3. Click **Add**.

The MyKerio dashboard appears, the appliance is displayed and its status is **Up** (status bullet is green).

If you miss the correct link during the installation, you can [add](#) Kerio Control to MyKerio later in the Kerio Control Administration.

2.5 Adding Kerio Operator to MyKerio

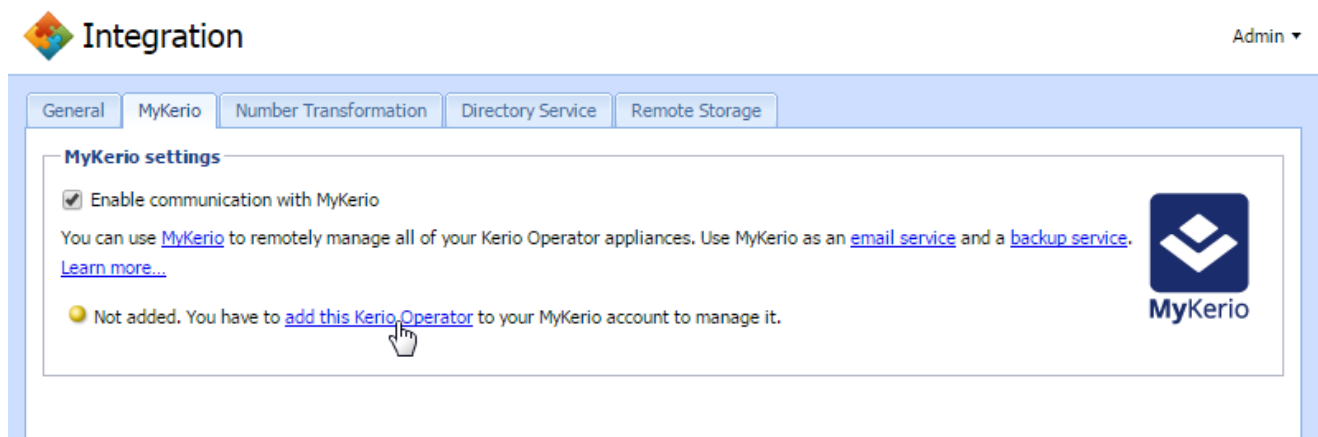
MyKerio is a cloud service that enables you to administer multiple instances of Kerio Operator appliances through a centralized web interface. This topic describes a process for adding Kerio Operator to MyKerio. There are two ways how to accomplish it:

- » [Adding Kerio Operator to MyKerio through Kerio Operator Administration](#)
- » [Adding Kerio Operator to MyKerio during the Kerio Operator installation](#)

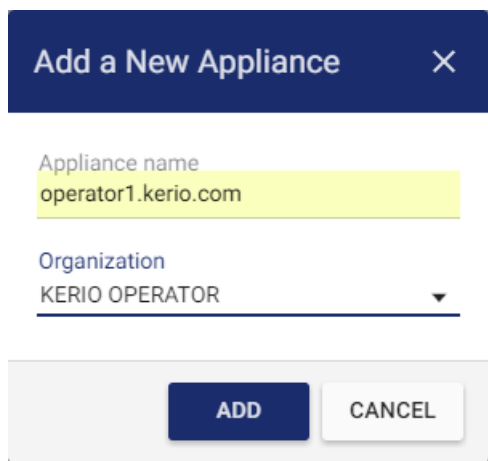
2.5.1 Adding Kerio Operator to MyKerio through Kerio Operator Administration

To link Kerio Operator to MyKerio you must enable access to MyKerio in Kerio Operator and sign up for MyKerio.

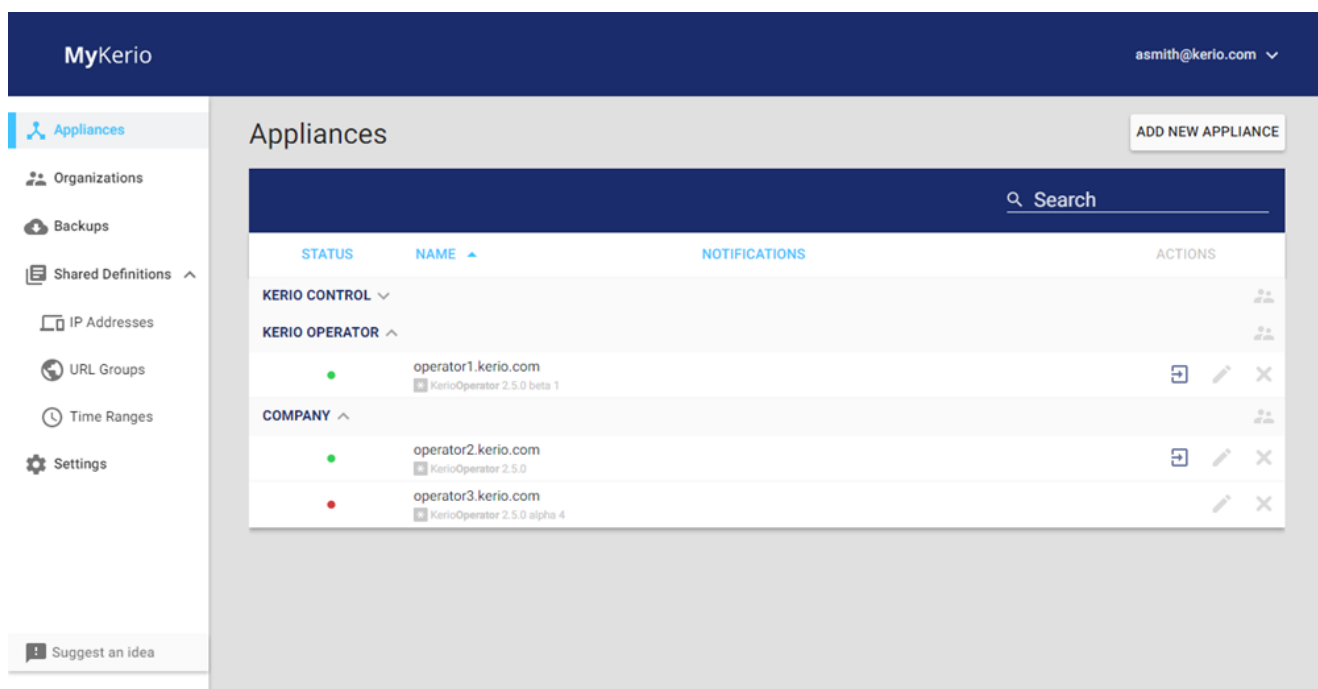
1. In the Kerio Operator administration interface, go to **Integration > MyKerio** .



2. Check **Enable communication with MyKerio**.
3. Click the link **add this Kerio Operator**. Your web browser opens <https://my.kerio.com/login>, where you can register or log in if you are already registered.
4. After successful login, MyKerio displays the **Add a New Appliance** dialog box.
5. Type the name of the Kerio Operator appliance (for example, your company name). If you have more organizations created in MyKerio, select also the organization. For more information, refer to [Managing users in organizations](#) (page 31).



6. Click **Add**.
- You are now connected to MyKerio and you can see the Kerio Operator appliance in the MyKerio dashboard.

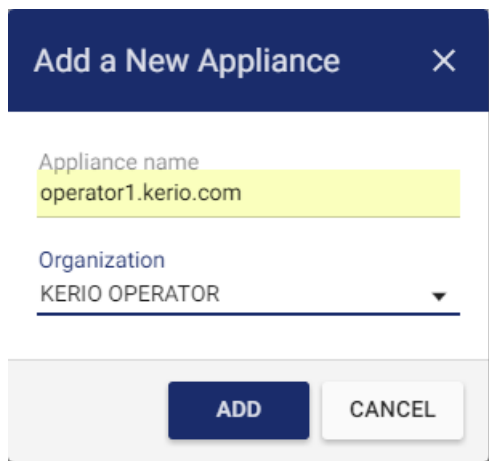


2.5.2 Adding Kerio Operator to MyKerio during the Kerio Operator installation

When you install a new Kerio Operator appliance, you can add it to MyKerio during the installation process. In the last installation dialog in the Kerio Operator console, you can find a link to MyKerio (see figure below):



1. Type the link to your browser. Your web browser opens <https://my.kerio.com/>, where you can register or log in if you are already registered. MyKerio with the **Add a New Appliance** dialog box opens.



2. Type the name of the newly installed appliance.

3. Click **Add**.

The MyKerio dashboard appears, the appliance is displayed and its status is **Up** (status bullet is green).

If you miss the correct link during the installation, you can [add](#) Kerio Operator to MyKerio later in the Kerio Operator Administration.

2.6 Backups in MyKerio

Your appliances can automatically back up and upload your configuration files to [MyKerio](#). MyKerio stores up to five backup files per appliance.

NOTE

When restoring the configuration to Kerio Control or Kerio Operator, if the hardware is different unselect the restoration of Network Interface settings. Although the new hardware has the same interfaces, their identifiers are different.

MyKerio also stores configuration backups of disconnected or removed appliances.

2.6.1 Configuring automatic backups to MyKerio

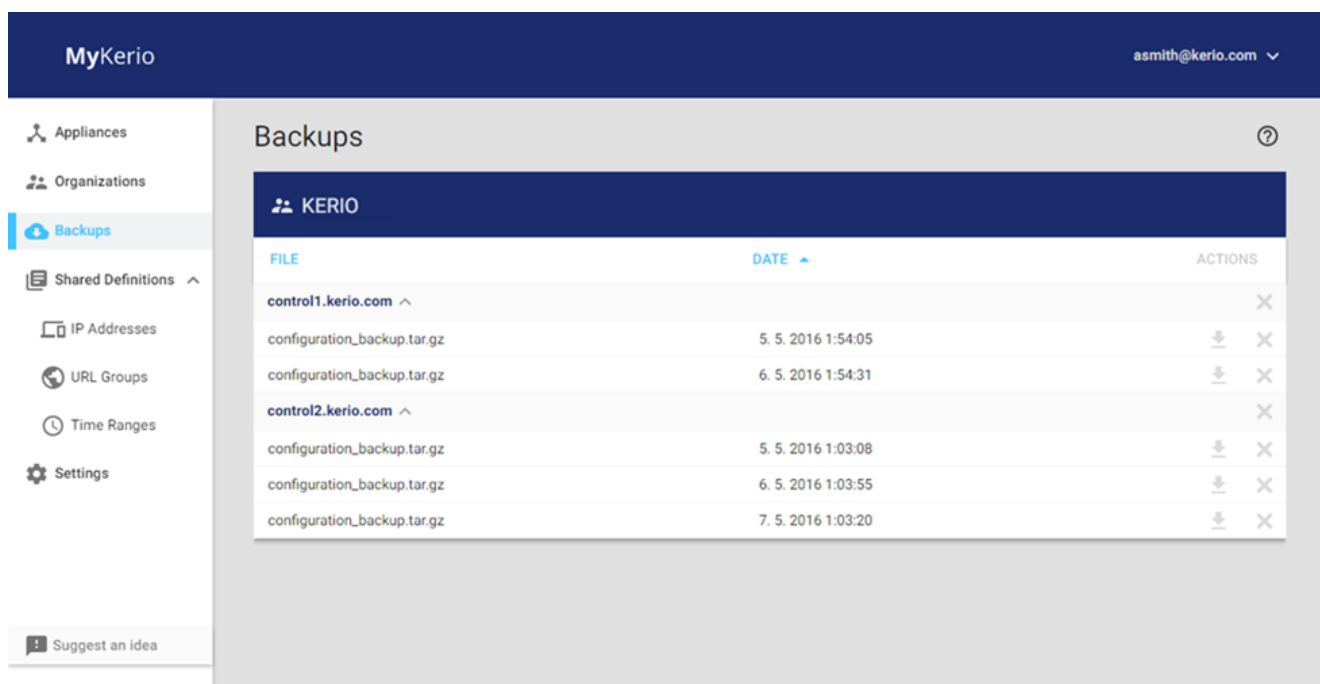
To back up your configuration files:

1. Add your appliance to MyKerio.

- To add Kerio Control, see [Adding Kerio Control to MyKerio](#).
- To add Kerio Operator, see [Adding Kerio Operator to MyKerio](#).


2. Configure your appliance to automatically back up your files to MyKerio.

- To configure Kerio Control, see [Saving configuration to MyKerio](#).
- To configure Kerio Operator, see [Saving Kerio Operator configuration to MyKerio](#).



2.6.2 Downloading and importing configuration backups from MyKerio

To download your configuration files from MyKerio:

1. In MyKerio, go to the **Backups** section.
2. Find the configuration backup you want to download.
3. Click .

Importing configuration backups to Kerio Control

NOTE

For more information about importing the configuration in Kerio Control, see the [Import configuration](#) section in the **Configuration Assistant** topic.

To import your Kerio Control backups:

1. In the administration interface, go to **Configuration > Remote Services > Configuration Backup**.
2. In the **Backup** section, click **Import configuration**.
3. To select the configuration file, click **Upload Configuration File**.
4. Select a method for the import and click **Next**.
5. Click **Finish**.

Kerio Control restarts and applies your configuration files.

Importing configuration backups to Kerio Operator

To import your Kerio Operator backups:

1. In the administration interface, go to **Configuration > Advanced Options > Backup and Recovery**.
2. In the **Recovery** section, click **Upload Backup File**.
3. Select a file you want to import.
4. Select items you want to recover.
5. Click **Recover**.

Kerio Operator restarts and applies your configuration files.

2.7 Installing Kerio Control Hardware Box through MyKerio

This topic describes how to add Kerio Control Hardware Box to MyKerio and complete the registration process and basic configuration of the box.

The advantage of this process is that a technician can perform the installation remotely. A non-technical assistant located on-site can switch-on and connect the Hardware Box to the network, and the technician can then add the Hardware Box to MyKerio and manage it.

If you have the software or virtual appliance version of Kerio Control, you can add the appliance from the web administration interface. For more information, refer to [Adding Kerio Control to MyKerio](#) (page 10).

Prerequisites

To add Kerio Control Hardware Box to MyKerio, you need:

- » the serial number on the bottom of your Kerio Control Hardware Box or from Kerio Online Store. A serial number is a 12-digit number, for example `SRLNMR123456`. For more information, refer to [Installing Kerio Control Hardware Box through MyKerio](#) (page 18).
- » your Kerio Control Hardware Box connected to the internet.
- » the local administrator's login credentials if your appliance is already set up locally.

Adding Kerio Control Hardware Box to MyKerio

NOTE

Verify that the Hardware Box can reach MyKerio. If the Internet provider does not provide a DHCP server, the Kerio Control Hardware Box cannot obtain its IP address, so you must configure it manually. For more information, see [Configuring network interfaces](#).

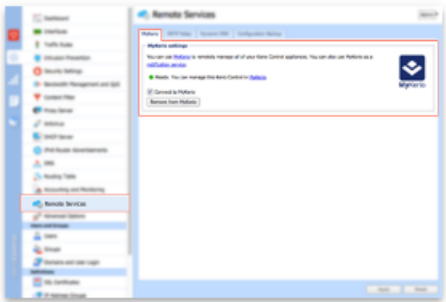
Add a New Appliance

1. **Log in** to MyKerio.
2. In the **Appliances** section, click **Add new appliance**.
3. In the **Add a New Appliance** dialog box, key-in the serial number of the appliance.
4. Click **Find this appliance**.

Add a New Appliance

All Kerio Control appliances

To add your appliance, go to your Kerio Control Administration to Remote Services.



Kerio Control Box

You can add any hardware appliance by providing license and serial number.

OR

FIND THIS APPLIANCE

CLOSE

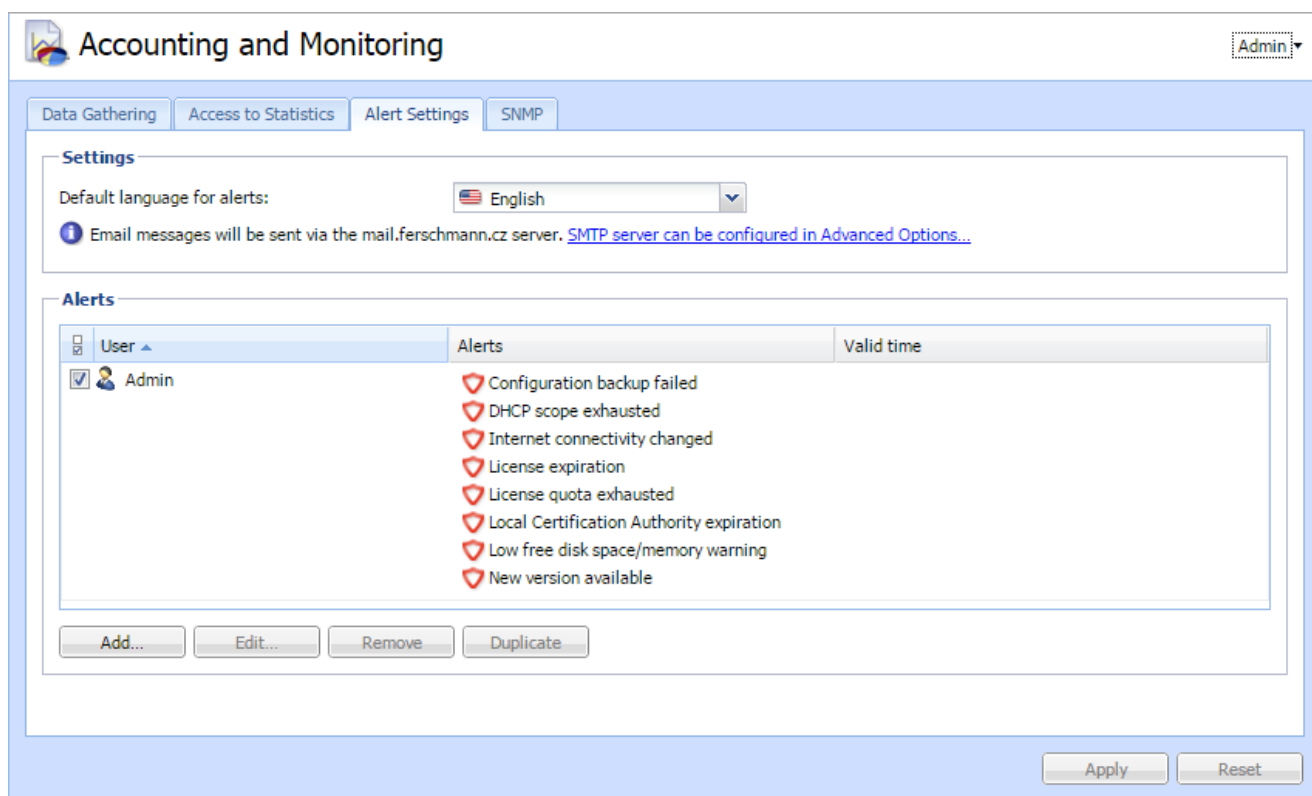
Set up the Appliance

If your appliance is already set up locally:

1. In the **Set up the Appliance** dialog box, verify the Kerio Control Hardware Box type and IP address, and key-in your local administrator's login credentials.
2. Read and confirm **Privacy Policy Terms and with End User License Agreement**.
3. Click **Next**.

If your appliance has not been set up locally:

1. In the **Set up the Appliance** dialog box, verify the Kerio Control Hardware Box type and IP address, and configure your local administrator's login credentials.
2. In the **Administrator email** field, key-in the administrator's email address. This can be changed later, if required.



3. Optionally, select **Allow Kerio Control to send anonymous usage statistics to Kerio Technologies**. This information helps us to understand how organizations use our products so that we can decide how to best improve them. Statistics do not include any confidential data (passwords, email addresses, etc.), and you can disable this option at any time under **Advanced Options > Updates**.

4. Click **Next**.

5. Key-in your local administrator's login credentials for verification.

6. Read and confirm **Privacy Policy Terms and with End User License Agreement**.

7. Click **Next**.

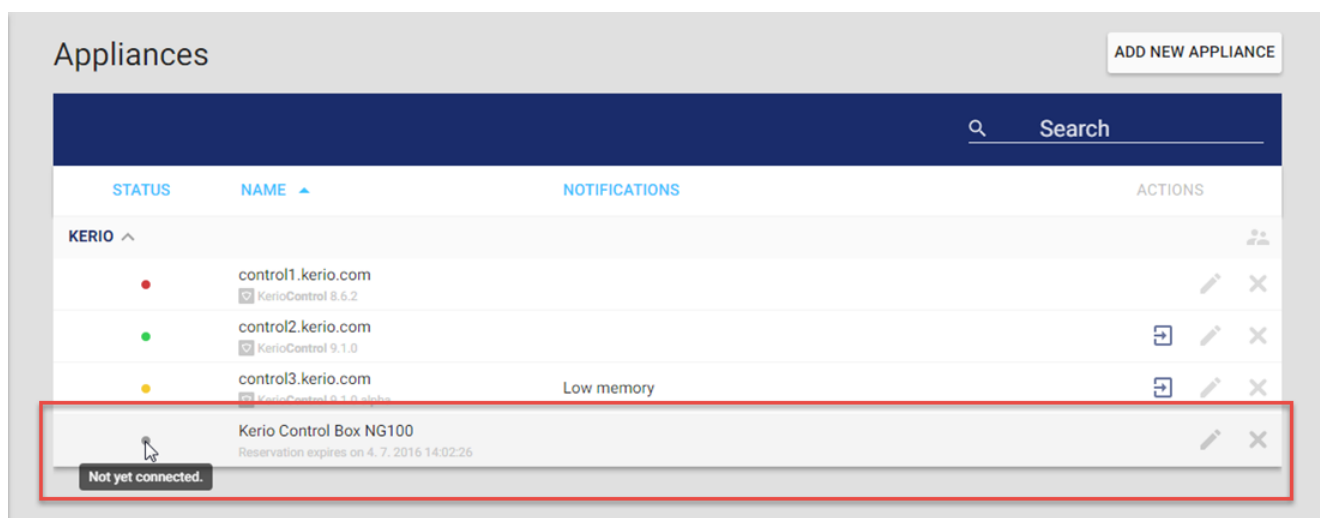
Add the Appliance to MyKerio

1. In the **Add the Appliance to MyKerio** dialog box, key-in a name for the appliance.

2. If you have more than one organization, use the **Organization** drop-down list to assign the appliance correctly.

3. Click **Finish**.

After you successfully connect the appliance you can see it in the **Appliances** section. Wait one or two minutes until the appliance is shown as **Up** (green).



2.8 Managing appliances in MyKerio

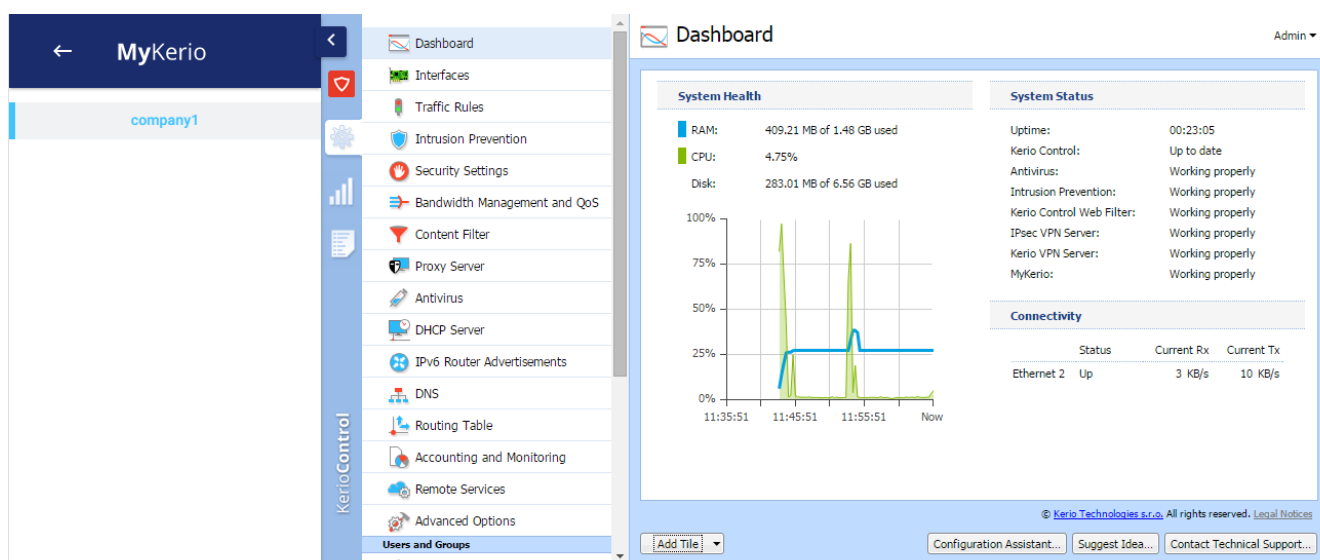
Learn how to manage appliances in MyKerio.

1. Log in to MyKerio.
2. Go to **Appliances**.
3. To open the administration interface for the appliance, click .

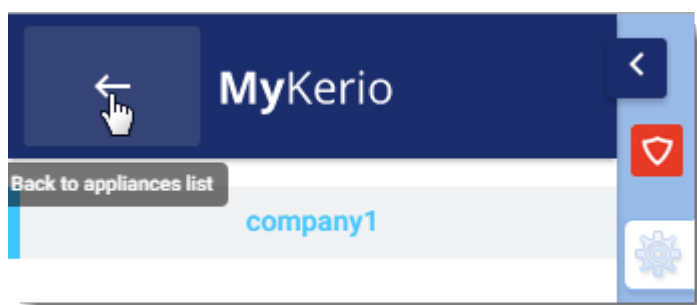
The appliance opens and you can administer your appliances as usual.

NOTE

You cannot access Kerio Control Statistics from Kerio Control Administration when it is opened in MyKerio.



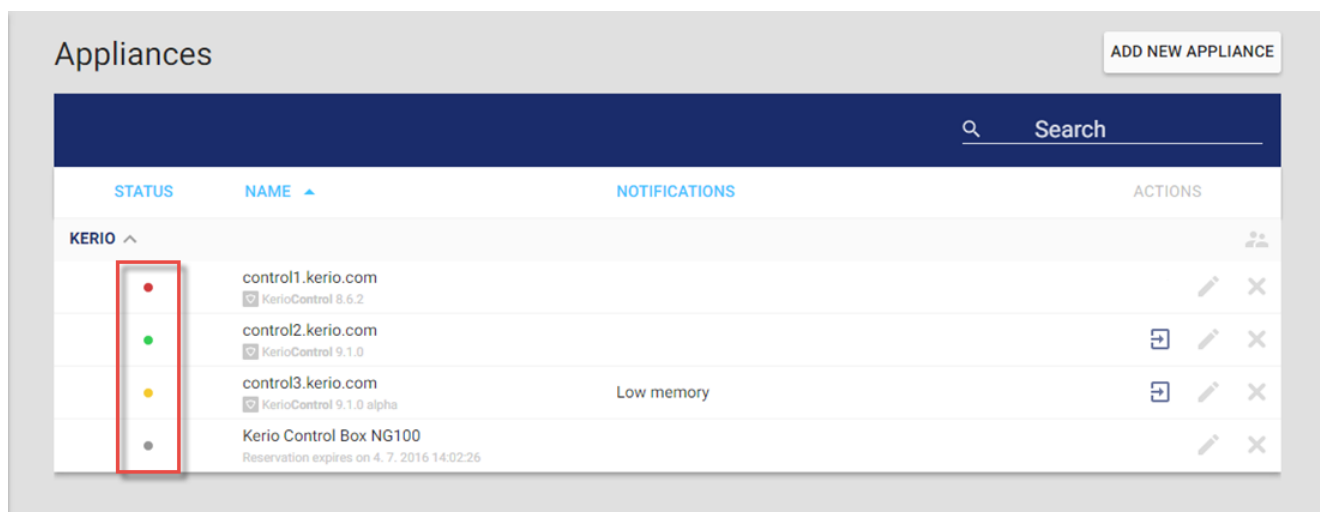
To exit the appliance interface, click the return arrow.



2.8.1 Displaying the appliance status

When you add your appliances to MyKerio, you can see their status in the **Appliances** section. MyKerio indicates the status with three colors:


- » Green – The appliance is online.
- » Yellow – The appliance is online but with some minor issues, for example, low memory or an update is available.
- » Red – the appliance is offline or with some major issues, for example, the license or the software maintenance has expired.
- » Grey – the appliance is reserved for an organization.



2.9 Removing appliances from MyKerio

You can remove your appliances from MyKerio directly or in the administration interface of Kerio Connect, Kerio Control, or Kerio Operator.

To remove appliances from MyKerio

1. In MyKerio, go to **Appliances**.
2. Select an appliance.
3. Click .
4. Click **Remove**.

2.9.1 Removing appliances through products' administration interfaces

1. In Kerio Connect, go to **MyKerio**.
 - a. In Kerio Control, go to **Remote Services > MyKerio**.
 - b. In Kerio Operator, go to **Integration > MyKerio**.
2. Click **Remove from MyKerio**.
3. Click **Yes** to confirm.

MyKerio settings

☒ Enable communication with MyKerio

You can use [MyKerio](#) to remotely manage all of your Kerio Connect appliances. [Learn more...](#)

● Ready. You can manage this Kerio Connect in [MyKerio](#).

[Remove from MyKerio](#)


Apply

Reset



Remote Services

Admin ▾

MyKerio

SMTP Relay

Dynamic DNS

Configuration Backup

MyKerio settings

You can use [MyKerio](#) to remotely manage all of your Kerio Control appliances. You can also use MyKerio as a [notification service](#) and as a [backup service](#).

Concerned about security? [Learn more...](#)

● Ready. You can manage this Kerio Control in [MyKerio](#).

☒ Connect to MyKerio

[Remove from MyKerio](#)


Apply

Reset



Integration

Admin ▾

General

MyKerio

Number Transformation

Directory Service

Remote Storage

MyKerio settings

You can use [MyKerio](#) to remotely manage all of your Kerio Operator appliances. Use MyKerio as an [email service](#) and a [backup service](#).

Concerned about security? [Learn more...](#)

● Ready. You can manage this Kerio Operator in [MyKerio](#).

☒ Connect to MyKerio

[Remove from MyKerio](#)


Apply

Reset

3 Monitoring

This section provides detailed information about receiving and sending email notifications and alerts, and information about MyKerio app for mobile devices.

3.1 MyKerio app for mobile devices	25
3.2 Receiving email notifications from MyKerio	27
3.3 Sending alerts and notifications via MyKerio	28

3.1 MyKerio app for mobile devices

The MyKerio app monitors the appliances you have in MyKerio and notifies you of any status changes. You can:

- » Check the status of your appliances at any time.
- » Receive notifications if the status of any of your appliances changes.
- » View system errors or other critical events related to your appliances.

Download the MyKerio app from:

- » [Android Play Store](#)
- » [Apple AppStore](#)

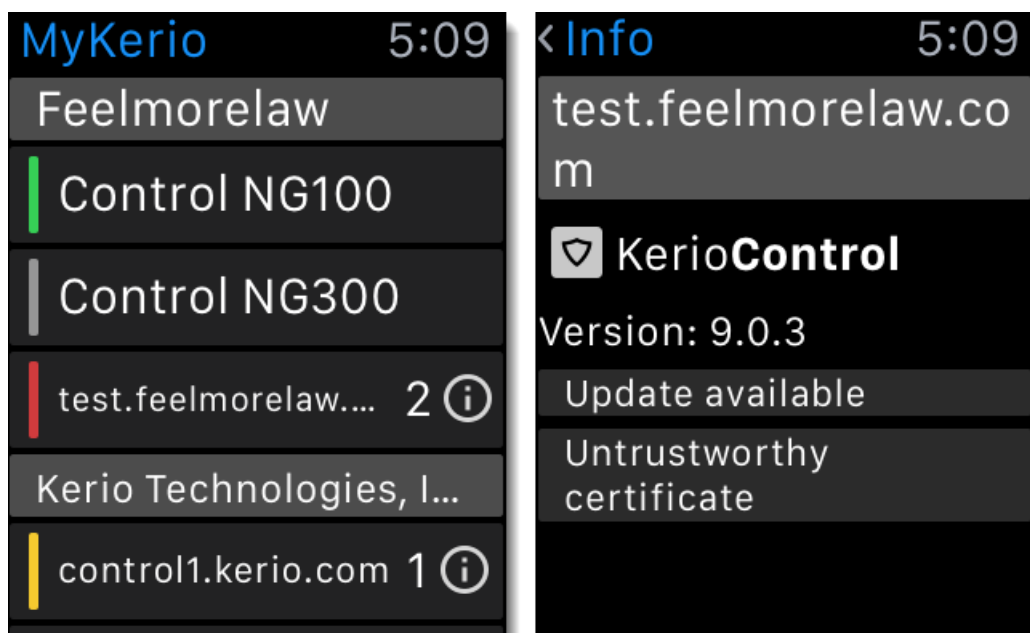
MyKerio sends following notifications:

- » Update available
- » Low memory
- » Problem with mapped domain
- » Expiration of maintenance subscription or licence
- » Backup line active
- » Expiration of certificates

3.1.1 Using the MyKerio app on Apple Watch

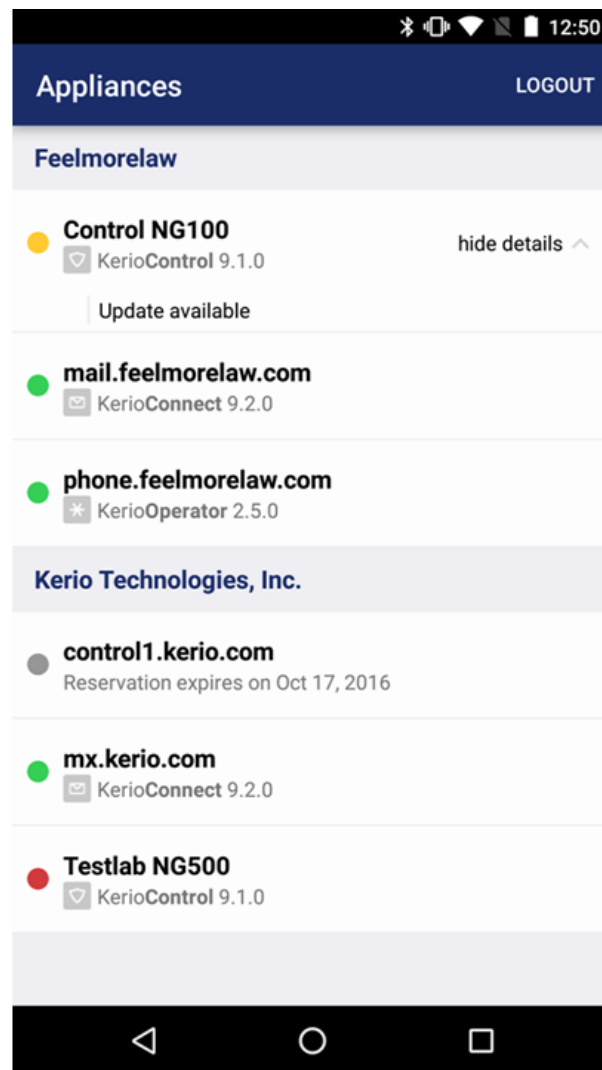
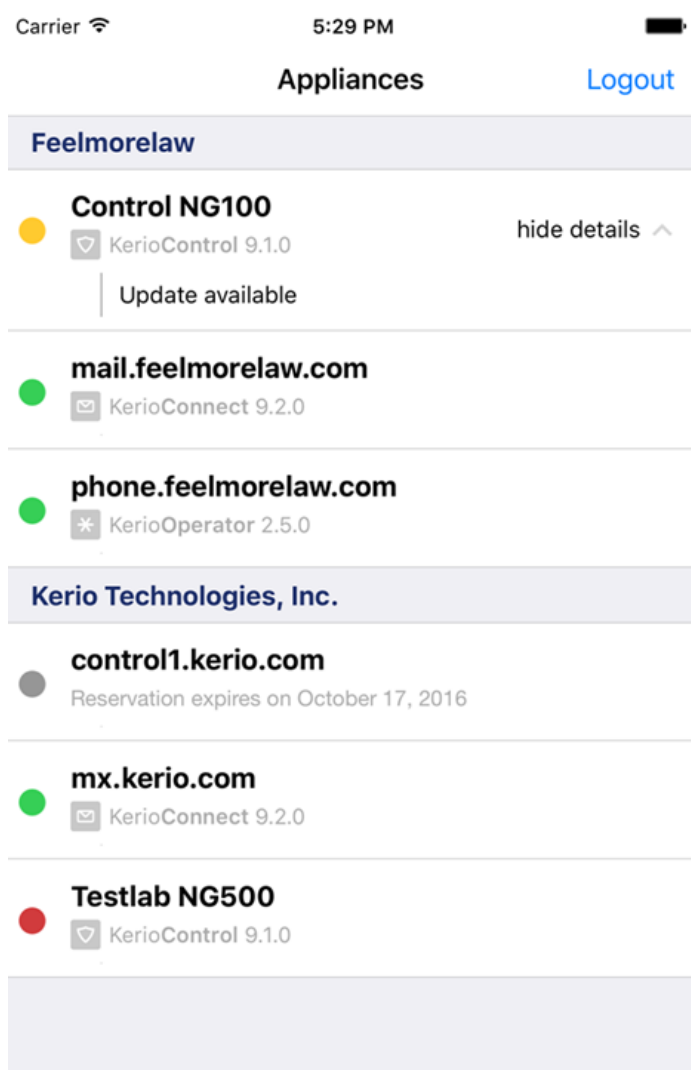
To use the MyKerio app on Apple Watch, you must:

1. Pair your iPhone with Apple Watch
2. Download and install the MyKerio app
3. Display the app on Apple Watch. On your iPhone, open the **Watch** app > **MyKerio**, and enable the **Show App on Apple Watch** option.
4. Log into the app on your iPhone



3.1.2 Displaying the appliance status

For more information, refer to [Displaying the appliance status](#) (page 22).



3.2 Receiving email notifications from MyKerio

By default, MyKerio sends email notifications, for example, when:

- » An appliance in MyKerio goes online or offline. MyKerio notifies all users in the organization.
- » MyKerio needs a confirmation of your email address.
- » You are invited to an organization.
- » You are removed from an organization.
- » You reset your password in MyKerio.

3.2.1 Disabling email notifications

To disable email notifications from MyKerio:

1. Log into MyKerio.
2. Go to **Settings**.
3. In the **User preferences** dialog box, deselect the **Receive email notifications from MyKerio** option.

Disabling the option does not affect emails about resetting passwords, inviting users to organizations, and with confirmations of users' email addresses.

For more information, refer to [Sending alerts and notifications via MyKerio](#) (page 28).

3.3 Sending alerts and notifications via MyKerio

NOTE

For more information, refer to [Receiving email notifications from MyKerio](#) (page 27).

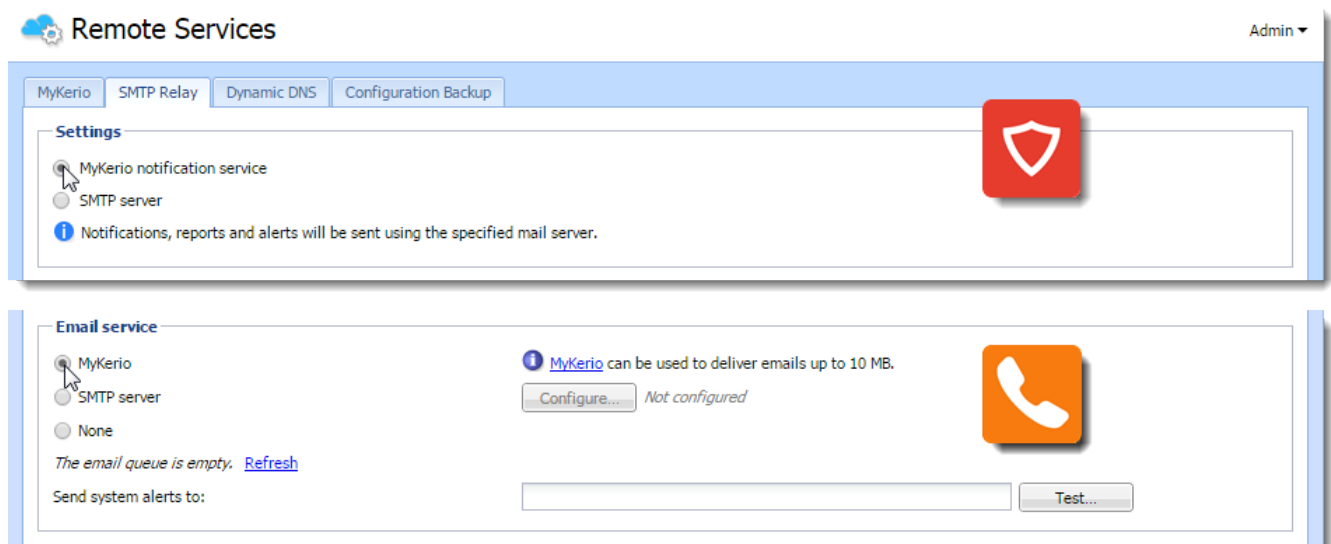
MyKerio notification service can send alerts and notifications from your appliance without any need to configure the SMTP relay.

You can use the MyKerio notification service without creating account in MyKerio.

The amount of emails this service can send is limited per 24 hours. If you expect a large amount of emails from MyKerio notification service, use the SMTP server instead.

3.3.1 Configuring MyKerio notification service

1. In the administration interface, go to:
 - a. **Remote Services > SMTP Relay > Settings** in Kerio Control.
 - b. **Advanced Options > General > Email service** in Kerio Operator.



2. Select:
 - a. **MyKerio notification service** in Kerio Control.
 - b. **MyKerio** in Kerio Operator.
3. Click **Apply**.
4. Click **Test**.
5. In the **Email Address** dialog box, type your email address to test the connection and click OK. You should receive a test message in your inbox.

4 Settings

This section contains detailed information about the following topics:

4.1 Adding and managing organizations	29
4.2 Managing users in organizations	31
4.3 Sharing definitions across Kerio Control appliances with MyKerio	33
4.4 Configuring 2-step verification in MyKerio	40
4.5 Access auditing	45
4.6 Change or reset your password	46

4.1 Adding and managing organizations

You can organize your appliances into MyKerio Organizations so that it's easy to see which appliances belong to different companies, sites, campuses, and so on.

NOTE

An appliance can only be added to one organization.

By default, there is one organization in your MyKerio account named after the domain of your email address. After logging into MyKerio, you can create and manage your organizations.

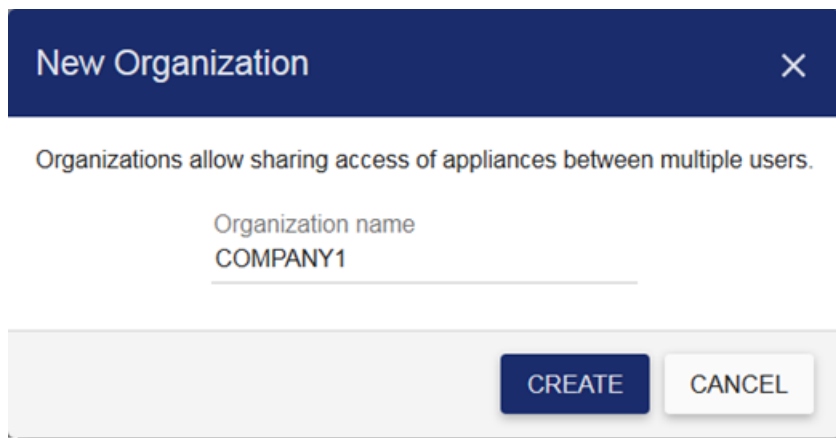
4.1.1 Adding new organizations to MyKerio

When you first register with MyKerio, you have only one organization created for you.

To add a new organization:

1. Go to **Organizations** in MyKerio.
2. In the **Organization** screen, click the **New Organization** button.
3. In the **New organization** dialog box, type a name for your new organization.
4. Click **Create**.

MyKerio creates the new organization.






New Organization

Organizations allow sharing access of appliances between multiple users.

Organization name
COMPANY1

CREATE CANCEL

4.1.2 Managing organizations in MyKerio

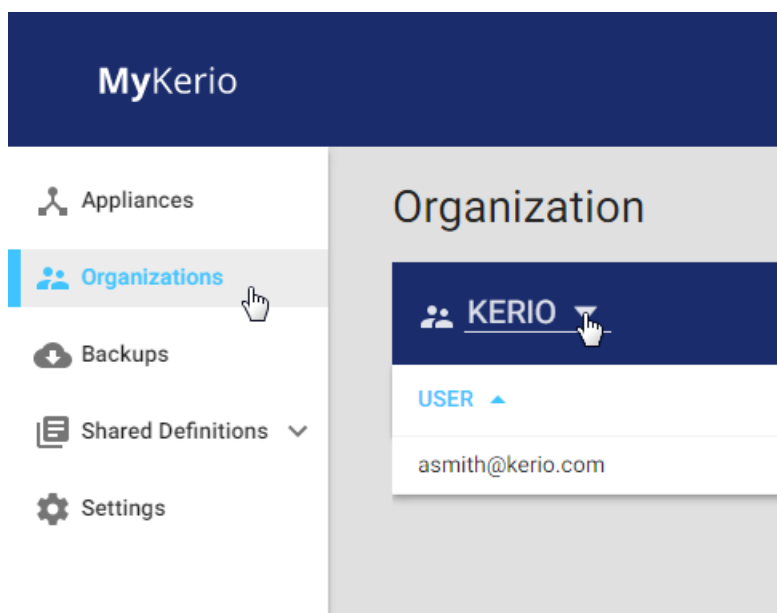
- » Click  to leave the displayed organization.
- » Click  to rename the displayed organization.
- » Click  to delete the displayed organization.

IMPORTANT

MyKerio deletes the organization even if the organization contains other users and appliances.

4.1.3 Switching between organizations

1. In MyKerio, go to **Organizations**.
2. Click the name of the organization.
3. In the drop-down menu, select the organization you want to display.



4.1.4 Managing users in organizations

For more information, refer to [Managing users in organizations](#) (page 31).

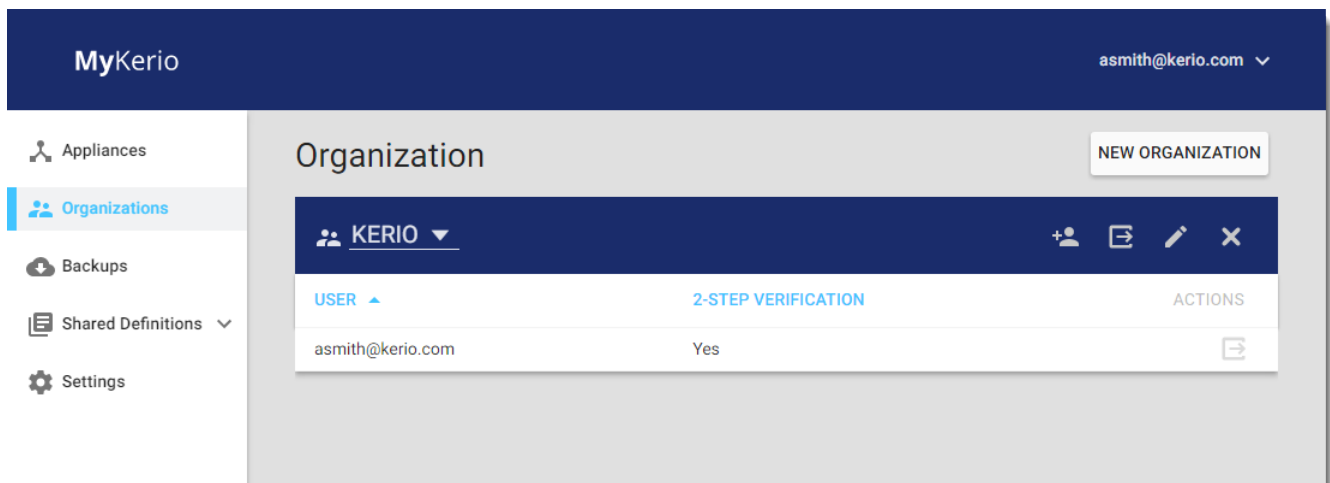
4.2 Managing users in organizations

You can give other administrators the ability to manage one or more of your organizations and appliances. These users then can rename the organization, add and manage appliances, and add or remove users.

4.2.1 Adding users to MyKerio

To allow other administrators to manage all the appliances within an organization, you must send them an invitation. Once you have invited them, they receive an email inviting them to become part of your organization:

1. Go to **Organizations** in MyKerio.

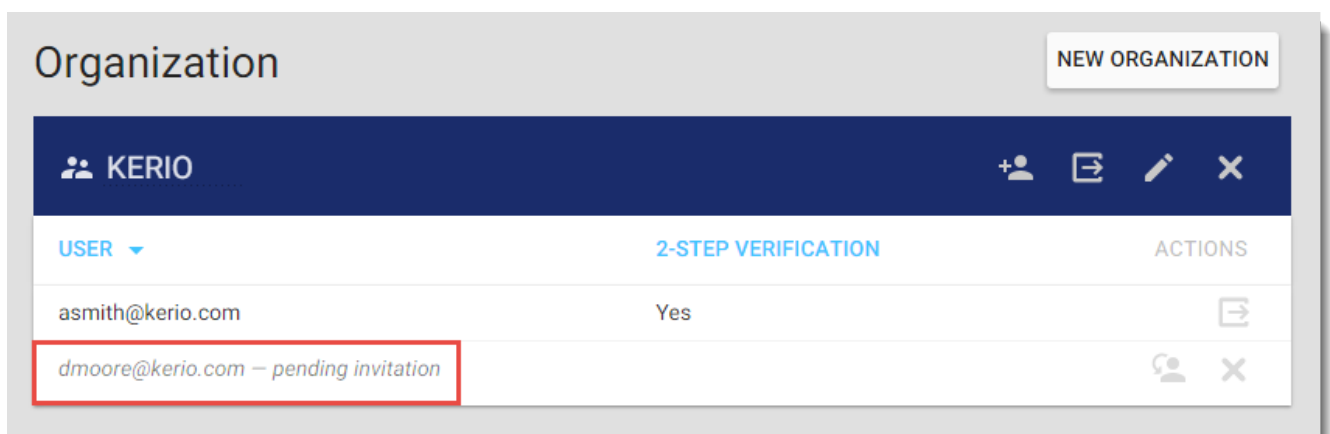


2. Click  to invite a user.

3. In the **Invite User to Organization** dialog box, type the user's email address. MyKerio sends an invitation email and the pending invitation appears in the list of users for the selected organization.

IMPORTANT

Ensure that the email address is typed correctly. The person that receives the email will have administration rights to your appliances.



4. The invited user receives the email (see below) and clicks **Accept invitation** to complete the invitation process.



User asmith@kerio.com has invited you to shared KERIO organization.

Accept invitation



Now you can see the new user in your MyKerio organization.

NOTE


The invitations are valid for 7 days, expired invitations disappear from the list. You can also [resend](#) and [revoke](#) the pending invitation.

Resending and revoking pending invitations

After you send an invitation to the organization, you can:

- » Click  to resend the invitation email. Resending the invitation resets the expiration time of the invitation back to 7 days.
- » Click  to revoke the pending invitation. Revoking the invitation disables any existing links in the invitations for the certain email address.

4.2.2 Deleting users from organizations

Click  to delete a user from the displayed organization.

If you want to delete a user from all your organizations, you need to delete them from each organization separately.

4.2.3 Adding and managing organizations

For more information, refer to [Adding and managing organizations](#) (page 29).

4.3 Sharing definitions across Kerio Control appliances with MyKerio

NOTE

MyKerio applies Shared definitions only to Kerio Control appliances. Also, this feature is only available in Kerio Control 9.0 and newer.

MyKerio allows you to share definitions for IP address groups, URL groups and time ranges across Kerio Control appliances.

You can share definitions among all the Kerio Control appliances within one organization. You can:

- » Create definitions directly within MyKerio and share them across appliances within the same organization
- » Import definitions from an existing Kerio Control appliance and share them with other Kerio Control appliances within the same organization

If you create shared definitions in MyKerio that already exist in the appliance, MyKerio converts them to shared definitions.

Once your Kerio Control appliance uses shared definitions, you manage these definitions in MyKerio, and they become read-only in the appliance.

You can also create and keep definitions directly in Kerio Control appliances. These local definitions cannot be shared with other Kerio Control appliances.

Defining shared IP address groups

In the **IP Addresses** section, you can create:

- » Single IPv4 or IPv6 addresses
- » Groups of IPv4 or IPv6 addresses
- » Hostnames
- » IP address ranges for IPv4 or IPv6
- » IPv4 subnets with masks
- » IPv6 prefixes

Kerio Control uses predefined IP address groups in other configuration dialog boxes, such as those for traffic and URL rules.

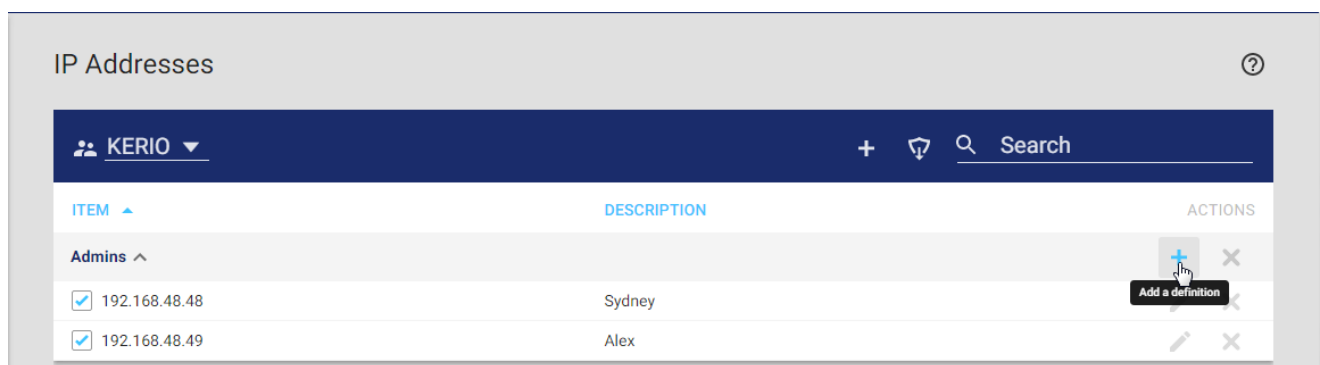
Adding new IP address groups

To create a new IP address group, you must first create a new definition group and then add new items:

1. In MyKerio, go to **Shared Definitions > IP Addresses**.
2. If you have more than one organization, select the appropriate one.



3. In the toolbar, click the **+** icon.
4. In the **Add IP Address Group** dialog box, type a name for the group.
5. Click **Add**. MyKerio creates a new IP address group and you can add items.
6. Click the **+** icon on the row with the IP address group name.



7. In the **Add IP Address** dialog box, select one of the following:

- **Addresses** - Type the IP address, range, network, subnet, or prefix. Click the **Address Examples** link for all patterns accepted by Kerio Control.
- **IP Address Group** - Type another group of IP addresses. Groups can be cascaded.
- **Firewall** - Firewall is a special group that includes all the firewall's IP addresses.

IMPORTANT


If you add a domain name, you must use the [Kerio Control DNS server and enable the DNS cache](#). If you use an IP address or host name you can use any DNS server.

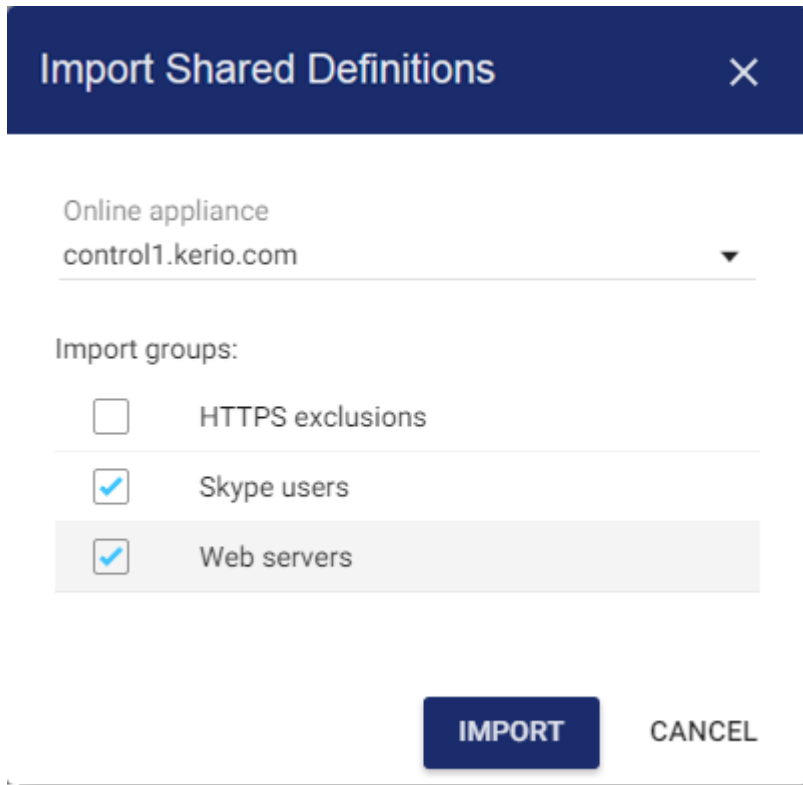
8. (Optional) In the **Description** field, type a description of the item.

9. Click **Add**.

Importing existing Kerio Control IP address groups

To import shared IP address groups from Kerio Control to MyKerio, you must first select the organization where the appliance is included and then import IP address groups. Imported groups are automatically shared with other Kerio Control appliances in the organization.

1. In MyKerio, go to **Shared Definitions > IP Addresses**.
2. Select the appropriate organization.
3. Click  in the toolbar.
4. In the **Import Shared Definitions** dialog box, select the appliance from the drop-down list.
5. Select the groups you want to share.



6. Click **Import**.

From now on, you can see the IP address groups you selected both in the organization in MyKerio and in all Kerio Control appliances included in the same organization.

Defining shared URL groups

URL groups enables you to define content rules in Kerio Control. For example, to disable access to a group of web pages, you can define a URL group and assign permissions to the group, rather than defining permissions for each individual content rule. A URL group rule is processed faster than a larger number of separate rules for individual URLs.

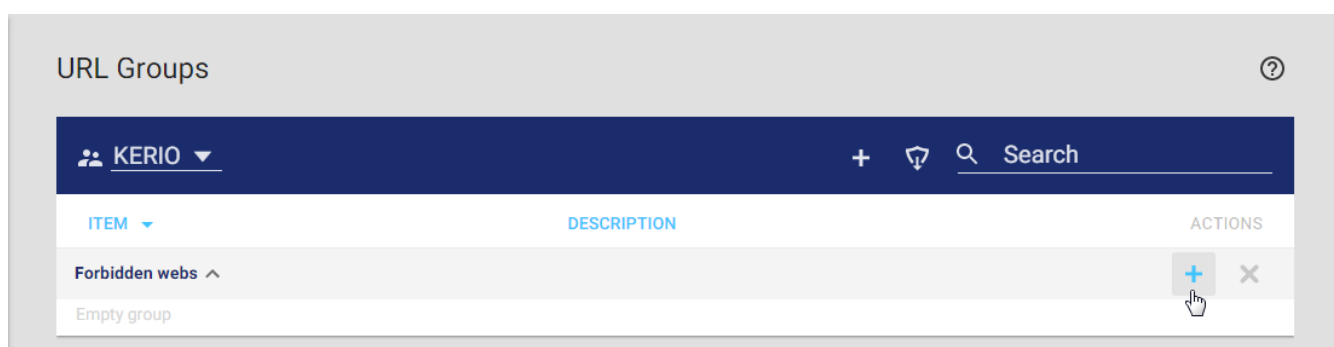
Adding new URL groups

To create a new URL group, you must first create a new definition group and then add a new URL/URL group or regular expression:

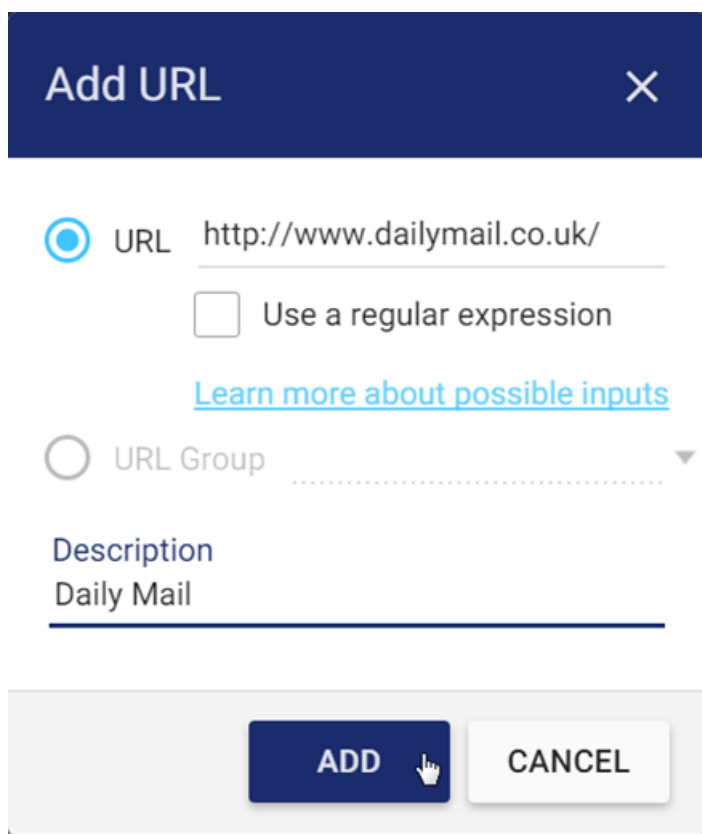
1. In MyKerio, go to **Shared Definitions > URL Groups**.
2. If you have more than one organization, select the appropriate one.



3. In the toolbar, click the + icon.
4. In the **Add URL Group** dialog box, type a name for the group.
5. Click **Add**. MyKerio creates a new URL group and you can add items.
6. Click the + icon on the row with the URL group (see figure below).



7. In the **Add URL** dialog box, add a URL or another URL group. A URL can be specified by using:
 - The full address of a server, document or web page without protocol specification (<http://>).
 - Substrings with wildcard characters: * or ?: An asterisk (*) stands for any number of characters, a question mark (?) represents one character.
 - Regular expressions. For details, see [Wildcards and regular expressions in URL](#)
8. (Optional) In the **Description** field, type a description for the URL. Especially if you use a regular expression, you should provide a description.
9. Click **Add**.



Importing existing Kerio Control URL groups

To import shared URL groups from Kerio Control to MyKerio, you must first select the organization where the appliance is included and then import URL groups. Imported groups are automatically shared with other Kerio Control appliances.

1. In MyKerio, go to **Shared Definitions > URL Groups**.
2. Select the organization.

3. Click  in the toolbar.

4. In the **Import Shared Definitions** dialog box, select the appliance from the drop-down list.
5. Select the groups you want to share.
6. Click **Import**.

From now on, you can see the imported URL groups for the selected organization both in MyKerio and in the individual Kerio Control appliances included in the same organization.

Defining shared time ranges

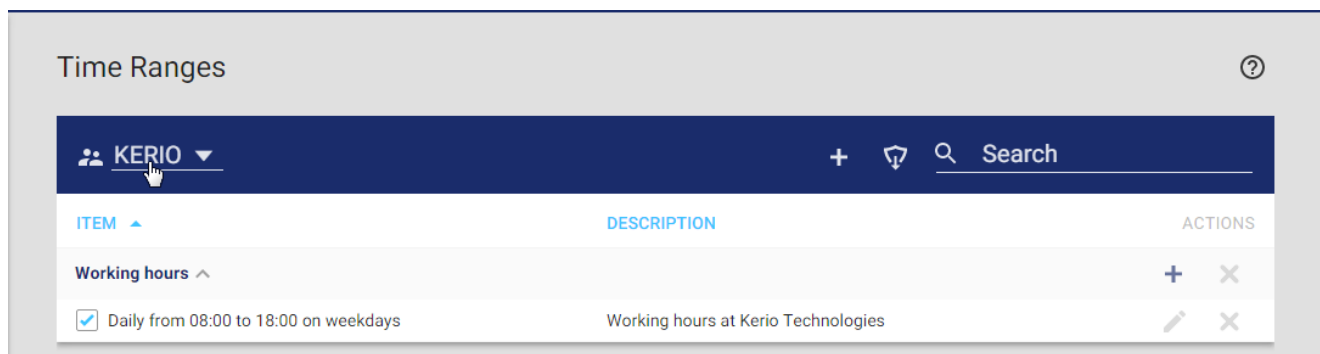
Time ranges define when Kerio Control rules should be valid.

Each time range can consist of multiple time spans with different settings.

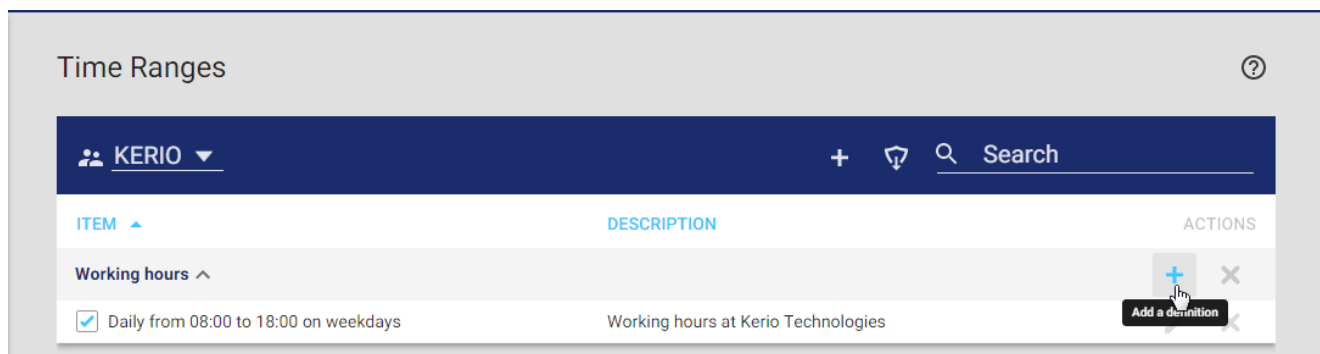
Adding new time ranges

To create a new time range, you must first create a new definition group and then create a new time range item:

1. In MyKerio, go to **Shared Definitions > Time Ranges**.
2. If you have more than one organization, select the appropriate one.



3. In the toolbar, click the **+** icon.
4. In the **Add Time Range Group** dialog box, type a name for the time range.
5. Click **Add**. MyKerio creates a new time range and you can add items.
6. Click the **+** icon on the row with the time range (see figure below).



7. In the **Add Time Range** dialog box, configure the frequency, start and end times and days, if applicable.

8. Click **Add**.

All Kerio Control appliances in the organization KERIO can now see and use the new shared time range.

Importing existing time ranges

To import time ranges from Kerio Control to MyKerio, you must first select the organization where the appliance is included and then import the time ranges. Imported time ranges are automatically shared with other Kerio Control appliances.

1. In MyKerio, go to **Shared Definitions > Time Ranges**.

2. Select the organization.

3. Click  in the toolbar.

4. In the **Import Shared Definitions** dialog box, select the appliance from the drop-down list.

5. Select the time ranges you want to share.

6. Click **Import**.

From now on, you can see selected time ranges for the selected organization in both MyKerio and the individual Kerio Control appliances included in the same organization.

4.4 Configuring 2-step verification in MyKerio

You can add an extra layer of security to your account by setting up 2-step verification, which uses an application on your smartphone or computer to confirm your identity. If you lose the device that has the authenticator installed, you can use backup codes generated by MyKerio; or sent to you by text message (SMS). See [Generating backup codes](#) and [Verifying your identity with the backup SMS codes](#).

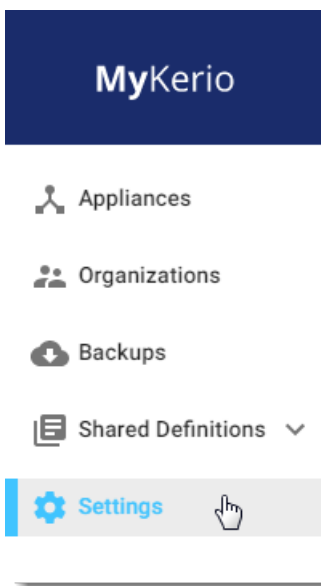
Once 2-step verification is in place, you must use your credentials to authenticate and type a special time-limited code generated by the authentication application. The authenticator needs to support RFC 6238. Examples include:

- » Google Authenticator – Available for iOS, Android and Windows Phone
- » [FreeOTP authenticator](#) – Available for iOS and Android
- » [Authenticator for iOS](#)
- » [Authenticator for Windows Phone](#)
- » [WinAuth for Windows OS](#)

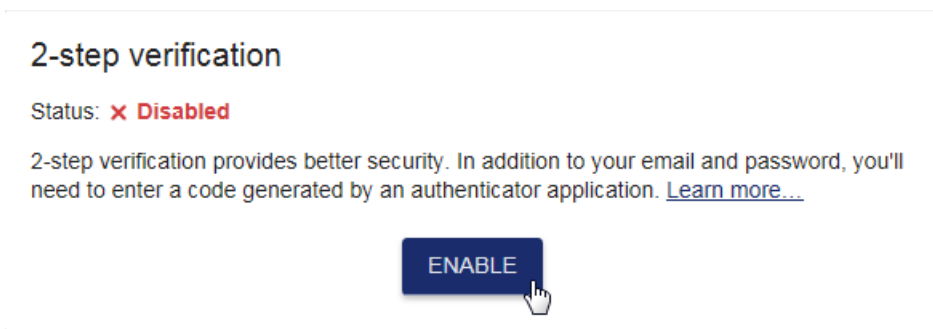
4.4.1 Enabling 2-step verification

To set up 2-step verification in MyKerio:

1. In the MyKerio interface, go to **Settings**.



2. In the **2-Step Verification** section, click **Enable**. The **Enable 2-Step Verification** dialog box appears.



3. Open the authenticator application and scan the QR code (barcode) or type the alphanumeric code shown below the QR code. You then get a time-limited, six-digit verification code. The authenticator generates a new code every 30 seconds. All codes generated on the basis of the MyKerio QR code are valid for MyKerio authentication.

Enable 2-Step Verification



2-step verification adds extra security to your account by using an application on your smartphone to confirm your identity. To enable 2-step verification, scan the QR code with your smartphone's camera using an authenticator application, then enter the verification code in the box below. [Additional instructions and a list of recommended authenticator applications...](#)



RDOAAB5WH7ZGW232

Verification code

961157|



VERIFY AND SAVE

CANCEL

4. Type the verification code from the authenticator app.

5. Click **Verify and save**.

From now on, 2-step verification is required when signing in to MyKerio.

4.4.2 Generating backup codes

MyKerio allows you to save several backup codes for authentication without the authenticator.

1. In the MyKerio interface, go to **Settings**.

2. In the **2-Step Verification** section, click **Generate**. The **Backup Codes for 2-Step Verification** dialog box appears.

2-step verification

Status: ✓ Enabled

DISABLE

Backup codes: ✗ None

Backup codes can only be used once and should be stored safely.

GENERATE

3. Click **Print** or **Save as file**. If you generate a new code set, all codes from the old set become invalid.

Backup Codes for 2-Step Verification ✕

If you don't have access to your device to get an authentication code, you can use offline backup codes.

Note: Each code can be used only once.

◦ 506932	◦ 302778
◦ 247825	◦ 817764
◦ 077551	◦ 739364
◦ 033436	◦ 500001
◦ 060653	◦ 572459

PRINT **SAVE AS FILE**

CLOSE

IMPORTANT

Each code can be used only once. However, you can generate new code sets as needed.

4.4.3 Verifying your identity with SMS codes

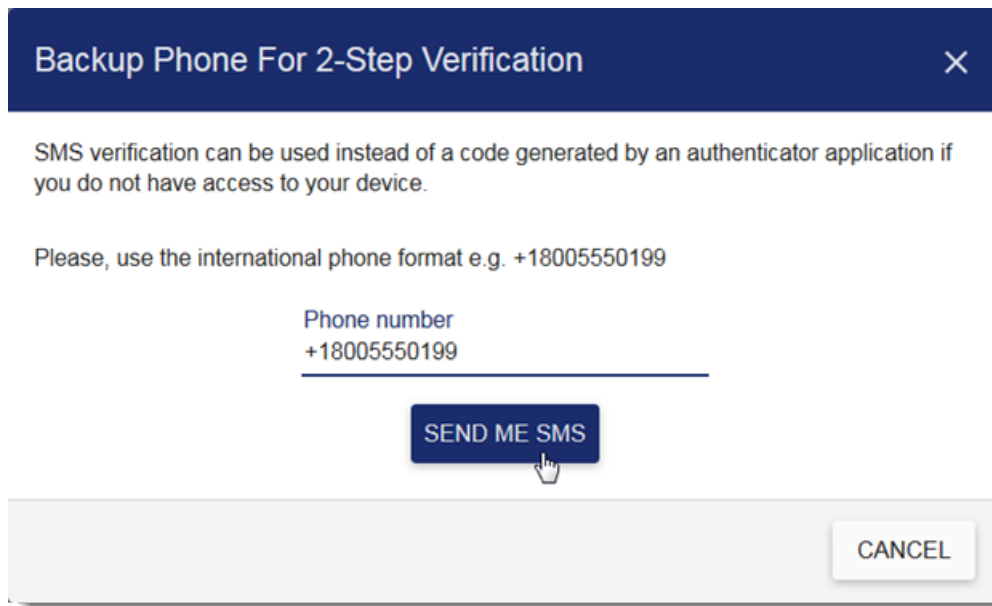
To use backup SMS codes, you must save your phone number in MyKerio settings.

1. In the **MyKerio** interface, go to **Settings**.
2. In the **2-Step Verification** section, click **Set backup phone**.
3. The **Backup Phone For 2-Step Verification** dialog box appears.
4. Type your phone number. The number must include the international prefix and you can use various formats, such as:

- + 1 (408) 496-4500
- + 7 (495) 9136823

• +420 377 338 901

5. Click **Send me SMS**.



The dialog box has a dark blue header with the title "Backup Phone For 2-Step Verification" and a close button (X). The main content area is white and contains the following text: "SMS verification can be used instead of a code generated by an authenticator application if you do not have access to your device." Below this, it says "Please, use the international phone format e.g. +18005550199". There is a text input field labeled "Phone number" containing the value "+18005550199". Below the input field is a dark blue button labeled "SEND ME SMS" with a mouse cursor hovering over it. At the bottom right of the dialog is a light gray button labeled "CANCEL".

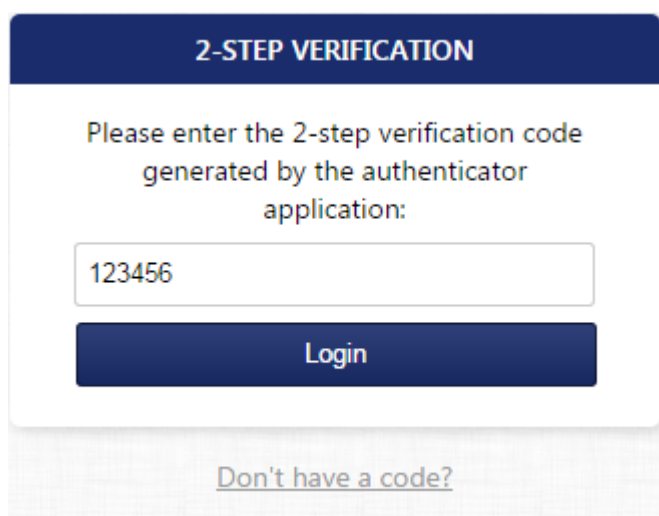
6. Type the code you receive via text message into the **Code from SMS** field.

7. Click **Verify and save**.

4.4.4 Cannot access your authenticator?

If you do not have your authenticator linked with the MyKerio account, you can use one of the backup codes or SMS code for 2-step verification.

1. In your browser, go to <https://my.kerio.com>.
2. Type your credentials in the login dialog box. The **2-step verification** dialog box appears.
3. In the **2-step verification** dialog box, click **Don't have a code?**



The dialog box has a dark blue header with the title "2-STEP VERIFICATION". The main content area is white and contains the following text: "Please enter the 2-step verification code generated by the authenticator application:". Below this is a text input field containing the value "123456". Below the input field is a dark blue button labeled "Login". At the bottom of the dialog is a light gray button labeled "Don't have a code?".

4. Type the backup code, or click **Send SMS** and type the SMS code into the dialog box.

5. Click **Verify and Login**.

4.4.5 Disabling 2-step verification

To disable 2-step verification:

1. In the MyKerio interface, go to **Settings**.
2. In the **2-Step Verification** section, click **Disable 2-step verification**. The **Disable 2-Step Verification** dialog box appears.

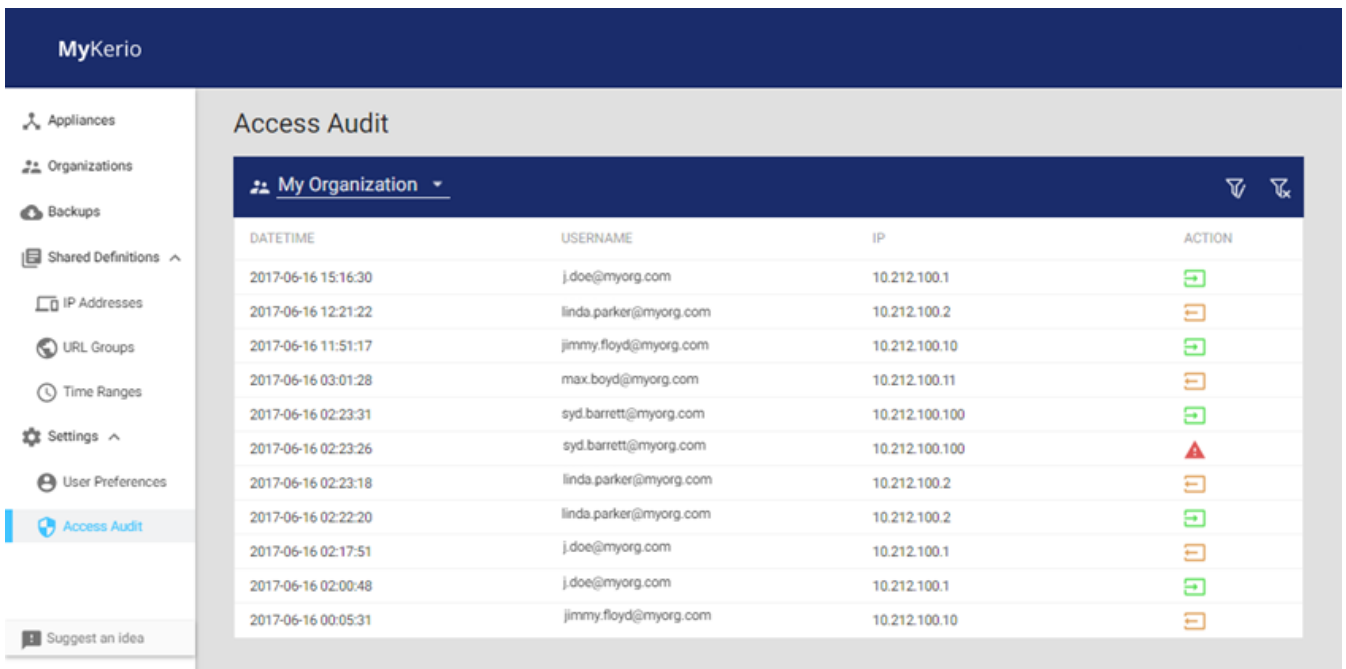


3. Type your MyKerio password to confirm the action.
 4. Click **Disable 2-step verification**.
- MyKerio disables 2-step verification and you no longer need it to access MyKerio.

4.5 Access auditing

MyKerio records details of each successful and failed login and logout attempts. These access audit trails provide a means to help accomplish several security-related objectives, including intrusion detection, and problem analysis.

Log in to MyKerio and go to **Settings > Audit Access** to view access audit trails.



Screenshot 2: The Access Audit screen

On the **Access Audit** screen, you can choose the organization to view the recorded access audit trail of its users.

Audit Filters [X]

Search:

Audit actions:

<input type="checkbox"/>	Login	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Logout	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Failed login attempt	<input checked="" type="checkbox"/>




Start Date

End Date

APPLY FILTERS **CANCEL**

Screenshot 3: Access Audit Filters

Use **Audit Filters**  to filter trail records based on:

- » The **IP Address** of user's machine or device.
- » The time range by specifying a **Start Date** and an **End Date**.
- » The type of access attempt by selecting **Login** , **Logout**  or, **Failed login attempt** .

Click **Apply filters** to only show access logs that match the filters configured.

4.6 Change or reset your password

If you forget or lose your password, you can always change or reset it.

4.6.1 Changing your password

To change your MyKerio password:

1. Log in to MyKerio.
2. Go to **Settings**.
3. In the **Change password** section, type your current and new passwords. MyKerio requires complex passwords.
4. Click **Change password**.

Change password

Current password

.....

New password

.....

✓ At least 8 characters long

✗ Characters from 3 different groups (lowercase, uppercase, numbers, symbols)

✓ Cannot include part of full name, email or username

Confirm password

.....

CHANGE PASSWORD



4.6.2 Resetting your password

If you lose your MyKerio password:

1. Go to <https://my.kerio.com/login>.
2. Click **Forgot password**.
3. In the **Reset your password** dialog box, type your email address and click **Send**.
4. Go to your mailbox and wait for a message with the subject Reset your MyKerio password.
5. In the message body, click **Change password**. Your browser opens a dialog box where you can change your password.
6. Type your password twice.
7. Click **Set New Password**.

You can now log in to MyKerio with your new password.

5 Troubleshooting and support

This topic explains how to resolve any issues encountered during installation of MyKerio. The main sources of information available to solve these issues are:

- » This manual - most issues can be solved through the information in this help system.
- » Knowledge Base articles
- » Web forum
- » Contacting Technical Support

If this manual does not satisfy your expectations, or if you think that this documentation can be improved in any way, let us know via email on: documentation@gfi.com.

5.1 Receiving emails via MyKerio notification service does not work

MyKerio notification service includes a local email blacklist to temporary suspend sending emails to recipients with a history of bounce messages. The blacklist blocks each invalid email address for 2 weeks. MyKerio removes the email address from the blacklist after 2 weeks from the last bounce messages.

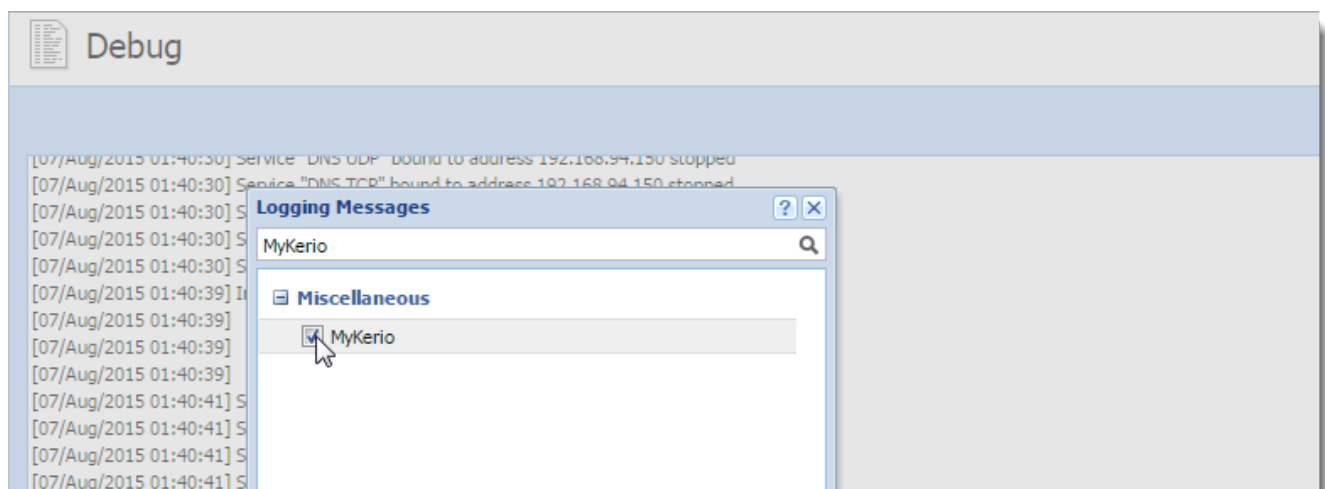
Identifying problems with email addresses in the administration

If you use MyKerio notification service and delivering emails from your appliances doesn't work, you can have an invalid or blocked email address configured in the appliance.

If blacklisted email address is typed in alerts or statistics reports, consult the **Warning** log and check your Internet connectivity, traffic rules and so on.

Otherwise, consult the **Debug** log for more information:

1. In the administration interface, go to **Debug log**.
2. Right-click in the main window.
3. In the context menu, click **Messages**.
4. In the **Logging Messages** dialog box, select **MyKerio**.



5. Click **OK**.

From now on, the Debug log records all MyKerio activity such as requests, responses, errors.

NOTE

After debugging, deselect MyKerio in the **Logging Messages** dialog box. Otherwise, the appliance continues to record the MyKerio communication and may slow down the server performance.

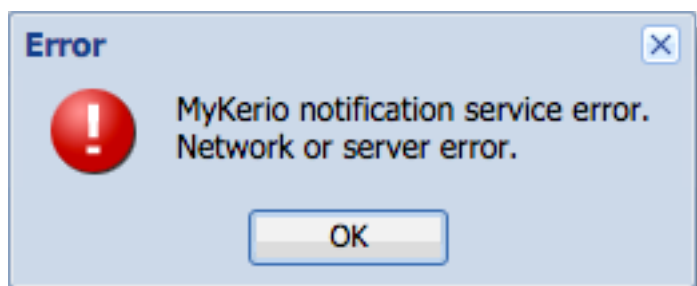
Testing SMTP relay email addresses

You can test the SMTP relay in following places:

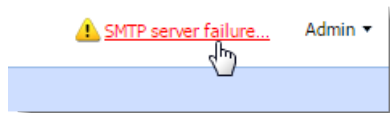
- » **Remote Services > SMTP Relay** in Kerio Control
- » **Advanced Options > General** in Kerio Operator.

If you use blacklisted email address as a test email address and the test fails due to an incorrect email address:

- » Kerio Control displays the error dialog box



- » Kerio Operator displays the SMTP server failure notification and logs an error in the Error log.



Examples of Debug log messages

Debug log message	Description
[07/Aug/201815:27:00] {MyKerio} Operation failed Recipient asmith@example.local: Email address format is not valid.	The recipient's email address format is not valid or the TLD domain does not exist.
[07/Aug/2018 15:29:57] {MyKerio} Operation failed Recipient asmith@example.com: Email send failed. Recipient is blacklisted due to bounce messages.	The recipient has a history of bounce messages and the MyKerio notification service cannot deliver the email. The recipient is temporarily blacklisted for 2 weeks.
[07/Aug/2018 15:30:15] {MyKerio} Operation failed Email to asmith@example.com rejected. Your appliance is not allowed to send emails due to too many bounced emails.	The connected appliance has tried to send emails to multiple recipients which have a history of bounce messages. All emails from that appliance will be rejected until the number of the blacklisted recipients decreases. MyKerio automatically removes email addresses from the blacklist after 2 weeks from the last attempt to send email.
[08/Mar/2018 15:32:45] {MyKerio} Operation failed Email to asmith@example.com rejected. Your appliance exhausted email quota.	The connected appliance has sent more that 100 emails within 24 hours and exceeded the email quota. The time period is counted from the first sent email within the time period and resets after 24 hours.

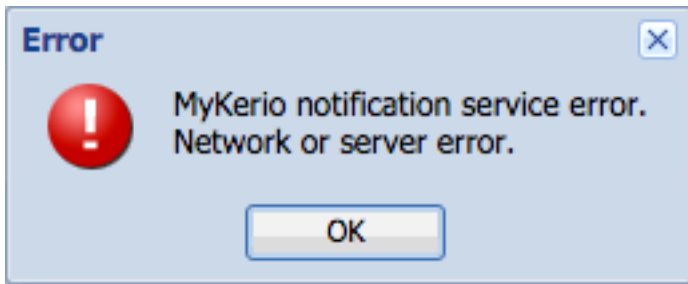
Testing SMTP relay email addresses

You can test the SMTP relay at the following places:

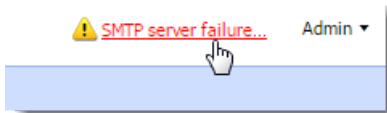
- » **Remote Services > SMTP Relay** in Kerio Control
- » **Advanced Options > General** in Kerio Operator.

If you use blacklisted email address as a test email address and the test fails due to an incorrect email address:

- » Kerio Control displays the error dialog box.



- » Kerio Operator displays the **SMTP server failure** notification and logs an error in the **Error** log.



Identifying problems with email addresses in MyKerio

MyKerio displays an error message if you type invalid email address during your:

- » Registration. (MyKerio sends you confirmation email).
- » Attempt to reset your MyKerio password (MyKerio sends you email where you can set a new password).

Verify the email address. If the email address is valid, try to, for example, send an email message from a different email address to see whether your blacklisted email address can receive messages.