GFI AppManager™ AI

Administrator Guide



GFI Software™

Table of contents

Introduction to GFI AppManager AI 4
- How it works 4
- SMB or MSP use case 4
- Supported products 5

Getting Started 5
- Account registration 5
- Appliance deployment 7
  - GFI KerioConnect® 7
  - GFI KerioControl 7
  - GFI Archiver AI 9
  - GFI Exinda AI 11
  - GFI LanGuard 11

Using GFI AppManager AI 12
- Home 12
  - Overview 12
  - Notifications 13
  - Configuration 14
  - IP address groups 14
  - URL groups 15
  - Backups 16
- Definitions 16
  - IP address groups 16
  - URL groups 16
  - Account groups 16
  - Appliance groups 17
  - Time range groups 18
  - MyKerio 19
- Alerts 20
  - Notifications 20
  - Alerts 20
  - Destinations 22
- Users 23
- Task Scheduler 24
  - Creating a scheduled task 24
- Reports 25
  - How to create a report 25

Products 26
News 26
Profile 27
Setting up Two-Factor Authentication 27
Passkey Registration 27
Passkey Authentication 27
Manage 28
Removing from GFI AppManager AI 28
GFI AppManager AI Settings 29

GFI AppManager AI 29
Who can access it? 29
Licensing 29
How to use the AI add-on 29
Sample use case 30
What's beyond the AI capabilities? 31

GFI KerioControl Management 31
Adding an IP Address to an IP Address group 31
Adding an IP Address to a Traffic Rule 31
ShieldMatrix UI 32
Maximum Concurrent Connections 32

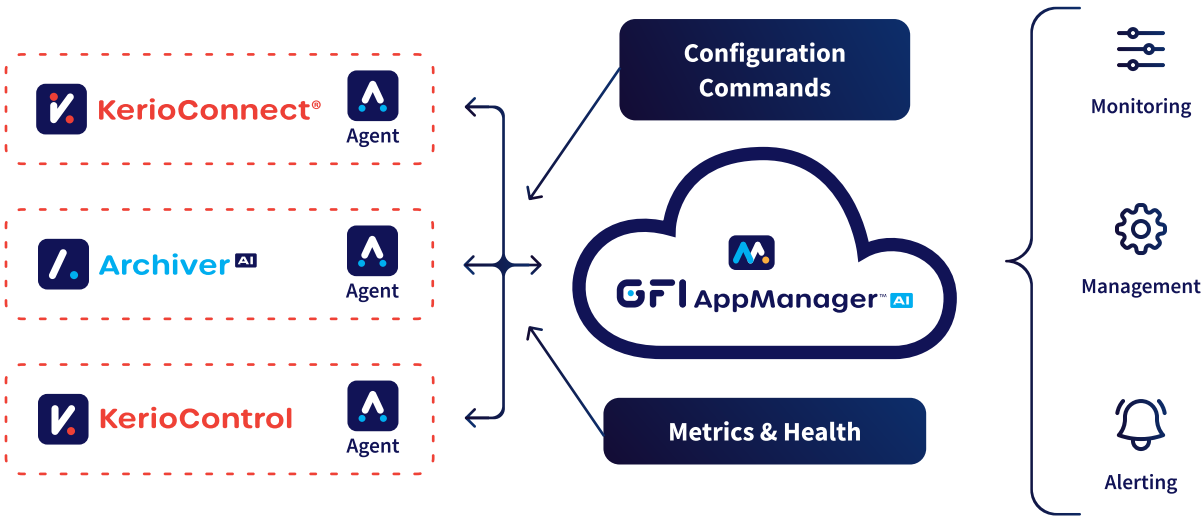
GFI KerioConnect® Management 33
DKIM Validation 33

Support 33
GFI Archiver AI Management in GFI AppManager AI 34
Get help 35

Last modification: 23/08/2026

How it works

Each product deployment will have its own agent responsible for sending metrics and health information to the GFI AppManager AI. On the other hand, configuration commands can be sent from the GFI AppManager AI to each deployment, and each product can be managed remotely through GFI AppManager AI's web interface.



SMB or MSP use case

The information that is going to be shown initially in the GFI AppManager AI's dashboard depends on the type of customer that is accessing GFI AppManager AI:

- **SMB**: They have a single organization and a single account. They will have access to their own deployments.
- **MSP**: Will have a single organization with access to multiple customer accounts, and within these accounts, they will have access to each customer's deployments.

Note: These settings are not interchangeable, so we advise you to identify the use case that suits your needs best before registering in GFI AppManager AI.



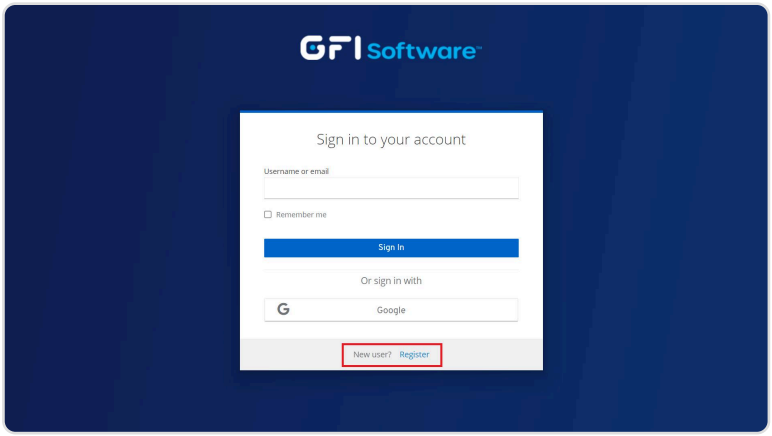
Supported products

Product	Version
GFI KerioConnect®	10.0.2p2 and above
GFI KerioControl	9.4.3p1 and above
GFI Archiver AI	15.7 and above
GFI Clearview AI	7.5.7 and above
GFI LanGuard	12.15 and above
GFI Exinda AI	7.5.7 and above

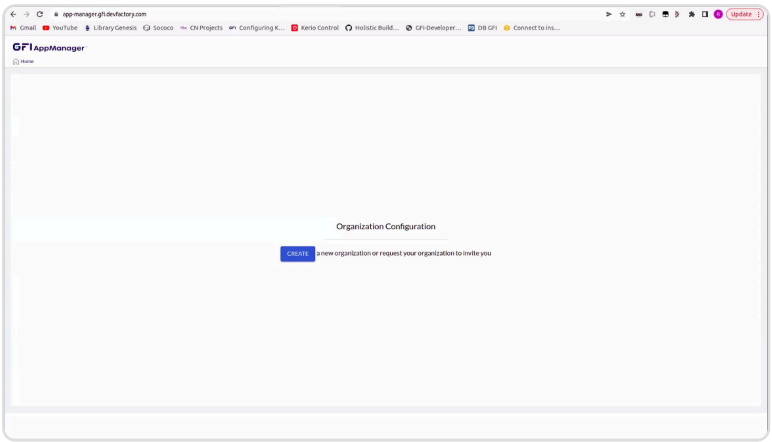
Getting Started

Account registration

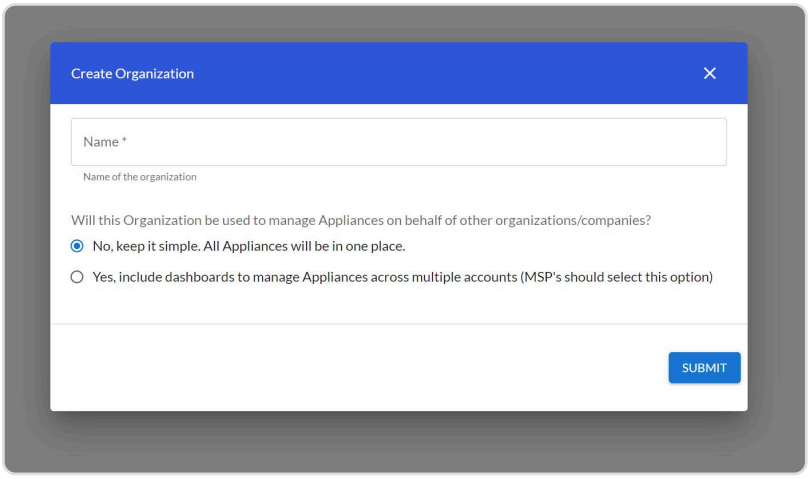
1 Visit AppManager.ai and **register** for a new account.



2 Once you are logged in, **create** the first organization you want to manage.

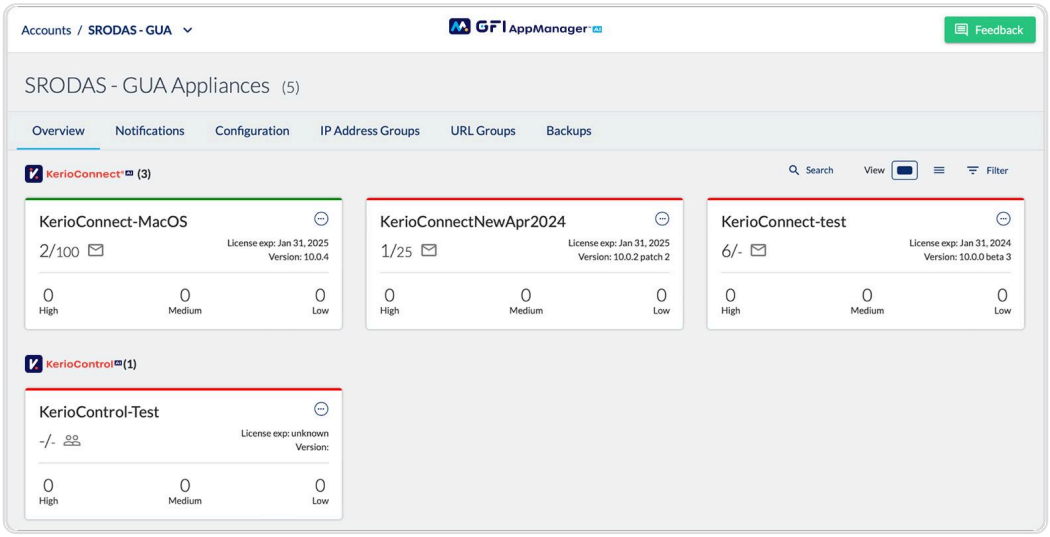


3 Enter the organization's name and decide if you want to manage only a single organization through this account or multiple ones. Click Submit to create the organization.



4 **Scenario A**: "No, keep it simple. All appliances will be in one place."

GFI AppManager AI will create the new organization and redirect you to its **Overview** page. The page will not show any data because appliances are not yet associated with this GFI AppManager AI account.



Scenario B: "Yes, include dashboards to manage Appliances across multiple accounts (MSPs should select this option)."

GFI AppManager AI will create the new organization and redirect you to the **Home** page. Click the (+) Add button in the top right to add all the organizations you want to manage.

5 You can add appliances to a GFI AppManager AI organization in 2 ways:

1. During the installation of the latest version of the product, the corresponding step should be confirmed in the installation wizard.
2. Through the product's admin UI.

Appliance deployment

1 Download the product installers for the GFI AppManager AI integration from the Upgrade Center.

- GFI KerioControl 9.4.3.p1 and above
- GFI KerioConnect® 10.0.2 Patch 2 and above
- GFI Archiver AI 15.7 and above
- GFI Exinda AI 7.5.7 and above.
- GFI LanGuard 12.15 and above

Note: It's always recommended to download the **latest version** of the product as it includes the newest features and bug fixes.

2 Launch the installer and continue with the standard installation process.

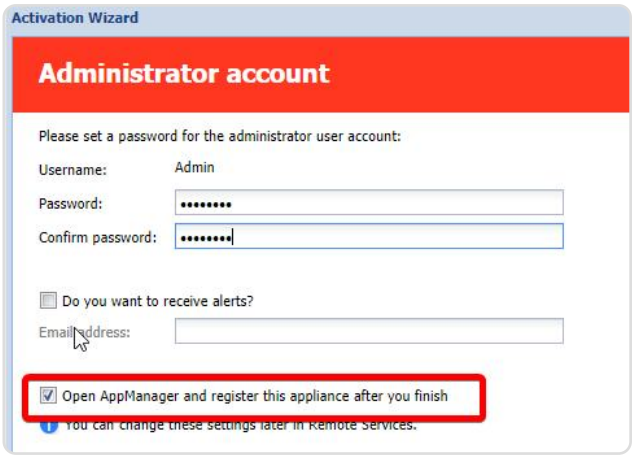
- GFI KerioConnect® (only Windows version available)
- GFI KerioControl (installing software appliance)
- GFI KerioControl (manual upgrade of existing appliances)
- GFI Archiver AI (installation procedure)
- GFI Archiver AI (upgrading procedure)
- GFI Exinda AI (installation procedure)
- GFI Exinda AI (upgrade procedure)
- GFI LanGuard (installation procedure)
- GFI LanGuard (upgrading procedure)

3 Consent to GFI AppManager AI registration during the installation process.

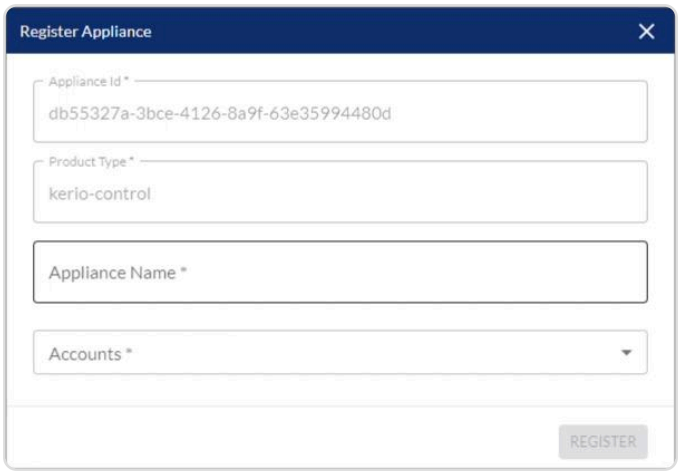
GFI KerioConnect®



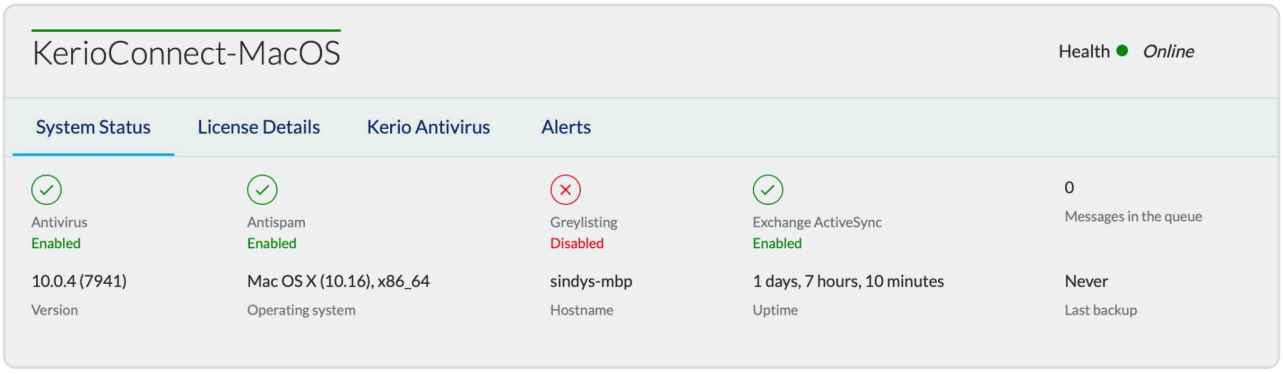
GFI KerioControl:



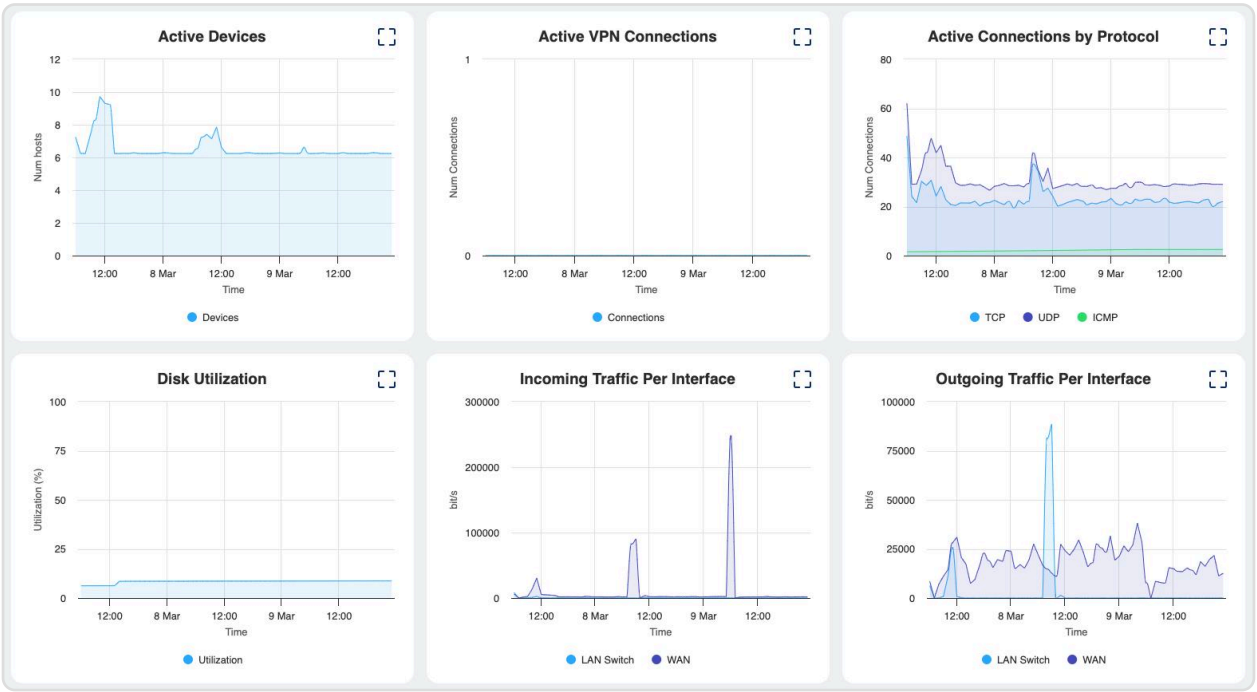
4 A new browser window will open. Set the appliance name and choose the GFI AppManager AI account to which this appliance will be linked.



Note: You can only assign appliances to existing GFI AppManager AI accounts.



Sample image of some of the information available in GFI AppManager AI



Sample image of the graphs available in GFI AppManager AI

Once the appliance is added, you will be able to **monitor** and **manage** the installation/device through GFI AppManager AI.

Device configuration export and restore behavior (For GFI KerioControl only)

This section explains how GFI AppManager AI handles configuration data during export and import when restoring a hardware appliance, either on the same appliance or when restoring a backup to a new appliance

Scenarios that affect configuration restore

1. **Restore from a different appliance**

   If the configuration being imported comes from a different appliance, the GFI AppManager AI-related data included in the backup is ignored during import, triggering registration from scratch.

2. **Restore from the same appliance (full backup restore)**

   When restoring a backup taken from the same appliance, a new checkbox is presented during the restore process. The user is asked whether they want to:

   - **Keep the existing configuration** (for example, to remain clean after a fresh reinstall), or
   - **Restore the previous configuration** from the backup.

   This gives administrators explicit control over how GFI AppManager AI configuration is handled during a same-appliance restore.

3. Restore initiated from the GFI AppManager AI side (implicit behavior)

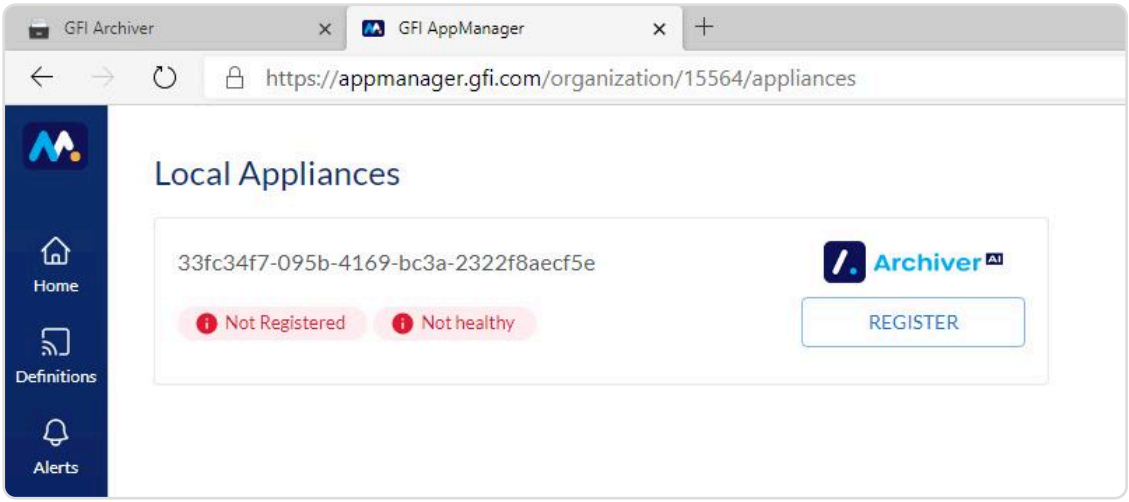
   When a restore is initiated from the GFI AppManager AI side, the system implicitly follows **Scenario 2,** but with one important difference:

   - The option to keep the existing configuration is automatically selected.
   - No choice is presented to the user (to prevent users from being locked out).

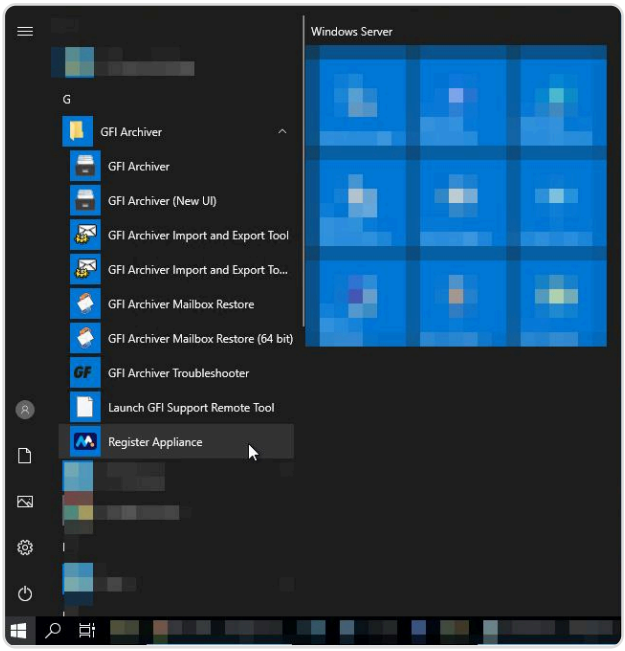
GFI Archiver AI:

There are 3 ways to register GFI Archiver AI to GFI AppManager AI

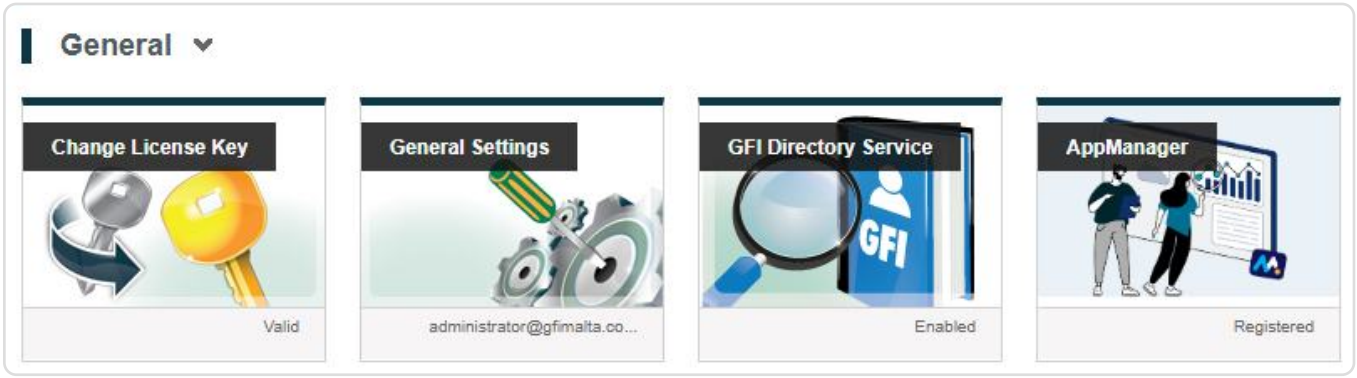
1. Upon updating GFI Archiver AI to the latest version, you are automatically redirected to the GFI AppManager AI webpage to sign in. Once you're signed in, you'll see the screen below. Click **Register** to register your GFI Archiver AI. For the latest version of GFI Archiver AI, go to Upgrade Center.



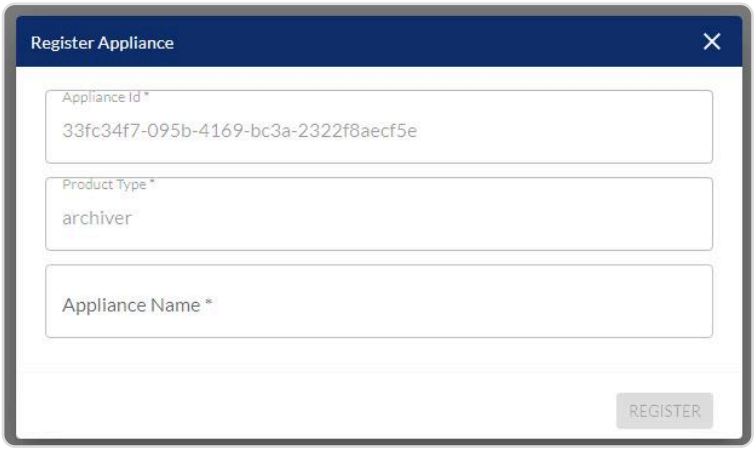
2 Alternatively, in Windows, select GFI Archiver AI and Register Appliances.



3 From within GFI Archiver AI - Go to the Configuration tab and scroll down to the General Section, click on GFI AppManager AI.



Register your GFI Archiver AI.



In the case of GFI Archiver AI, you will see the following screen with Product Type listed as GFI Archiver.

GFI Exinda AI

Before registering your GFI Exinda AI with GFI AppManager AI, ensure the following prerequisites are met:

- Ensure the GFI Exinda AI appliance has proper network connectivity and is time-synchronized correctly.
- The appliance must have a valid license applied.

Registration process:

- Log in to your GFI Exinda AI appliance web interface using admin credentials.
- Navigate to the Configuration > System > Setup.
- Look for the "AppManager" tab.
- Click the "Register" button, which should redirect you to the GFI AppManager AI portal, where you can log in with the credentials for the account under which this GFI Exinda AI will be registered.
- If prompted, accept the license agreement (EULA) for AI services.

After successful registration, your GFI Exinda AI appliance should appear in your GFI AppManager AI dashboard. You can verify the connection by checking if:

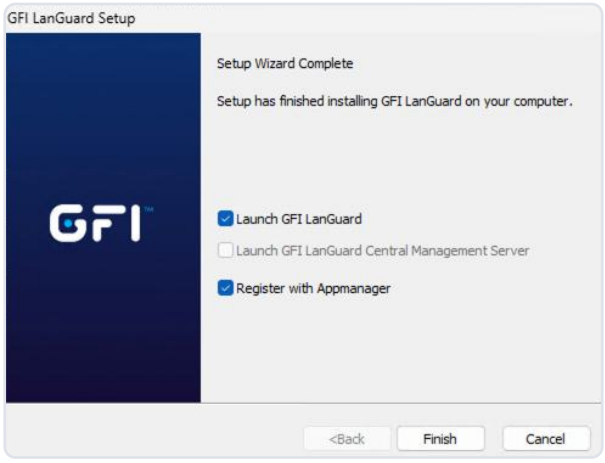
- The appliance shows as "online" in the dashboard.
- Traffic data is being correctly transmitted and displayed.
- You can access the appliance's management interface through GFI AppManager AI.

GFI LanGuard

Registration process:

To connect your GFI LanGuard installation to GFI AppManager AI for centralized management, follow these steps:

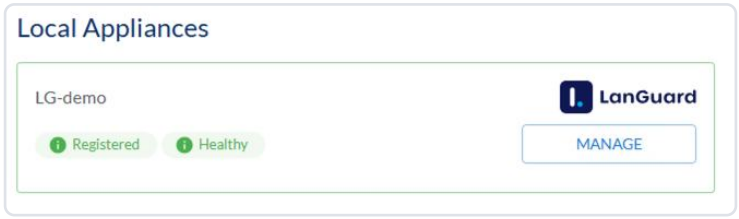
- Select the Register with GFI AppManager AI option in the final step of the installer. This launches the GFI AppManager AI portal.



- Log in to your GFI AppManager AI account. If you don't have one yet, create an account before continuing.
- Click Register.



- Define the Appliance Name for this GFI LanGuard installation.
- Wait for the GFI AppManager AI registration and health check to complete.



Once the health check finishes, your GFI LanGuard installation will be accessible through GFI AppManager AI.

Using GFI AppManager AI

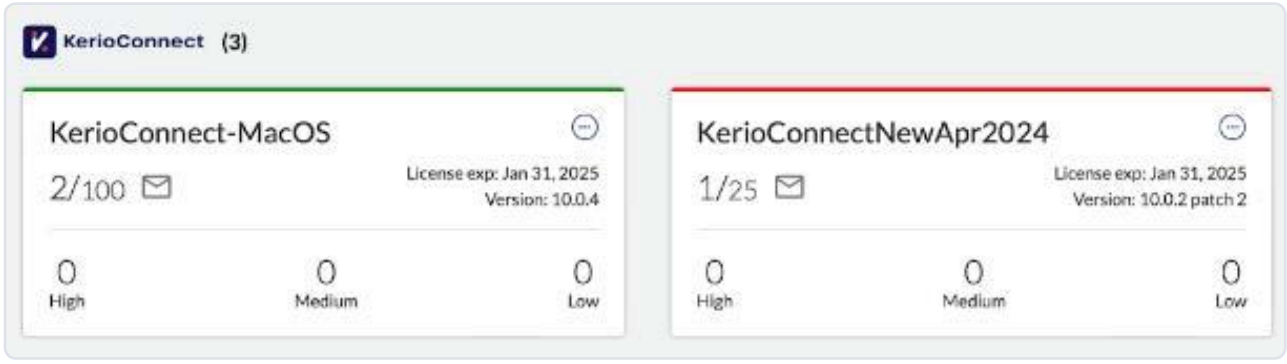
Home

Overview

- **Appliance status**

  When the appliances are added to GFI AppManager AI, you can see their status in the Home > Overview section. Colors indicate the status of the appliance:

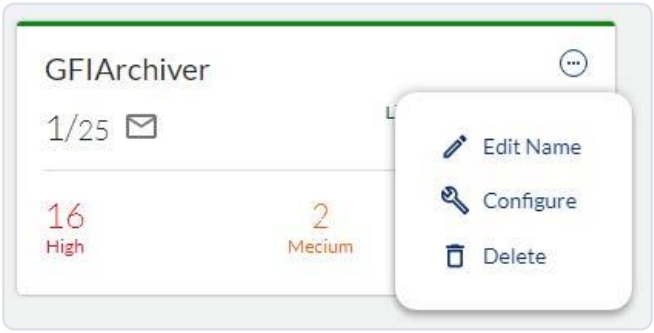
  - **Red:** The appliance is offline or has some major issues.
  - **Green:** The appliance is online.



From the Overview page, you also get a summary of Notifications generated by the specific appliance, grouped by status: High, Medium, and Low. Other information accessible from the Overview page includes the appliance's IP address and license details.

The Action button ⋯ is located on the right. By clicking on this button, you can:

- **Edit** the appliance name or assign it to a different account.
- **Configure** the appliance. This will redirect you to the main administration page.
- **Delete** the appliance from the account. This action is recommended only if the appliance has been uninstalled or if it is not working properly.



You can click each listed appliance to configure its settings. The options available in GFI AppManager AI for GFI KerioControl, GFI KerioConnect®, and GFI Archiver AI are the same as those you can configure from each product administrator's interface. For more information on the options you can change, please refer to the manual for each product.

→ GFI KerioConnect® Help

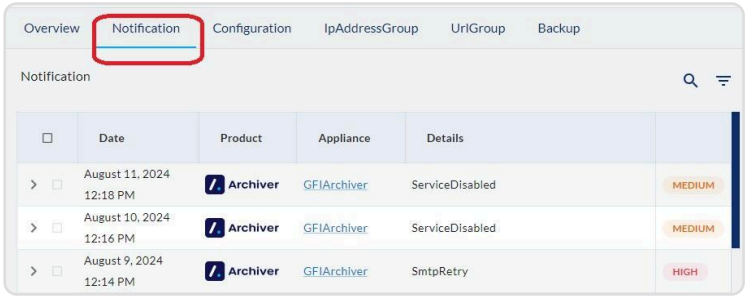
→ GFI KerioControl Help

→ GFI Archiver AI Help

→ GFI Exinda AI Help

Note on dashboard graphs and metrics: When viewing data over longer time ranges (7 days or more), GFI AppManager AI retrieves information from an aggregated metrics store. As a result, data points are averaged over time to simplify the display. For instance, a spike of 104,000 may appear as 54,000 when shown over 14 days, since the data reflects an average rather than specific peaks. Therefore, the level of detail is higher when viewing data for a single day compared to a broader time range.

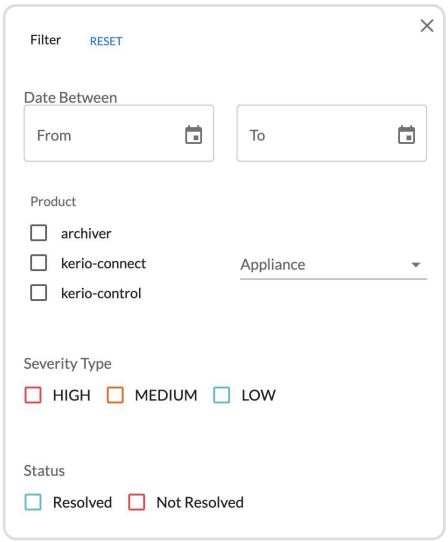
Notifications



The notification section in GFI AppManager AI will show all the notifications that each appliance has generated, along with the following information:

- Date of the event
- Product
- Appliance Name
- Details of the event
- Type of Alert: High, Medium, and Low.

You can expand the notification to see the Message related to the event. From this view, you can use the button to manage the alert that triggers this notification, or the button to remove it. You can also toggle the button to mark the notification as resolved/unresolved. You can use the button to filter notifications by different criteria.



Configuration

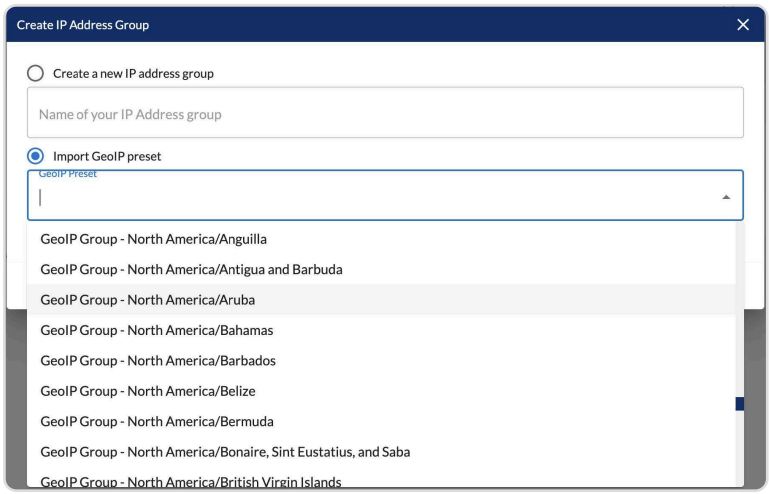
From the configuration section, you can perform the following actions:

- Managing accounts
  - Rename account
  - Delete account (Coming soon)

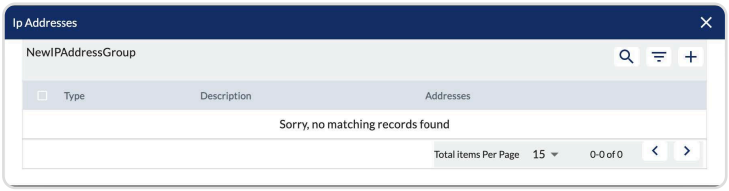
IP address groups

IP addresses are identifiers assigned to devices connected to a TCP/IP Network. IP address groups can be used in other configuration dialogs throughout GFI AppManager AI.

- Add a new IP address group:
  - From the IP address groups section click on + CREATE IP ADDRESS GROUP
  - In the following dialog, you have 2 options:
    - Enter the name of the IP address group or
    - Import a GeoIP preset group (This option is available only with GFI KerioControl 9.4.5 and above, and applies exclusively to GFI KerioControl appliances).

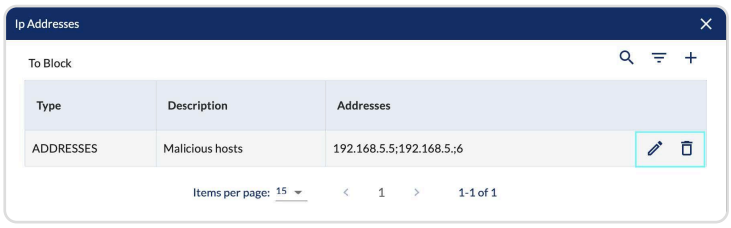


  - Click **CREATE.**
- Add an IP address:
  - Select the icon on the IP address group to open the IP address list. Click on the plus sign to add a new IP address.



  - Type in a description of the IP address for reference, and choose the IP .
  - Address Type:
    - **Addresses** can include an IP address, an IP address range, a network, a subnet, or a prefix.
    - An IP address group is a group of IP addresses. Groups can be cascaded.
    - A firewall is a special group including all the firewall's IP addresses.
  - Click **Save** to complete the process.

- Manage IP addresses:
  - Once IP addresses have been created, they can be edited or deleted using the buttons on the left.



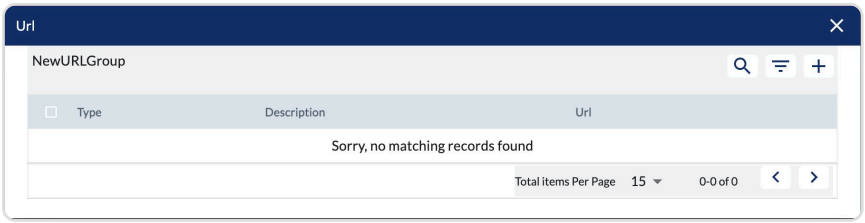
URL groups

URL groups allow administrators to define different rules or configurations for a group of web pages rather than do it individually. A URL group rule is processed faster than a greater number of separate rules for individual URLs.

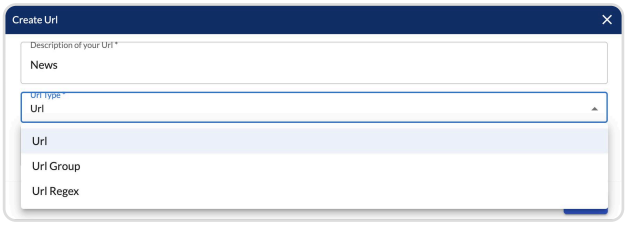
- Create URL groups
  - From the URL groups section, click on + CREATE URL GROUP
  - In the following dialog, enter the name of the URL group.



    - Click **CREATE**
- Add a URL
  - Select the icon on the URL group to open the URL list. Click on the **plus** sign to add a new URL



  - Type in a description of the URL group and choose the URL type, which can be specified as follows:
    - Full address of a server, a document, or a web page (http://).
    - Another URL group. Groups can be cascaded.
    - Regular expressions

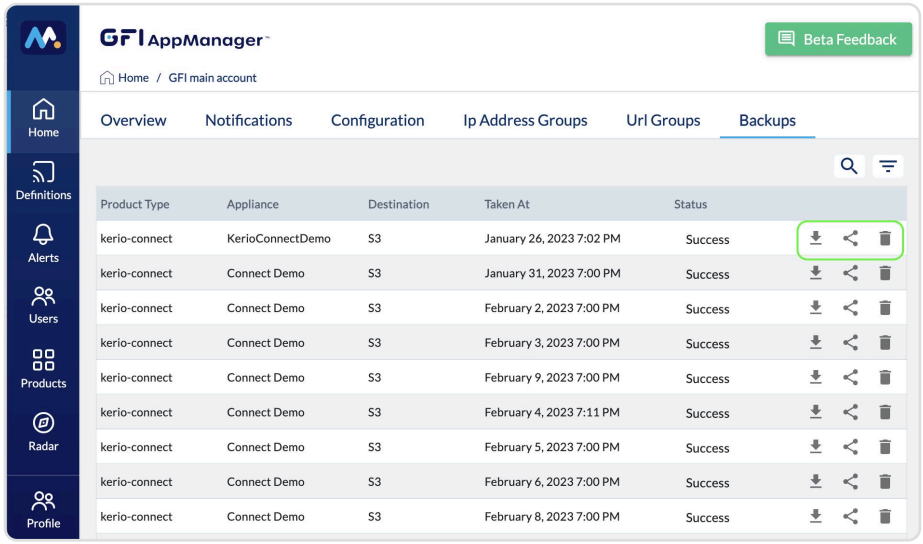


- Manage URLs:
  - Once URLs have been created, they can be edited or deleted using the buttons on the left.



Backups

Your appliances' configurations can be automatically backed up to GFI AppManager AI. From the Backups tab, you can access the list of backups per appliance and download the configuration file backup you need, share it, or delete it.



Definitions

GFI AppManager AI allows you to share definitions for IP address groups and URL groups throughout the appliances that GFI AppManager AI manages, and Account groups and Appliance groups can be used to define alerts and notifications.

IP address groups

Refer to the IP address groups section under Home in this document.

URL groups

Refer to the URL groups section under Home in this document.

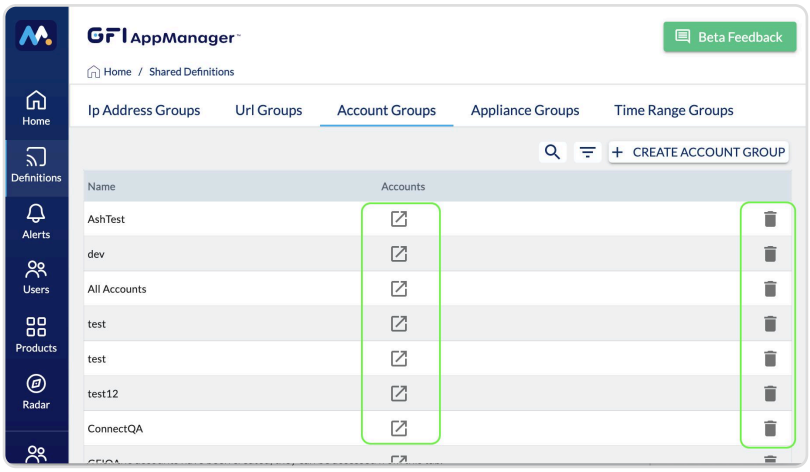
Account groups

Account groups can be created to manage accounts as a whole rather than individually. Then these groups can be used to define alerts and notifications that will be applied to all the organizations that belong to them.

- **Create an account group**
  - Go to **Definitions** on the left-side menu.
  - From the Account groups section, click on + CREATE ACCOUNT GROUP .
  - In the following dialog, enter the name of the Account group.
  - Select or type the accounts that will be part of this group.
  - Click **SAVE.**



When the accounts have been created, they can be accessed for managing or deleted from this tab.



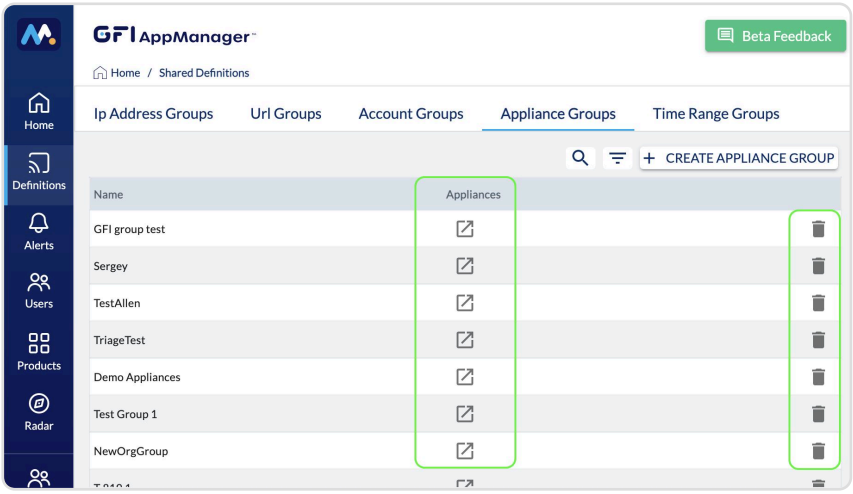
Appliance groups

Appliance groups can be created to manage appliances as a whole rather than individually; for example, production appliances or test appliances may be managed differently. These groups can be used to define alerts and notifications that apply to all appliances they contain.

- **Create an appliance group**
  - From the Appliance groups section click on + CREATE APPLIANCE GROUP .
  - In the following dialog enter the name of the Appliance Group.
  - Select the appliances that will be part of this group.
  - Click **SAVE**.



When the Appliance groups have been created, they can be accessed for management or deleted from this tab.



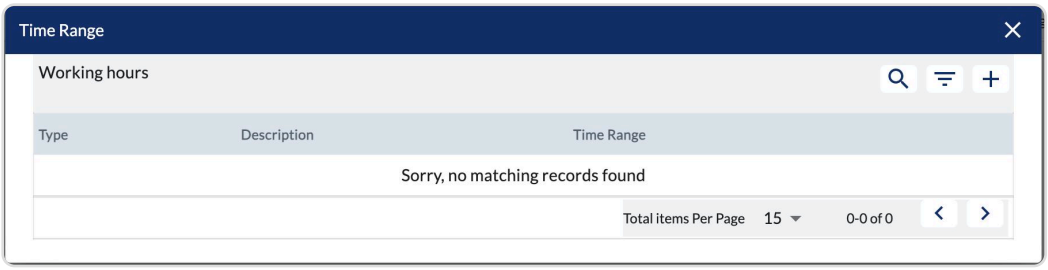
Time range groups

Time ranges define when GFI KerioControl rules are valid. Each time range can consist of multiple time periods with different settings.

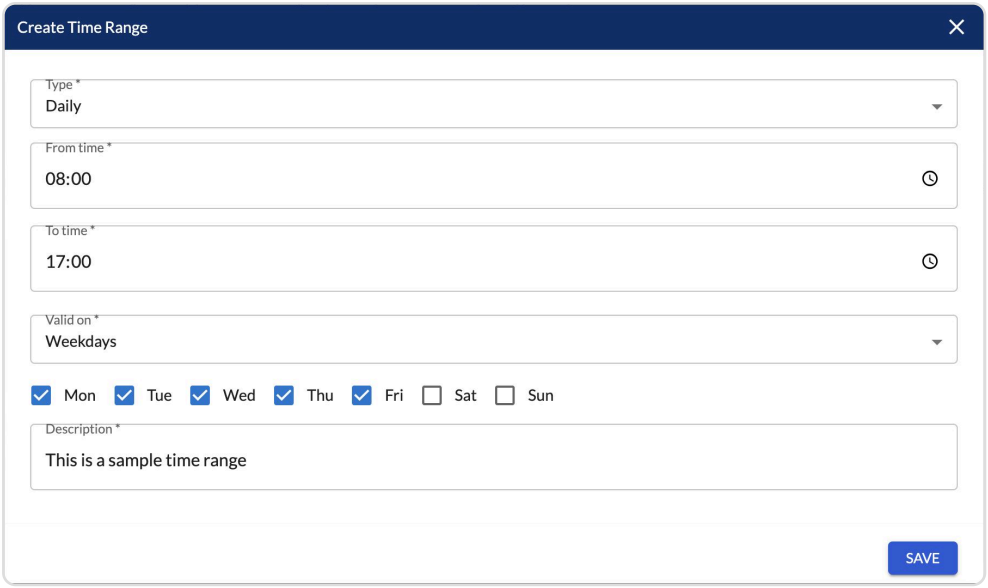
- **Create a Time range group**
  - From the Time range groups section, click on + CREATE TIME RANGE GROUP .
  - In the following dialog enter the name of the Time range group.
  - Click **CREATE.**



- **Add a time range**
  - Select the icon on the Time range group to open the Time range list. Click on the plus sign to add a new Time range



  - Type in a description of the Time range and other required information as shown in the dialog below:

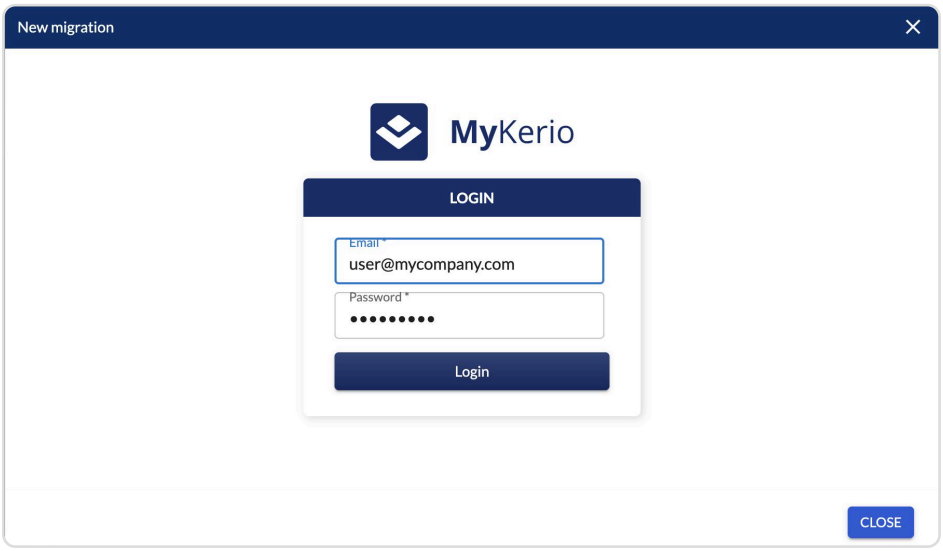


  - Click **SAVE.**

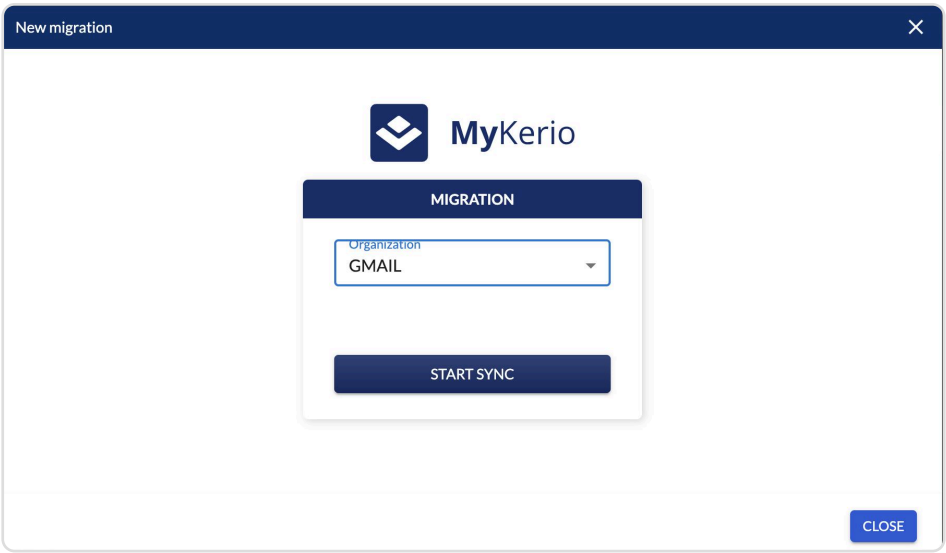
MyKerio

In this section, administrators can migrate from MyKerio to GFI AppManager AI once the GFI KerioConnect® and GFI KerioControl appliances have been upgraded to compatible versions. MyKerio shared definitions can be transferred to GFI AppManager AI with the following steps:

- Click the + NEW MIGRATION and log in to MyKerio.



- Select the relevant Organization and hit “Start Sync.”



- GFI AppManager AI will then display the synced Shared Definitions.

If you have multiple MyKerio accounts, each needs to be migrated individually. By clicking the "Start sync" button, customers can transfer their MyKerio Shared Definitions to GFI AppManager AI. However, migrating appliances and users will need to be done manually. For instructions on how to do this, refer to the Getting Started section.

Alerts

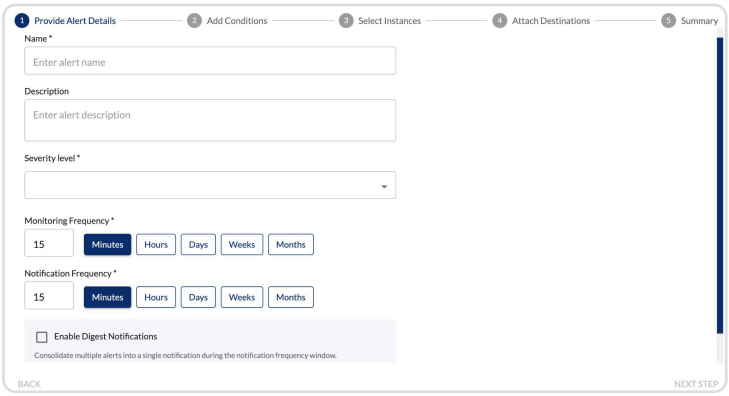
Notifications

Refer to the Notifications section under **Home** in this document.

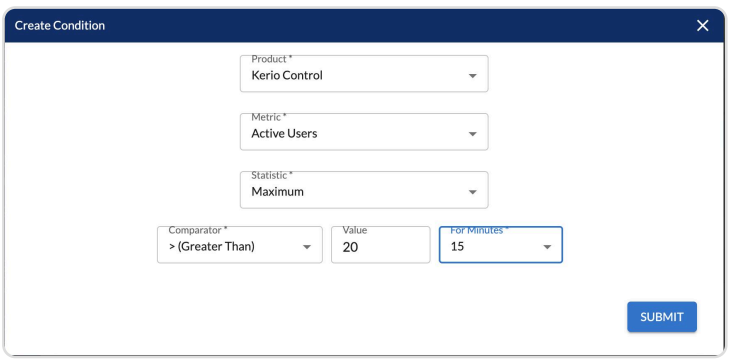
Alerts

Under the Alerts section, you will see a list of all the alerts that have been created, including the name of the alert, the groups that it applies to, and the severity of the alert. From this section, you can edit existing alerts or create new ones.

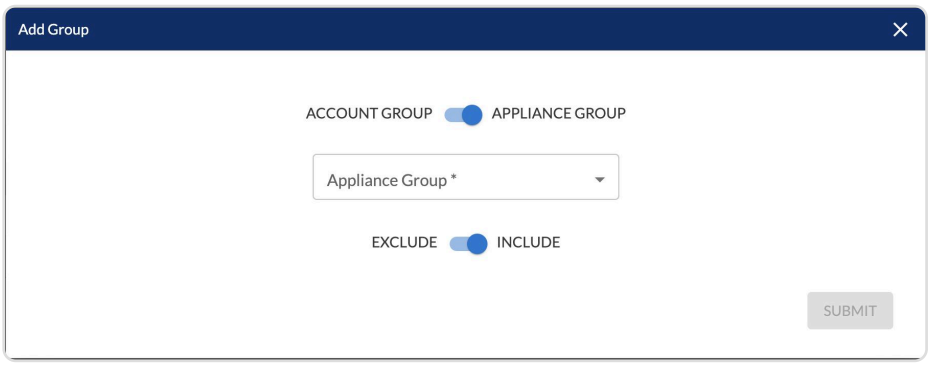
- Create Alerts
  - From the Alerts section, click on + CREATE ALERT .
  - In the following dialog, enter the requested information:
    1. **Name**: Type a name for your alert in the "Enter alert name" box.
    2. **Description**: (Optional) Provide a brief description.
    3. **Severity level**: Click the dropdown and select a severity level (e.g., Low, Medium, High).
    4. **Monitoring frequency:** Enter a number (e.g., 15) and select a time unit (Minutes, Hours, Days, etc.). *Example: 15 minutes means the system checks every 15 minutes*
    5. **Notification frequency:** Enter a number (e.g., 15) and choose the time unit. *Example: 15 minutes means you get notified at most once every 15 minutes*
    6. **Enable digest notifications:** (Optional) Check this box if you want to combine multiple alerts into one message during the notification window.

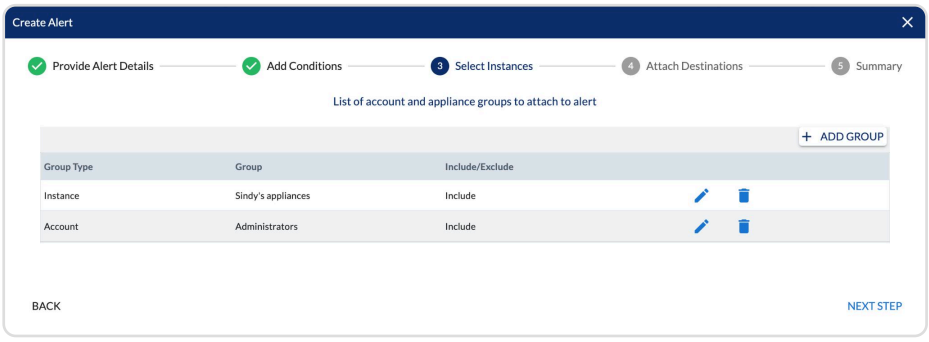


  - In the second step, define the conditions that need to be met for the Alert to be triggered. Click on + CREATE CONDITION to add a new condition. Multiple conditions can be defined using AND/OR logic that must be met for the Alert to be generated.
    1. Choose the product for which you are creating the condition.
    2. Choose the metric you want to monitor and use to trigger the alert.
    3. Select the statistic you want to use: Minimum, maximum, or average.
    4. Select the comparator, the value against which the statistic will be measured, and the length of time the condition should be valid for the alert to be triggered.

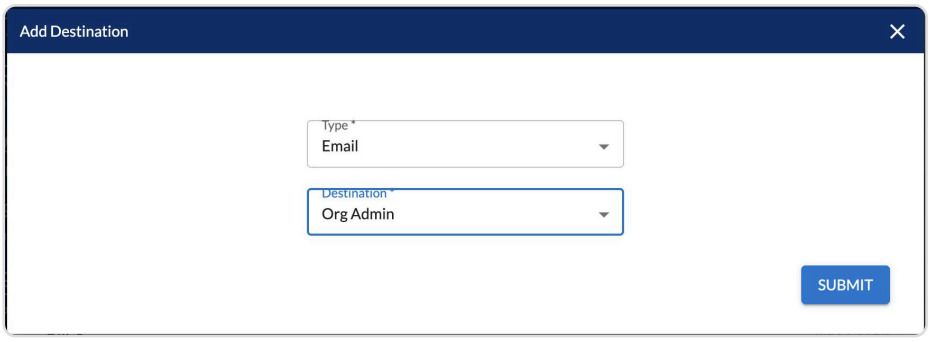


- In the next step, select the appliances that need to meet the conditions defined to trigger the alert. Click on the + ADD GROUP button. Here, you can use Include/Exclude criteria for all appliances and accounts in the groups defined in the Appliance Groups or the Account Groups section. Note that you can have multiple appliance groups or account groups in the same alert.

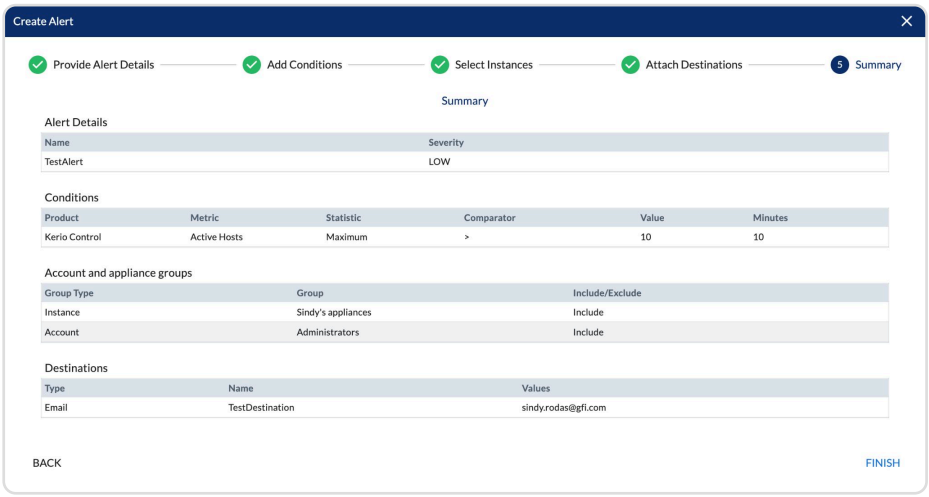




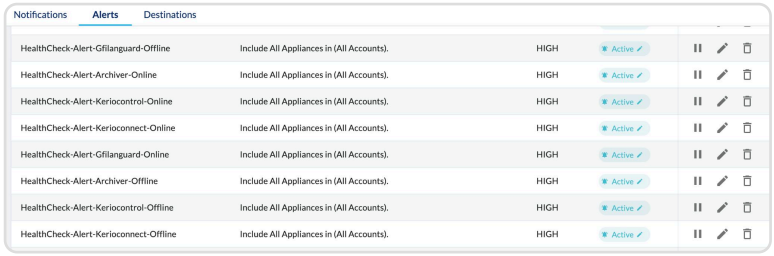
- Next, choose the Destination, which indicates to the GFI AppManager AI whether to send the notification by email and which destinations to include. Click on + ADD DESTINATION . Destinations are defined in the following section of this document.



- The final section will show a summary of the alert. You can click on **finish**, and the alert will be created.



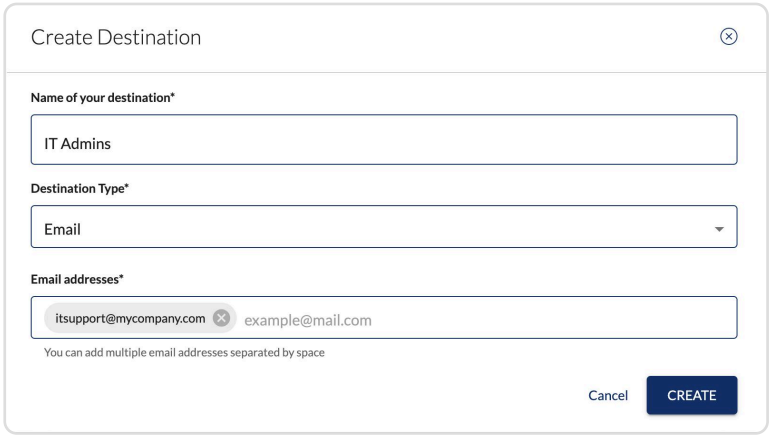
- After creating your alerts, you can view, edit, or delete them directly from the same tab. You also have the flexibility to pause notifications at any time and resume them as needed.



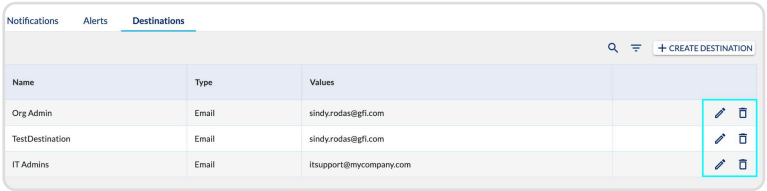
Destinations

Destinations are used when creating Alerts to indicate to the GFI AppManager AI who should be notified whenever the alerts are triggered. From the Destinations section, you can see a list of the destinations that are already created, and you can create more.

- **Create a destination**
  - From the Account groups section, click on + CREATE DESTINATION .
  - In the following dialog, enter the name of the Destination.
  - Select or type the destination: Email
  - Click **Create**.



  - Once a destination has been created, you can edit or delete it from the same tab.



Users

In the **Users** section, you can see users who have been invited to join the organization in GFI AppManager AI. You can see the following information for each user:

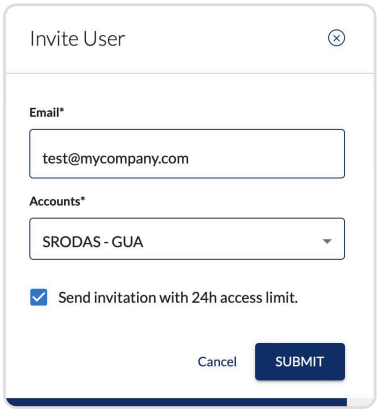
- First Name
- Last Name
- Email
- Status: Active or Invited
- Role: Org Admin or Member
- 2FA Status: Enabled or disabled
- Account Name: Indicates the account the user has access to. It can be the whole organization, or, for MSP configuration, access to a single account within the organization.
- Password expiry status
- Last login: Date of when the user last logged in to GFI AppManager AI
- Created: Date of when the user was created



- Invite a user
  - From the Users section, click on + INVITE USER .
  - In the following dialog, enter the email address of the user and select the organization or account to which the user will be granted access.

    Note: For organizations handling multiple accounts, when a user is added to the main organization, they will gain access to all accounts within that parent organization. If added to a single account, they'll only have access to that specific account. Remember, this setting can't be changed later, so it's crucial to verify the level of access you want to grant before inviting new users.

  - Optionally, you can set the invitation to have a 24-hour access limit.
  - Click **Submit.**



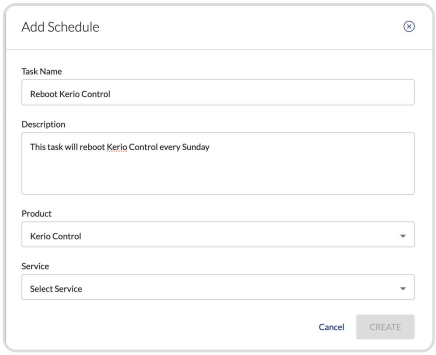
  - Once a User has been invited, you can monitor their status as it changes from “Invited” to “Active” when they accept the invitation.
  - Click on the ☰ icon at the end of each user to perform the following actions:
    1. Delete User
    2. Disable User
    3. Reset Password

Task scheduler

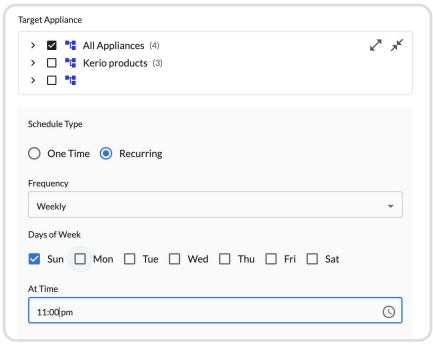
The Task Scheduler feature allows administrators, resellers, and MSPs to automate routine management tasks across appliances and products within their organization. It supports actions such as rebooting devices, activating services, clearing logs, or managing network interfaces on a schedule you define. This helps ensure consistency, saves time, and reduces manual effort.

Creating a scheduled task

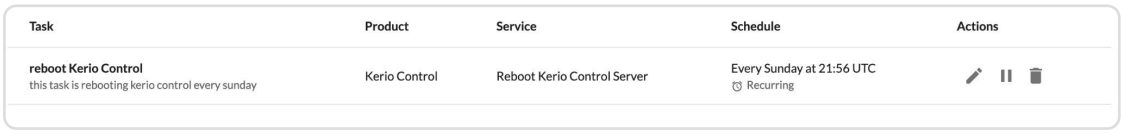
1. Navigate to the Task Scheduler section from the left-side menu.
2. Click Add Schedule to begin creating a new task.
3. Define Task Details:
   - Enter a name for the task (e.g., Reboot GFI KerioControl).
   - Provide a brief description if needed.
4. Select Product and Service:
   - Choose the product the task applies to (e.g., GFI KerioControl).
   - Select the service action, such as:
     1. Reboot GFI KerioControl Server
     2. Enable/Disable network interface
     3. Disconnect VPN clients
     4. Clear logs
     5. Choose Target Appliances or Accounts



5. Select specific appliances or apply to all matching product types.
6. Set the Schedule:
   - Choose between One-Time or Recurring tasks.
   - For recurring tasks:
     1. Set the frequency (e.g., Weekly)
     2. Choose the day (e.g., Sunday)
     3. Set the exact time (e.g., 11:56 PM)



7. Create the Task:
   - Click Create to activate the schedule.
   - The task is now listed and will execute automatically as defined.



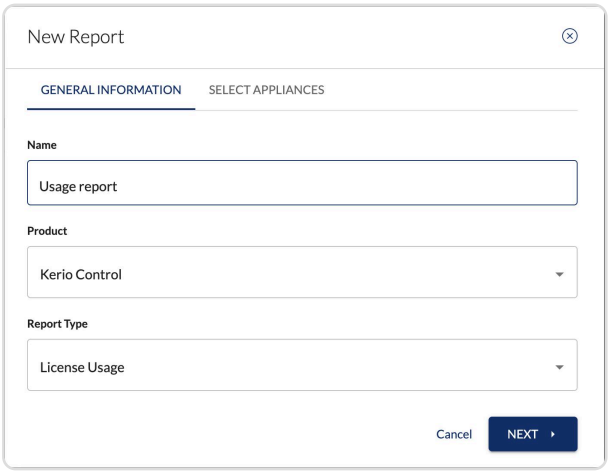
From here, you can edit, pause, or delete the tasks.

Reports

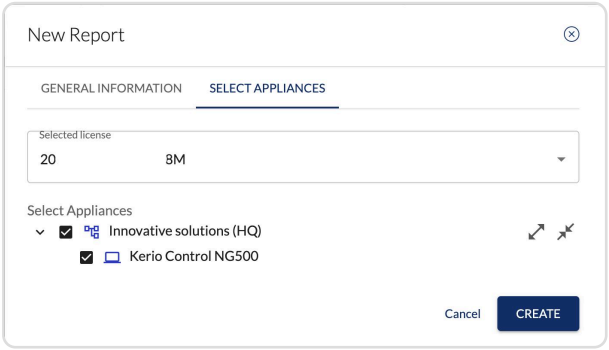
The Reporting feature enables Managed Service Providers (MSPs) to gain real-time visibility into license usage across multiple deployments using the same license key. This solves a key challenge in the GFI KerioControl MSP licensing model, which is billed based on the peak usage across all connected appliances. MSPs can now proactively monitor and report usage throughout the month, down to the level of individual customer deployments.

How to create a report

1. Access the reports section in the left-side menu.
2. Click the **Add** button in the top right corner to start creating a new report.
3. Define Report Details:
   - Enter a **name** for the report (e.g., NG 300 Usage Report).
   - Select the **product** (e.g., GFI KerioControl, GFI LanGuard).
   - Choose **License Usage** as the report type.



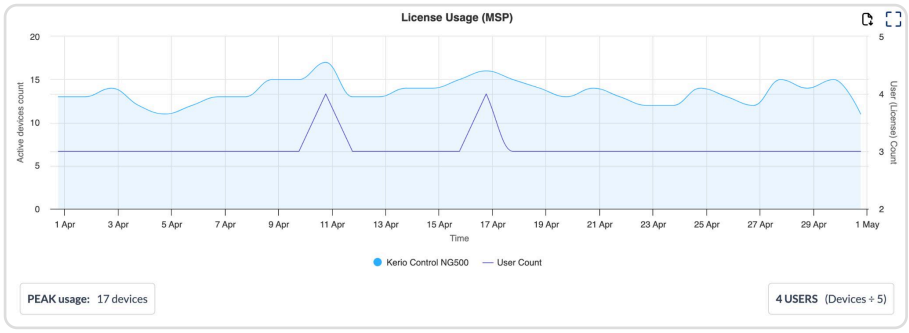
4. Select Licenses and Appliances:
   - GFI AppManager AI will show all available licenses.
   - Select the specific license you want to track.
   - Choose the GFI KerioControl (or GFI LanGuard) appliances using this license. You can select multiple deployments even if they are on different customer sites.



5. Create the Report:
   - Click **Create**. Your report will be generated and listed in the Reports dashboard.

6 View and Analyze the Report:

- Click on the report name to open it.
- Review total license usage, peak usage, and breakdowns by customer (based on deployment).
- Use the interactive graphs to filter data by deployment or customer.

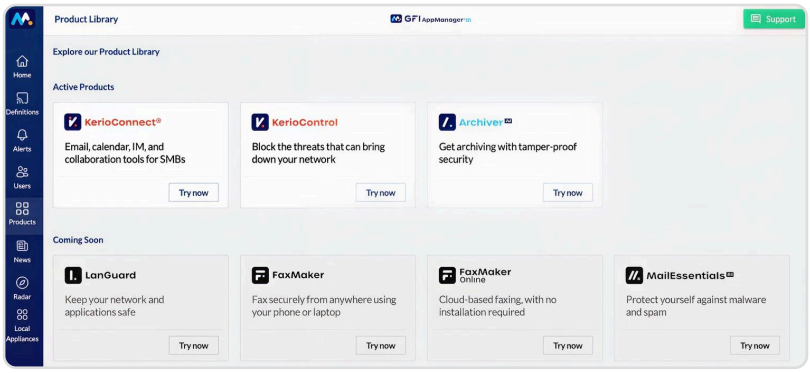


7 Use the Report for Billing:

- Use the detailed graphs to understand which customers consumed how many seats. The green graph shows the billable usage, while the blue and other colored graphs show customer-specific consumption. This allows transparent billing based on real data.

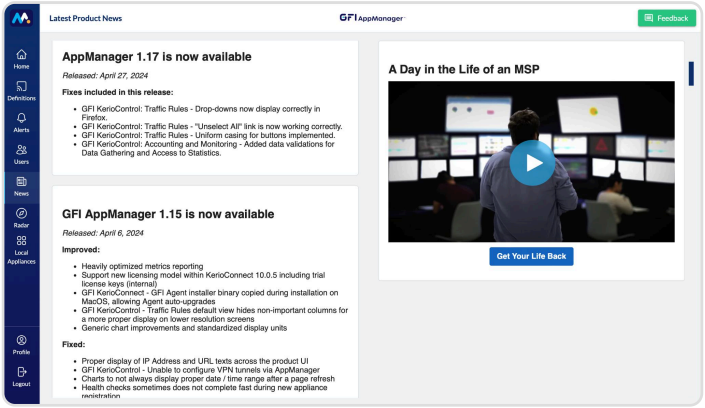
Products

In this section, you can explore GFI's product library. The "Active Products" section includes products already available in GFI AppManager AI, along with a preview of upcoming products. Additionally, you can access and try all the products in the GFI portfolio from here.



News

In the News section, you can find the Latest Product information. When you spot an exclamation mark on the news icon, it means there is unread news waiting for you. We suggest checking the news regularly to stay up to date on the latest releases and product info.



Profile

In the profile section, you can manage your account's security settings. Here, you can set or update your password to ensure the confidentiality of your account. Additionally, you can enable two-factor authentication, which adds an extra layer of security by requiring a secondary verification method, such as a unique code sent to your mobile device, to access your account. This helps safeguard your account against unauthorized access and enhances overall security.

Setting up Two-Factor Authentication

1. Install one of the following applications on your mobile device:
   - FreeOTP
   - Google Authenticator
2. Scan the QR code displayed on GFI AppManager AI.
3. Enter the one-time code provided by the application and click **Submit** to finish the setup. You can also add a device name to help you manage your OTP devices.

Passkey Registration

Passkeys let users register a device-based credential instead of using a password. This reduces the risk of stolen credentials or phishing attacks.

1. Go to **Profile > Authentication > Passwordless.**
2. Click on **Set up Passkey > Register.**
3. Add a label to identify the device, then click **OK**.



Passkey Authentication

Users who have registered a passkey can log in using their device credentials instead of a username and password.

1. On the GFI AppManager AI login page, enter your email address and click on **Sign in.**
2. This screen will prompt for the password. Below the Sign in button, click the option **Try another way.**
3. This will display the option to sign in using a security key.
4. Click on **Sign in with security key.**
5. Complete the device's authentication method (fingerprint, PIN, etc.).



Manage

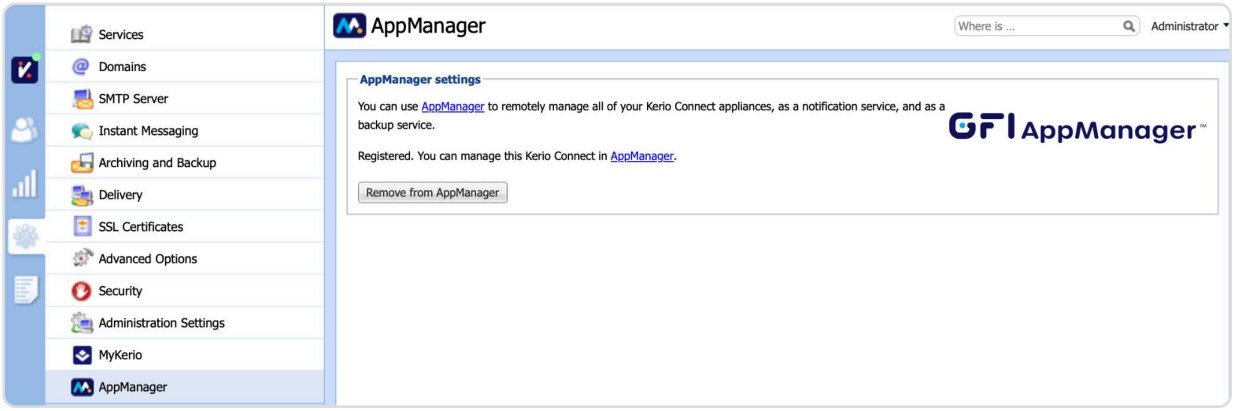
Under Profile > Manage, you can customize GFI AppManager AI attributes for your console like the following:

1. **Primary custom logo**: Specify the custom logo to be used on the majority of pages where branding appears. File size is limited to 256KB, accepted types are jpeg, png or svg.
2. **Secondary custom logo**: Specify a smaller custom logo for the side menu bar where branding appears. File size is limited to 256KB, accepted types are jpeg, png, or svg.
3. **URL to be used for the news page**: URL to be used for the News page. The content will also be displayed for organizations that the current organization manages.
4. **Auto-Logout settings**: You'll be logged out after this period of inactivity (with a 5-minute warning). The accepted value is between 15 and 120 minutes.

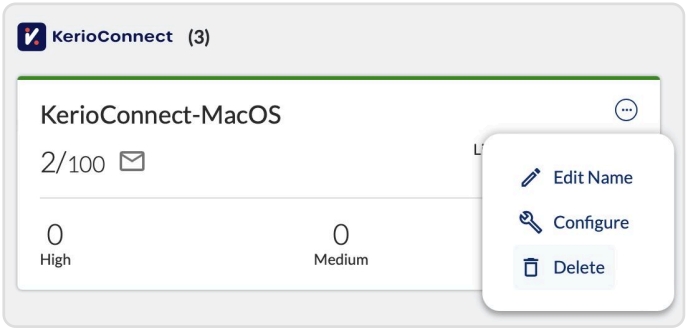
Removing from GFI AppManager AI

To efficiently remove an appliance from GFI AppManager AI, it's crucial to adhere to a specific set of steps:

1. Trigger Removal from Within the Appliance's Administrator Interface:
   - Access the Administrator interface of the appliance you wish to remove.
   - Navigate to the GFI AppManager AI section.
   - Click on “Remove from AppManager”



2. Delete the Appliance from GFI AppManager AI:
   - Once you've triggered the removal process from within the appliance's interface, proceed to GFI AppManager AI.
   - Locate the appliance you just removed from the unit. This can be found in the list of managed appliances.
   - Identify the specific appliance you want to delete, then select the three-dot menu associated with it.
   - From the dropdown menu, choose the "Delete" option.
   - Confirm the deletion when prompted to finalize the appliance's removal from GFI AppManager AI.



GFI AppManager AI Settings

In the GFI KerioControl Administration interface, the GFI AppManager AI settings allow you to:

- Enable or disable communication with GFI AppManager AI.
- Check the version of the GFI Agent currently running in the GFI KerioControl deployment.
- Restart the agent.
- Completely stop the agent.

This is especially useful when communication issues occur between the GFI KerioControl deployment and GFI AppManager AI.

GFI AppManager AI

The AI add-on is a new feature of GFI AppManager AI, the centralized platform for managing multiple GFI products, including GFI KerioControl, GFI KerioConnect®, GFI Archiver AI, and others. The add-on lets users retrieve information and manage appliances without having to search through documentation manually.

Who can access it?

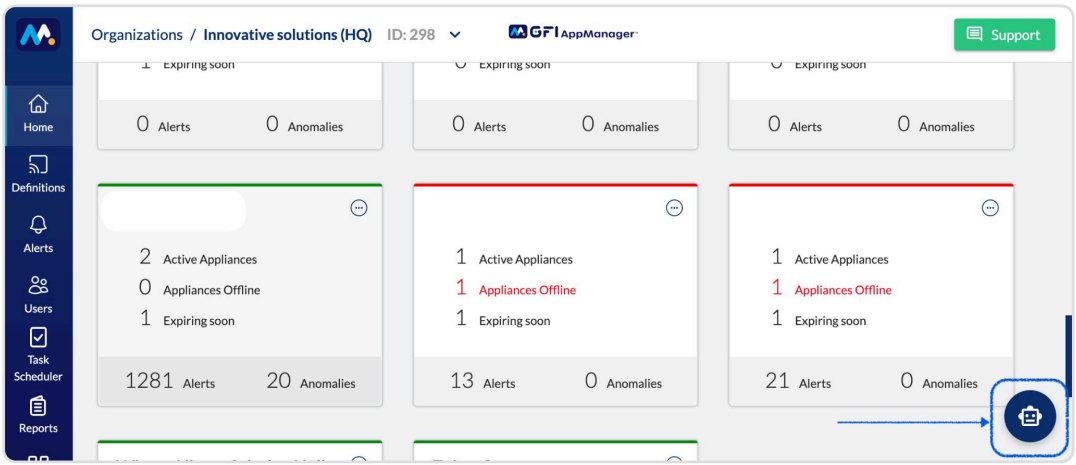
- **Resellers**: GFI AppManager AI is available for resellers managing multiple customer accounts.
- **Reseller Teams**: Any colleague within a reseller organization with access to GFI AppManager AI can use the AI add-on.
- **Customers**: Available to those with at least **one appliance,** though the benefits increase significantly for those managing multiple appliances.

Licensing

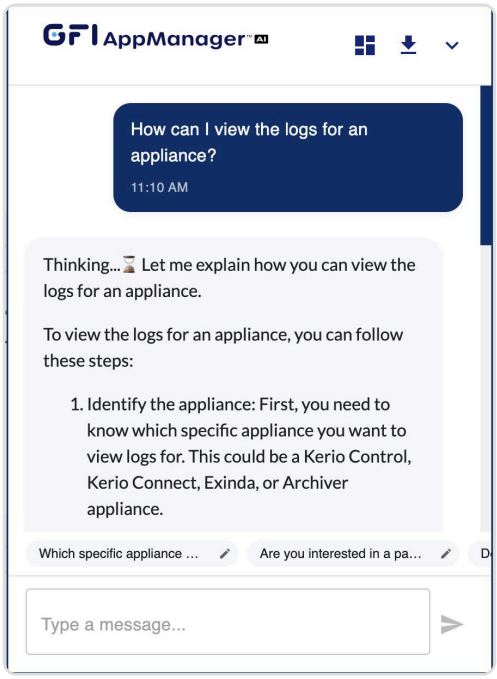
The AI add-on is licensed per GFI AppManager AI instance. It is available for resellers and customers managing multiple appliances. It is not included in the standard GFI AppManager AI package and must be purchased separately.

How to use the AI add-on

Once the AI add-on is enabled for your organization, a floating button will appear in the lower-right corner of your browser window when GFI AppManager AI is open.



Click the button to open the assistant window, where you can ask questions about your organization and the products registered in GFI AppManager AI.

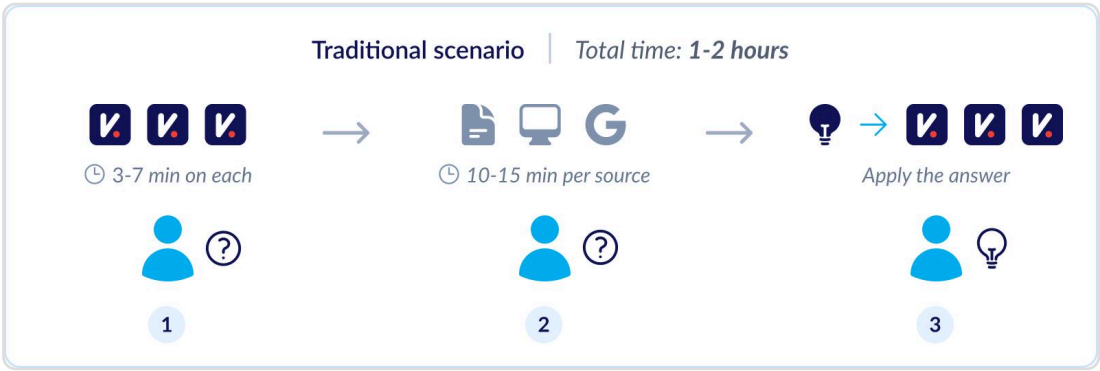


Sample use case

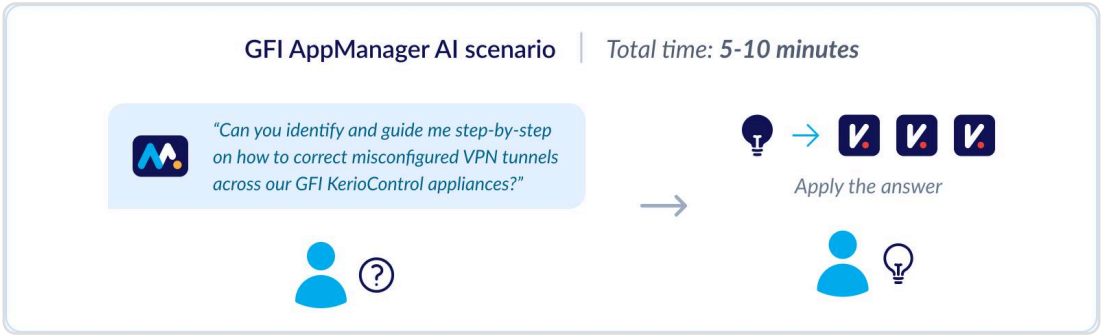
Issue: Identify misconfigured VPN tunnels in the managed GFI KerioControl appliances and fix them.

Traditional scenario:

- Check each GFI KerioControl Appliance, and review whether it has VPN tunnels configured.
- If the setting isn't obvious or there is a lack of prior knowledge of VPN tunnels, the user also needs to read the documentation.
- After some time, the user will find the answer and proceed to apply it to all the appliances they manage.



With GFI AppManager AI:



What's beyond the AI capabilities?

The AI add-on gives fast, accurate answers, but it won't:

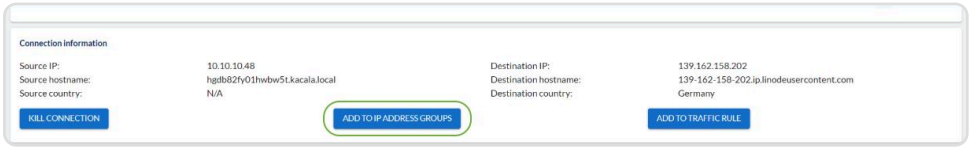
- **Perform actions:** It guides users but does not change configurations.
- **Replace expert decision-making:** It offers suggestions, but complex security or networking decisions still require human expertise.

GFI KerioControl Management

Note: Some of these features are exclusively available through GFI AppManager AI and are not included in the local administrator interface of GFI KerioControl.

1 Adding an IP address to an IP address group

1. Navigate to the GFI KerioControl device homepage via GFI AppManager AI.
2. Select 'Status' > 'Active Connections' from the left menu.
3. Identify the desired active connection and click on it.
4. At the bottom of the page, click 'Add to IP address groups'.



5. Select either the source or destination IP address group.
6. Click 'Save'.

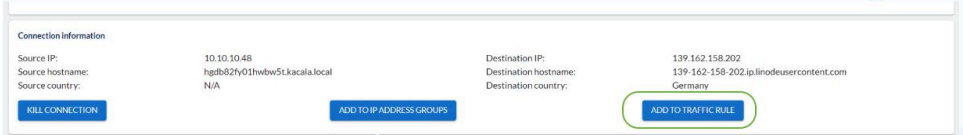


7. To confirm, return to the homepage, go to 'Definitions' > 'IP address groups', and verify the addition.

Note: IPs added this way will be marked "Enabled via active connections".

2 Adding an IP address to a traffic rule

1. Access the GFI KerioControl device homepage through GFI AppManager AI.
2. Click on 'Status' > 'Active Connections' from the left menu.
3. Select the relevant active connection.
4. Scroll down and click 'Add to Traffic Rule'.



5. Choose the appropriate source or destination Traffic group.
6. Click **Save.**



7. To confirm the addition, navigate back to 'Configuration' > 'Traffic Rules' and check the specified Traffic Rule.

3 ShieldMatrix UI

The Shield Matrix UI provides a visual map of network security rules for GFI KerioControl. It shows allowed and blocked traffic paths between network segments, making it faster to review and adjust security rules.

How to Access and Use:

1. In the GFI AppManager AI dashboard, go to your **GFI KerioControl** appliance.
2. Select **Configuration > Shield Matrix** from the side menu.
3. Go to the Status and Configuration tab. From here, you can:
   - Enable or disable the Shield Matrix.
   - Set actions for high-, medium-, and low-confidence threats.
   - Enable automatic updates.
   - Specify how often to check for updates, in minutes.
4. Go to the Connections tab. From here, you can monitor Shield Matrix connections as follows:
   - Timestamp
   - Source IP addresses
   - Destination IP addresses
   - Protocol
   - Hit count
   - Threat confidence level
   - Action taken (logged/dropped)

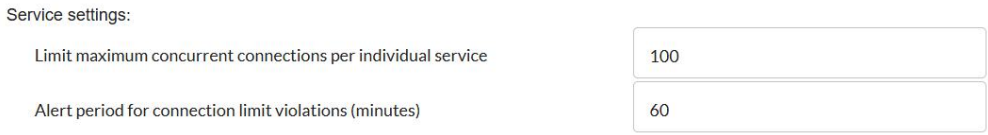
   You can see whether the traffic was dropped, the severity, the source IP, and the timestamp.

4 Maximum concurrent connections

GFI AppManager AI's configuration options for GFI KerioControl allow administrators to set the maximum number of concurrent connections for each service or protocol. This value specifies how many active sessions a service or protocol (for example, DNS, HTTP, or SMTP) can accept simultaneously.

By default, services are configured with a limit of 100 concurrent connections. You can increase this value based on workload requirements. For instance, setting the DNS limit to 300 allows GFI KerioControl to handle 300 simultaneous DNS connections.

Note:
- Configuration is applied per service/protocol.
- Higher values may increase resource utilization.



GFI KerioConnect® Management

DKIM Validation

This feature checks if incoming emails have valid DKIM signatures.

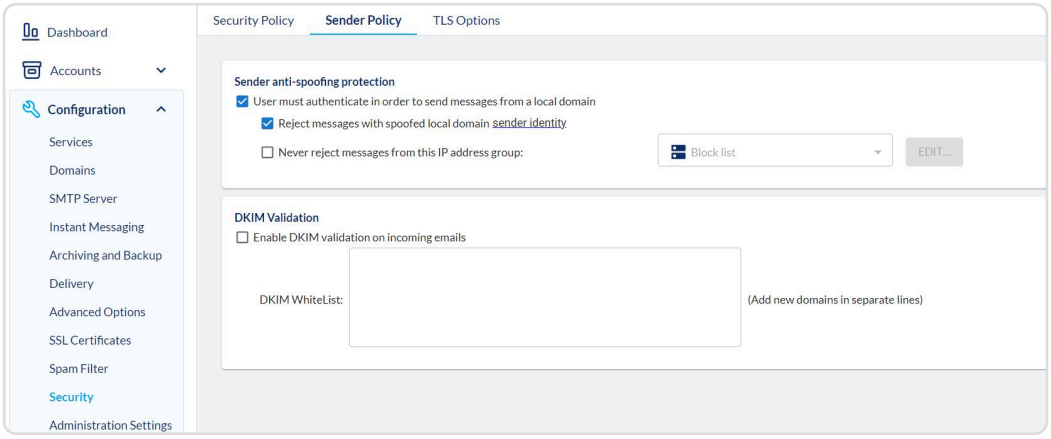
You can control this feature via configuration changes in the mailserver.cfg using the following variables:

```
<variable name="EnableDKIMValidation">1</variable>

<variable name="DKIMDomainWhiteList">gmail.com,hotmail.com</variable>
```

1. The first variable turns the feature on or off. By default, DKIM Validation is disabled because many domains still do not support it. (You can configure DKIM for your domains in GFI KerioConnect®; more information is available here.)
2. The second variable allows you to whitelist specific domains for your organization by listing them in a comma-separated format.

This can be enabled automatically in GFI AppManager AI (after upgrading to 10.0.6 build 8452 or later) by going to your **GFI KerioConnect® > Configuration > Security > Sender Policy.**



Note: Many domains still don't have DKIM configured, so monitor email traffic after you enable this feature to avoid service disruption.

Support

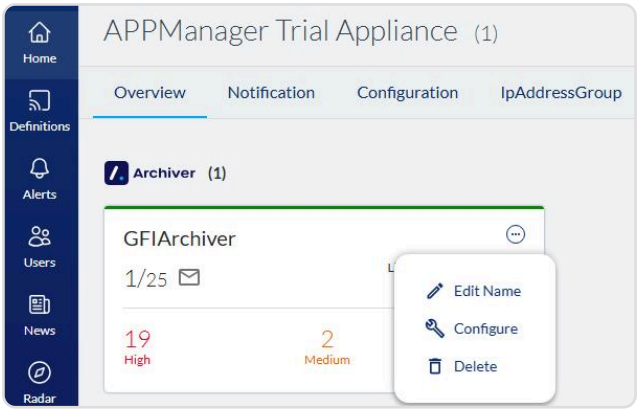
If you encounter any issues, you can refer to the following articles to reset the registration on GFI KerioConnect or GFI KerioControl.

- Resetting GFI KerioConnect®'s Connection to GFI AppManager AI: A Step-by-Step Guide
- Resetting GFI Agent Integration with GFI KerioConnect® on macOS
- Resetting GFI KerioControl's Connection to GFI AppManager AI

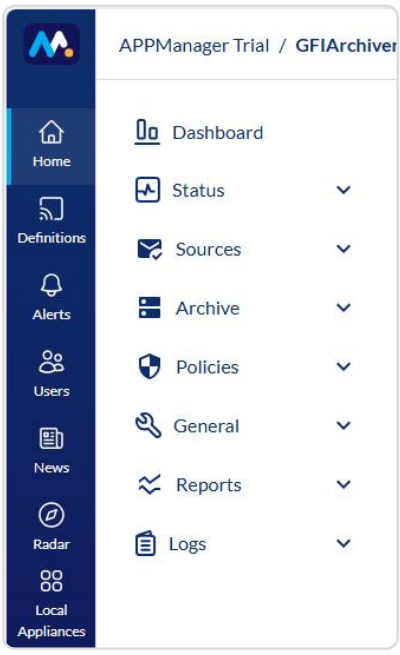
If you still face issues after following the above steps, refer to the article "Gathering_Information for Troubleshooting GFI AppManager AI Issues" to collect the necessary details needed to open a support ticket.

GFI Archiver AI Management in GFI AppManager AI

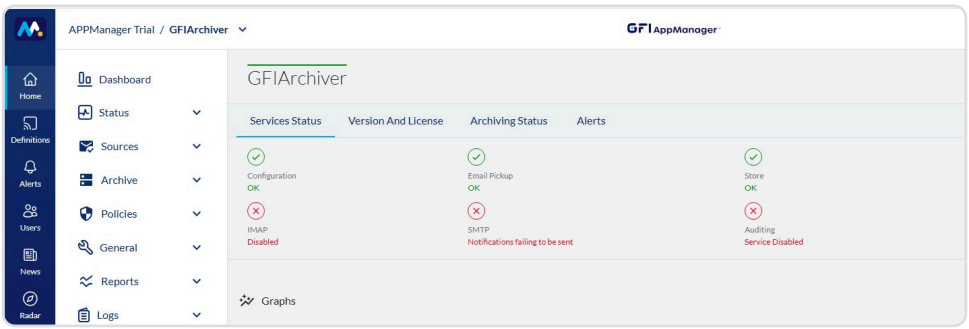
GFI Archiver AI can be easily managed from the GFI AppManager AI. Simply click on configure, as shown in the image.



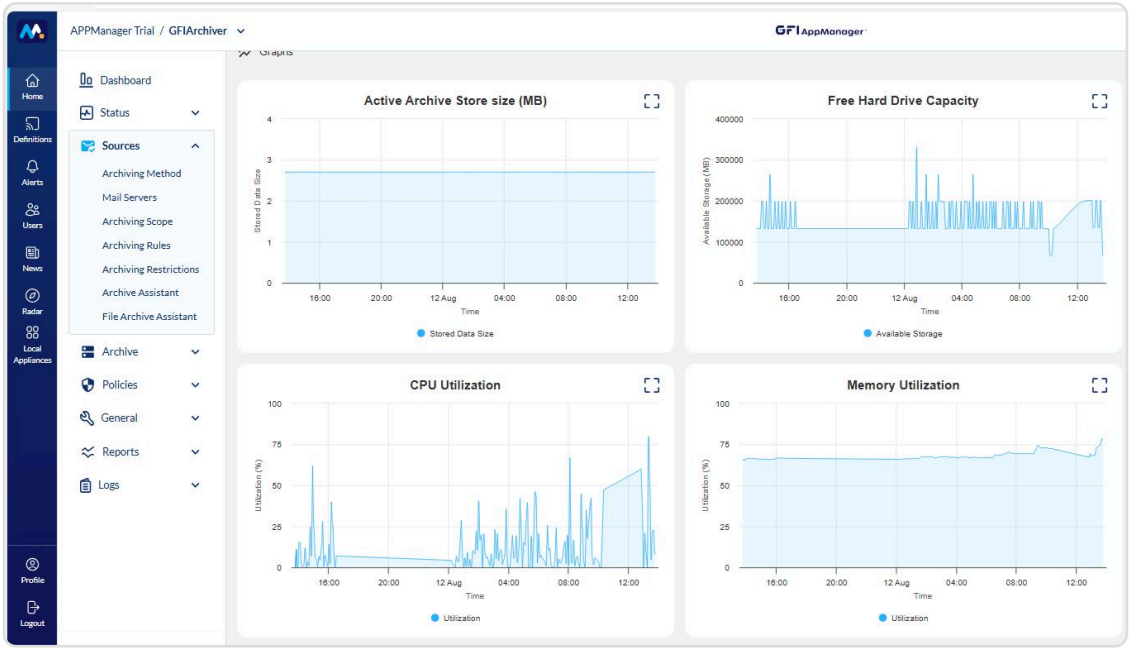
Clicking on “Configure” opens a new sidebar, as shown in the image below. You can manage your GFI Archiver AI from this sidebar. Clicking on the dropdown arrows will give you access to more features.



See the details of the status of your GFI Archiver AI in the Dashboard on GFI AppManager AI.



From within GFI AppManager AI, you can control your GFI Archiver AI with the dropdowns.



Note:

1. Registration of GFI Archiver AI to GFI AppManager AI is required to use the AI add-on.
2. Refer to the GFI Archiver AI admin guide for the GFI AppManager AI integration.

Get help

If you have questions or run into issues with GFI AppManager AI, open a support case on our Support portal. Knowledge base articles and FAQs are available there, too.

Copyright © GFI USA, LLC, All rights reserved.