



PeerIQ Manual

support@peersoftware.com

©1993-2025 Peer Software, Inc. All Rights Reserved

Updated December 2, 2025

Contents

1	Purpose of this Guide	7
2	Product Overview	8
2.1	Licensing	8
2.2	Deployment	8
3	Requirements	10
3.1	Hardware Requirements	10
3.1.1	Basic License	10
3.1.2	Advanced License	10
3.2	Hardware Settings	10
3.3	Software Requirements	11
4	Logging into PeerIQ	12
4.1	Managing Your PeerIQ Account	14
4.1.1	Changing Your Password	15
4.1.2	Updating Your Email Address	16
4.1.3	Managing Notification Preferences	16
4.1.4	Changing Your Time Zone Settings	16
4.1.5	Setting Your Session Timeout	17
4.2	Notifications	17
4.2.1	Accessing Notifications	18
4.2.2	Notifications Page	18
5	Setting Up Communication between the PMC and PeerIQ	19

5.1	Configuring PeerIQ's Connection to a Peer Management Broker	19
5.1.1	Typical Broker Deployments	19
5.1.2	Configuring the Broker Connection	23
5.1.3	Stopping Attempts to Connect to a Broker	24
5.1.4	Connection Issues	25
5.2	Enabling Peer Management Center to Send Data to PeerIQ	25
6	Monitoring the PeerGFS Environment	28
6.1	Using the Environment Monitoring Page Controls	28
6.2	Overview Page	28
6.2.1	Overview Page Cards	29
6.2.2	Modifying Thresholds	32
6.3	PMC Page	32
6.3.1	PMC Page Cards	33
6.4	Jobs Page	36
6.4.1	Job Page Cards	37
6.5	Agents Page	39
6.5.1	Agents Page Cards	39
6.6	Volumes Page	41
6.6.1	Volumes Page Cards	42
6.7	Watch Set Page	43
6.7.1	Watch Set Page Cards	44
6.8	License Page	45
6.8.1	License Page Card	45
7	Analyzing Your File Systems	47

7.1	Environment Monitor Configuration	47
7.1.1	Managing Environment Monitor Data	47
7.2	Using the FSA Page Controls	48
7.3	Extensions Page	48
7.3.1	Extensions Page Cards	49
7.4	Data Aging Page	52
7.4.1	Data Aging Page Cards	53
7.5	Hot Data Analysis Page	56
7.5.1	Hot Data Analysis Cards	57
7.6	Scans Page	61
7.6.1	Scans Page Cards	62
7.6.2	Viewing Detailed Scan Information	63
7.6.3	Viewing Detailed Host Information	64
7.6.4	Viewing Detailed Volume Information	65
7.7	File System Analytics Configuration	65
7.7.1	Process Scan Data	66
7.7.2	File System Analytics Data Retention	66

8 Analyzing File Activity 68

8.1	Users Page and Clients Page	68
8.1.1	Client Hostname or IP Address	69
8.2	Using the FAA Page Controls	69
8.2.1	Users Page and Clients Page Cards	70
8.2.2	Selected Volumes	71
8.2.3	All Users/Clients Activity Over Time	71

8.2.4	Users/Clients Activity Breakdown	71
8.3	User Activity Page and Client Activity Page	72
8.3.1	User Activity Page and Client Activity Page Cards	73
9	Activity Page	76
9.1	Overview	76
9.2	Filters	76
9.2.1	Date & Time	77
9.2.2	Users	77
9.2.3	Clients	77
9.2.4	Storage	78
9.2.5	Files & Folders	78
9.2.6	Activity Types	79
9.3	Summary + Report	80
9.4	Unsaved and Saved Reports	80
9.4.1	Unsaved Reports	81
9.4.2	Saved Reports	81
10	File Activity Report	82
10.1	Overview	83
10.1.1	Viewing truncated values with the eye icon	83
10.2	Users & Clients	83
10.3	Storage Hosts & Volumes	84
10.4	Files & Folders	84
10.5	Events	84
10.6	Exported Data	85

10.7	File Activity Analytics Configuration	85
10.7.1	File Activity Analytics Data Retention	85
10.7.2	File Activity Analytics Anomaly Detection	86
10.7.3	File Activity Analytics Real-Time Data	86
11	Administering PeerIQ	88
11.1	Broker Configuration Page	88
11.2	Email Configuration Page	88
11.2.1	Overview	89
11.2.2	SMTP Configuration Fields	89
11.2.3	Authentication Methods	90
11.2.4	Example: Office 365 Configuration	92
11.2.5	Configuring Office 365 / OAuth 2.0 in Microsoft Entra ID	92
11.2.6	Authorization and Redirect	94
11.2.7	Testing the Configuration	94
11.3	LDAP Configuration	95
11.3.1	Configuring Access for LDAP Users	96
11.3.2	Resolving NFS Usernames using the Resolve LDAP Information option	100
11.3.3	Resolving Active Directory (AD) Departments using the Resolve LDAP Information option	102
11.4	Logs Page	103
11.4.1	Filtering Log Contents	104
11.4.2	Sending Diagnostics	105
11.4.3	Saving Diagnostics	106
11.5	Software Status Page	106
11.6	Software Updates Page	107

11.6.1	Software Updates Page Cards	108
11.6.2	Updating PeerIQ	109
11.7	System Configuration Page	112
11.7.1	Resetting Configuration Options	112
11.7.2	Delete All Analytics Data	113
11.7.3	Managing Time Zone Settings	113
11.7.4	Session Timeout	113
11.7.5	Configuration	113
11.8	System Stats Page	114
11.8.1	Using the System Stats Page Controls	114
11.8.2	System Stats Page Cards	115
11.9	User Accounts Page	116
11.9.1	Adding and Removing Users	117

1 Purpose of this Guide

The purpose of this guide is to familiarize you with the process of deploying and configuring PeerIQ and introducing you to using PeerIQ. If you experience any issues, please visit <https://servicedesk.jira.peersoftware.com>.

2 Product Overview

PeerIQ is a comprehensive monitoring tool designed to provide real-time and historical insights into your Peer Global File Service (PeerGFS) environment and storage. It captures three types of data:

- **Environment Monitoring Data**

PeerIQ enables users to effectively monitor their jobs, Peer Management Center (PMC), connected Agents, and volumes, with the ability to store up to four weeks of history.

- **File System Analytics**

PeerIQ enables analysis of volumes connected to Agents, offering insights into the content of your storage over time and across your PeerGFS environment.

- **File Activity Analytics**

PeerIQ enables analysis of user activity across volumes, giving insight into user behavior across your PeerGFS environment.

2.1 Licensing

PeerIQ is available in two licensing levels: Basic and Advanced. Each license level determines the depth of analytics and insights available within the application.

- **Basic License:** Provides access to all Environment Monitoring and File System Analytics data. Within File Activity Analytics, only aggregated statistics are available, offering a summarized overview of user and client activity across the environment.
- **Advanced License:** Includes all functionality of the Basic license, with the addition of full real-time activity logging as well as detailed user and client analytics across all monitored storage environments. This level also enables ML-based anomaly detection, which identifies patterns of user or client behavior that deviate from typical activity.

Note: Please Contact Peer Software to discuss upgrading your license level.

2.2 Deployment

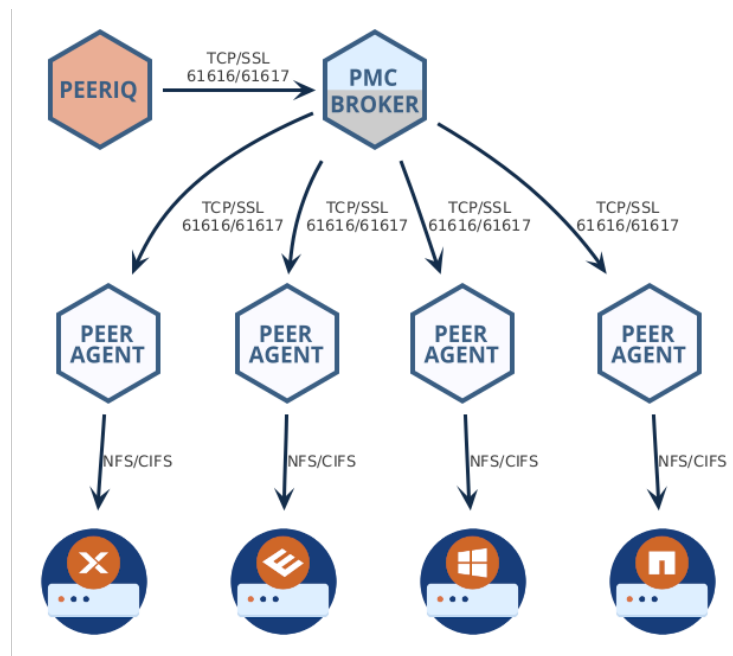
PeerIQ is a web-based application and is deployed via a virtual appliance. The PeerIQ virtual appliance is compatible with various platforms, including:

- Hyper-V on Windows Server 2019, 2022, and 2025

- VMware ESXi 6.7, 7.0, and 8.0
- Nutanix AHV

The virtual appliance enables easy deployment and use, reducing the setup and configuration time required.

PeerIQ seamlessly integrates with your existing PeerGFS environment, connecting to your PeerGFS system using the same broker network that links the PMC and Agents. This connection utilizes the same SSL and TCP connections on ports 61616 and 61617, ensuring secure communication between the various Peer components in your environment.



3 Requirements

3.1 Hardware Requirements

The PeerIQ virtual appliance is a preconfigured virtual machine image.

The specifications below represent the **minimum requirements** for deployment. Depending on the scale of your PeerGFS environment, data volume, and the number of monitored users or clients, additional resources may be required to maintain optimal performance.

3.1.1 Basic License

- A minimum of 4 CPU cores.
- 8 GB RAM.
- 120 GB virtual disk.

Note: The virtual disk should be **thick provisioned**, and **high-performance SSD storage** is recommended to ensure smooth operation.

3.1.2 Advanced License

- A minimum of 8 CPU cores.
- 16 GB RAM.
- 1.5 TB virtual disk, required to store approximately three months of real-time activity data.

Note: The virtual disk should be **thick provisioned**, and **high-performance SSD storage** is recommended to ensure smooth operation.

3.2 Hardware Settings

For proper operation, it is crucial to ensure time synchronization between the PMC, Agents, NAS platforms, and the virtual appliance server. By default, the PeerIQ appliance utilizes NTP (Network Time Protocol) and synchronizes with ubuntu.pool.ntp.org to maintain accurate time.

However, if you are using an ESXi appliance, it is important to note that host guest time synchronization is enabled and takes precedence over NTP time. This means that time synchronization within the ESXi environment will be prioritized.

3.3 Software Requirements

The PeerIQ application is a web-based application that can be accessed using one of the following browsers:

- Mozilla Firefox
- Microsoft Edge
- Google Chrome

4 Logging into PeerIQ

This section describes logging into PeerIQ for the first time. After logging in for the first time, you must immediately change your password and then log in again.

To log into PeerIQ:

1. Open a web browser.
2. Navigate to the PeerIQ web interface:
 - For Virtual Appliances: The PeerIQ interface is typically accessible at `https://<Appliance IP or Hostname>`. If you are unsure of your appliance's IP address, you can retrieve it from either:
 - Your hypervisor's management interface.
 - The console of the PeerIQ virtual appliance itself.
 - For Red Hat or Rocky Installations: The PeerIQ interface is typically accessible at `https://<Server IP or Hostname>:4430`. The port 4430 is set by default but can be modified during the installation of PeerIQ.

```
Welcome to the PeerIQ VM.
* Support:      https://www.peersoftware.com/support/
* Knowledge Base: https://kb.peersoftware.com/peerkb/

Web Login https://172.16.0.41/

* Username: admin
* Password: password

Please login to the VM using the console below to configure
system settings.

Console Default login

* Username: peersoftware
* Password: password

Ubuntu LTS PeerIQ000c2973f5f9 tty1
PeerIQ000c2973f5f9 login: _
```

3. In the login page, enter the default credentials: **admin** and **password**.

4. Click **Submit**.

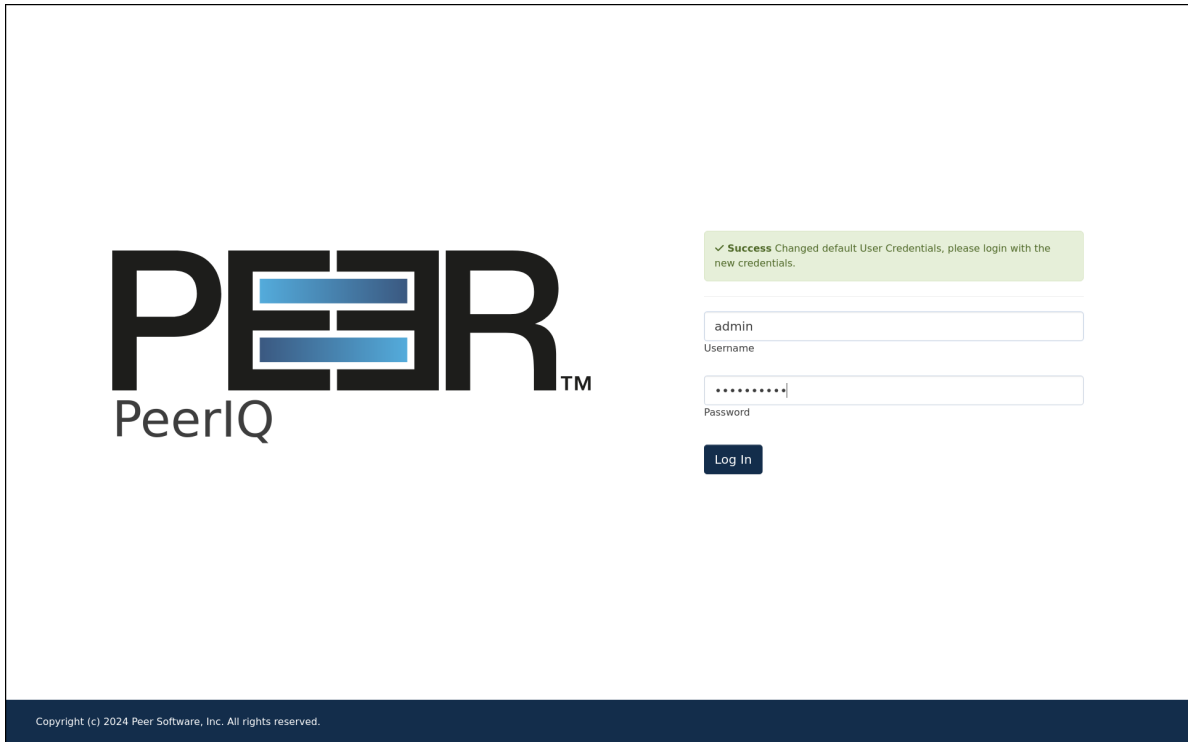
The End User License Agreement (EULA) is displayed on the login page the first time you log in. You must accept the EULA to use PeerIQ.

5. Click the **Accept terms and conditions** checkbox to accept the license agreement.

6. Change the default username and password of the default Administrator account.

A password must be at least eight characters in length, contain at least one number, one uppercase character, one lowercase character, and a special character (such as %, \$, #, {, }, ~, ^, \, &).

Once you have accepted the EULA and successfully changed the login credentials, the login page is redisplayed with a success message.



The screenshot displays the PeerIQ login interface. On the left is the PeerIQ logo, consisting of the word "PEER" in a large, bold, black font with a blue horizontal bar across the middle of the "E", and "PeerIQ" in a smaller, black font below it. To the right of the logo is a green success message box that reads: "✓ Success Changed default User Credentials, please login with the new credentials." Below this message are two input fields: the first is labeled "Username" and contains the text "admin"; the second is labeled "Password" and contains a series of dots. A blue "Log In" button is positioned below the password field. At the bottom of the page, a dark blue footer bar contains the text: "Copyright (c) 2024 Peer Software, Inc. All rights reserved."

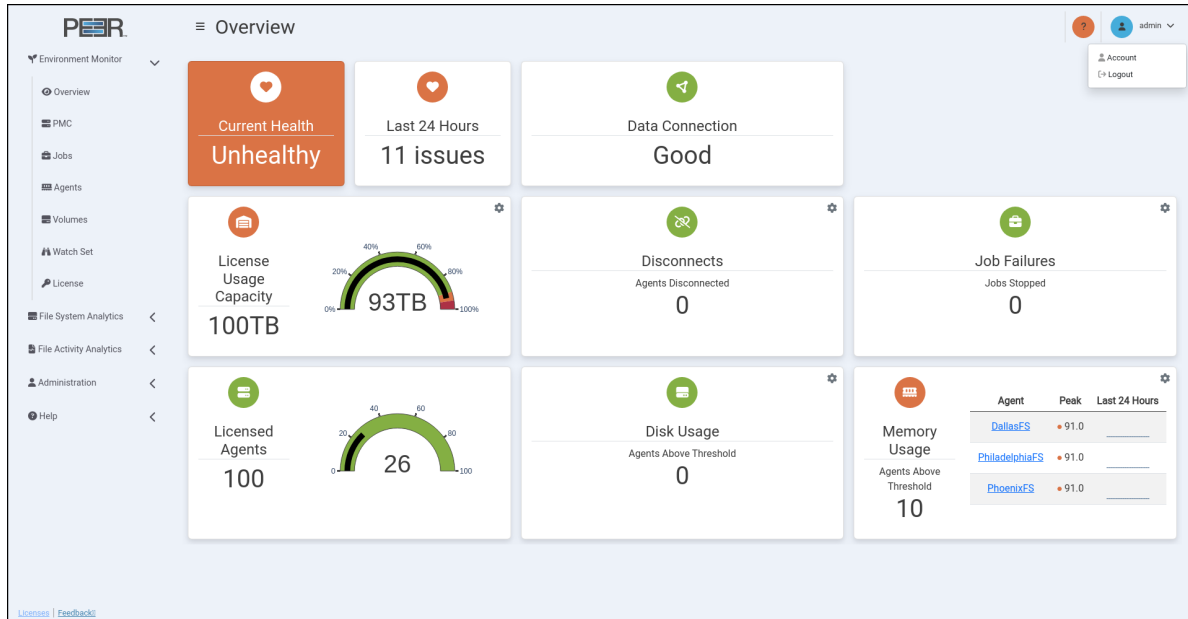
7. Log in again using your new password.

4.1 Managing Your PeerIQ Account

You can manage your PeerIQ account on the **Account** page, including changing your password and account details, adjusting your time settings and updating your preferences.

To access your account:

1. Click your username at the top of any PeerIQ page.



2. Select **Account**. The **Account** page is displayed.

The screenshot displays the PeerIQ Account page. The left sidebar is the same as the Overview page. The main content area shows several settings sections:

- Change Password:** Fields for Current password, New password, and Re-enter new password. A submit button is at the bottom.
- User Details:** Field for Email Address (example@example.com). A submit button is at the bottom.
- Notifications:** System notification checkbox is checked. A button for Set Notification Preferences is at the bottom.
- Time Settings:** Set the time zone of displayed data on PeerIQ. A dropdown menu shows 'Use Default (Coordinated Universal Time (UTC))'. A button for Set Time Zone is at the bottom.
- Session Timeout:** Set your web interface session timeout. A dropdown menu shows '10 minutes'. A button for Set Session Timeout is at the bottom.

4.1.1 Changing Your Password

This feature is not available for accounts managed through LDAP.

To change your password:

1. In the **Current password** field, enter your current password.

2. In the **New password** field, enter the new password.

A password must be at least eight characters long, contain at least one number, one uppercase letter, one lowercase letter, and one special character (such as %, \$, #, {, }, ~, ^, , &).

3. In the **Re-enter new password** field, re-enter your new password.

4. Click **Submit**.

4.1.2 Updating Your Email Address

The **User Details** card displays the email address associated with your PeerIQ account. To update it:

1. In the **Email Address** field, enter your new email address.

2. Click **Submit** to save the change.

This address is used for system notifications and account-related messages.

4.1.3 Managing Notification Preferences

The **Notifications** card controls whether system notifications are sent to your account. To change your preferences:

1. Select or clear the **System** checkbox to enable or disable system notifications.

2. Click **Set Notification Preferences** to apply your changes.

When enabled, system notifications provide alerts about account activity and important PeerIQ events.

4.1.4 Changing Your Time Zone Settings

Use the **Time Settings** card to configure the time zone displayed across the PeerIQ interface. Choose your preferred time zone from the dropdown menu:

- **Coordinated Universal Time (UTC)** – displays all time-related data in UTC.
- **Local Browser Time Zone** – matches the time zone of your web browser.

The default time zone is set by PeerIQ administrators, but each user can adjust this setting individually.

Click **Set Time Zone** to save your selection.

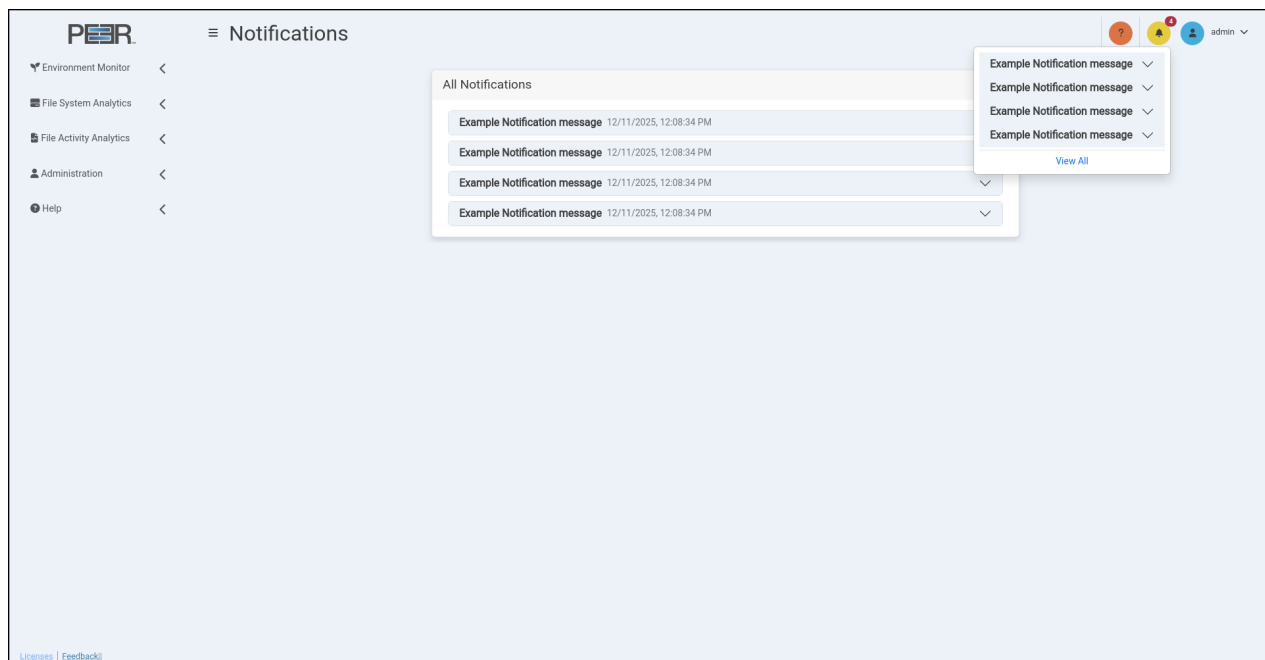
4.1.5 Setting Your Session Timeout

The **Session Timeout** card defines how long your session remains active before automatic sign-out. Use the dropdown menu to select your preferred timeout length, then click **Set Session Timeout** to apply the change.

Note: Updating the timeout affects only new sessions. Existing sessions remain active until they naturally expire or you sign out manually.

4.2 Notifications

PeerIQ provides a centralized notification system to alert users about important events, updates, and system activity. Notifications can be accessed from any page in the PeerIQ web interface.



4.2.1 Accessing Notifications

In the top-right corner of every page, a **yellow bell icon** indicates the presence of notifications. When new notifications are available, a **red badge** appears over the bell, displaying the number of unread items.

Click the bell icon to open a drop-down list showing recent notifications. Each entry includes a short description and timestamp.

- Clicking a notification expands it to display additional details.
- Selecting **View All** at the bottom of the drop-down opens the full **Notifications** page.

4.2.2 Notifications Page

The **Notifications** page lists all notifications generated by the PeerIQ system. Each message is shown with its timestamp and title.

Clicking the **downward arrow** on a notification expands it to display the full message content, providing additional context or details about the event.

Notifications are retained for review to help administrators and users monitor system activity and configuration changes across PeerIQ. PeerIQ keeps the ten most recent notifications available for review. When a new notification is added, the oldest entry is automatically discarded to maintain this limit.

5 Setting Up Communication between the PMC and PeerIQ

Before you can collect data in PeerIQ, you must set up communication between the PMC and PeerIQ. This involves two key steps:

1. **Configuring PeerIQ's connection to a broker:** Set up PeerIQ's connection to a Peer Management broker. The broker manages communication between the PMC and other PeerGFS components, such as Peer Agents, and facilitates communication between PMC and external applications, including PeerIQ.
2. **Enabling data transfer:** After configuring the connection to the broker, enable the transfer of data from the PMC to PeerIQ.

For detailed instructions, see these sections:

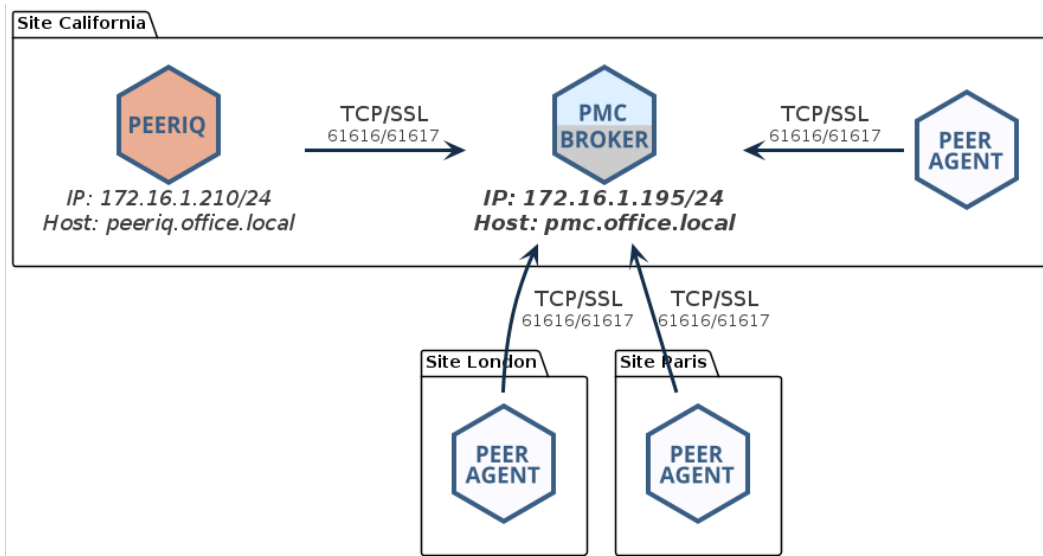
- [Configuring PeerIQ's Connection to Peer Management Broker](#)
- [Enabling Peer Management Center to Send Data to PeerIQ](#)

5.1 Configuring PeerIQ's Connection to a Peer Management Broker

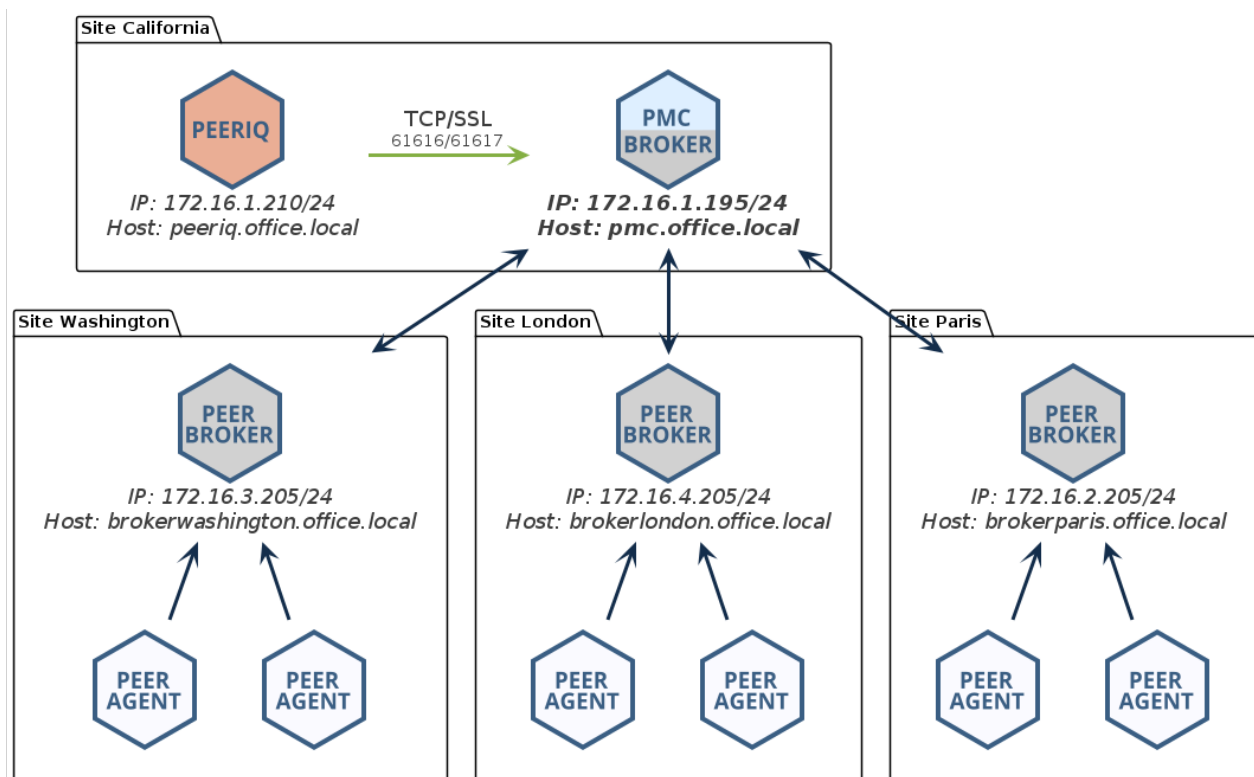
Depending on your current PeerGFS implementation, there are several methods for connecting PeerIQ to a Peer Management broker. This section first outlines common deployment scenarios and specifies which IP address or hostname should be used for the connection. It then provides step-by-step instructions for establishing the connection.

5.1.1 Typical Broker Deployments

Basic Configuration For a standard PeerGFS deployment, the most common configuration involves a single broker deployed on the PMC host. In this scenario, PeerIQ must be deployed on the same local network as the PMC host. To establish the connection, you can use either the IP address of the PMC host (e.g., *172.16.1.195*) or its fully qualified domain name (FQDN) (e.g., *pmc.office.local*).

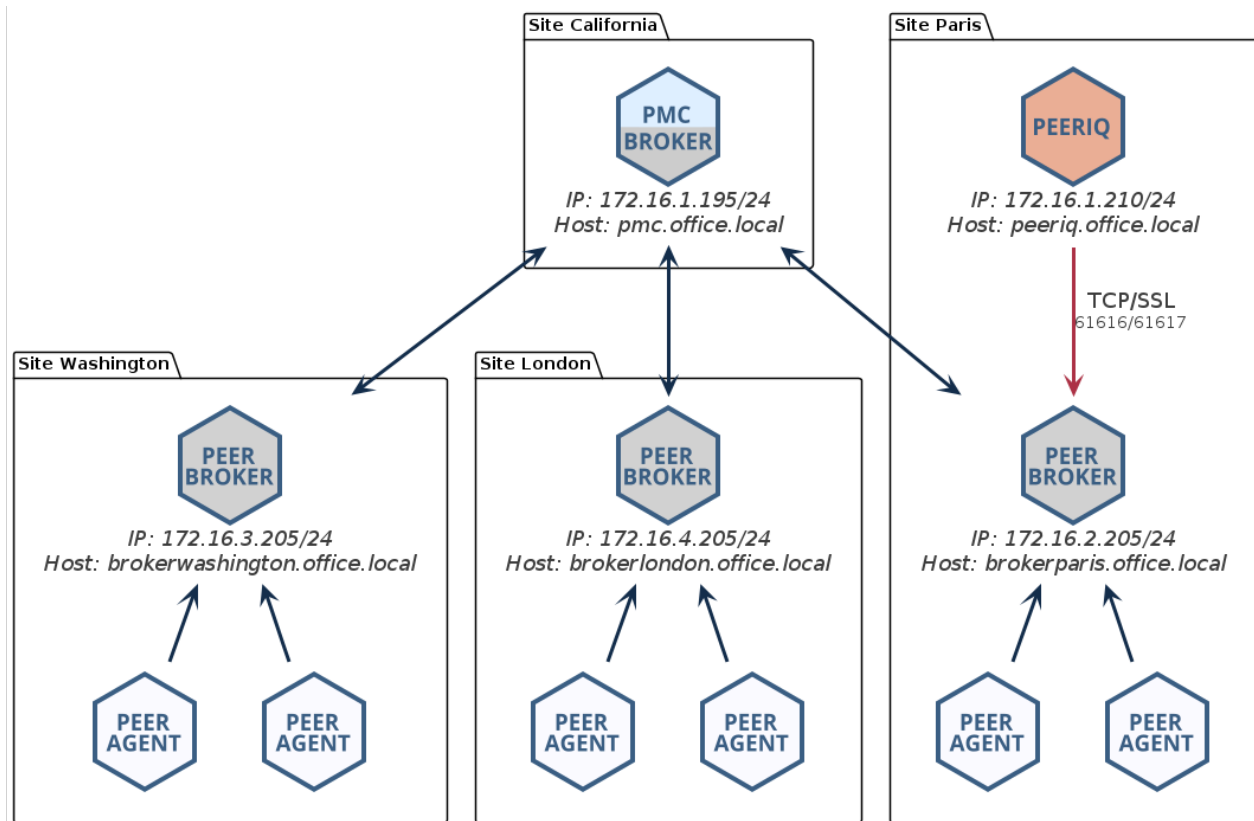


Network of Brokers If you have deployed a network of brokers, it is crucial to connect to the IP address of the PMC running the broker if they are on the same host, or to the broker with which the PMC has a direct network connection. In the following example, you could use either the IP address 172.16.1.195 or the FQDN *pmc.office.local*:

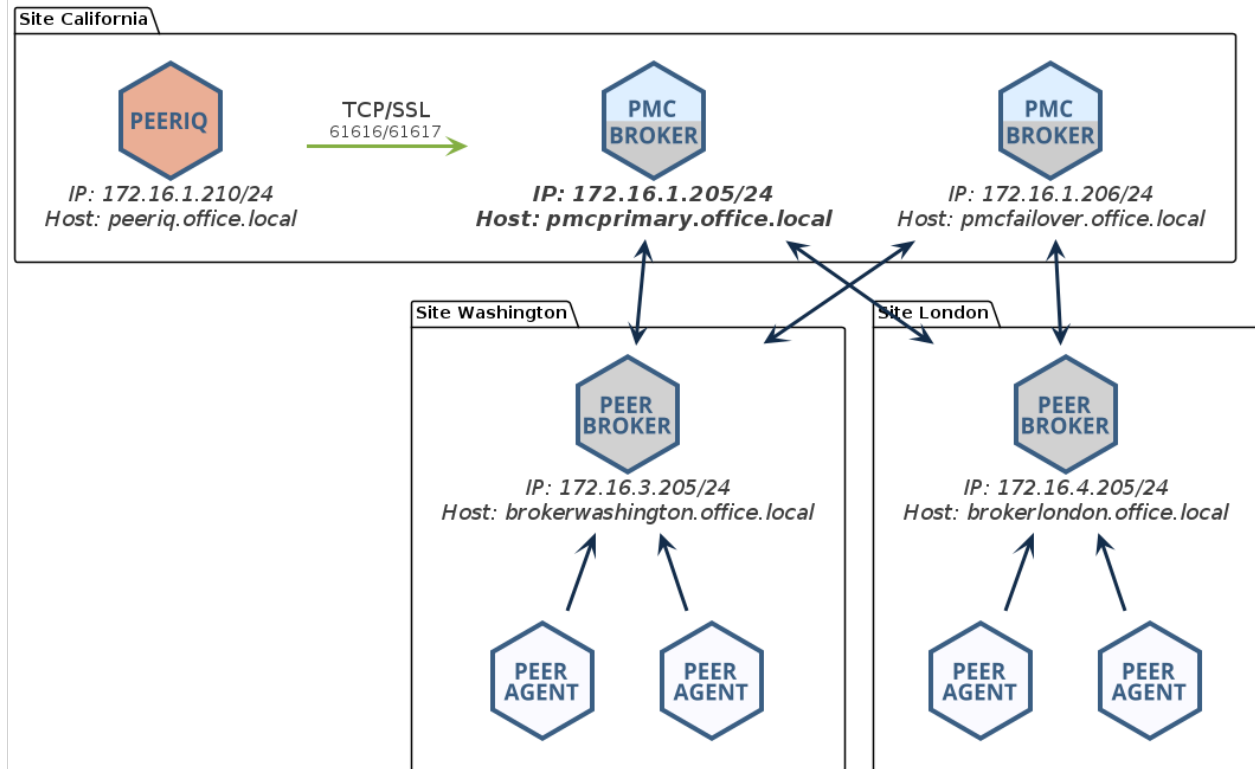


Attempting to connect to another broker within the network that does not have a direct link to the PMC will be unsuccessful and result in PeerIQ not receiving any data. In the following example, the

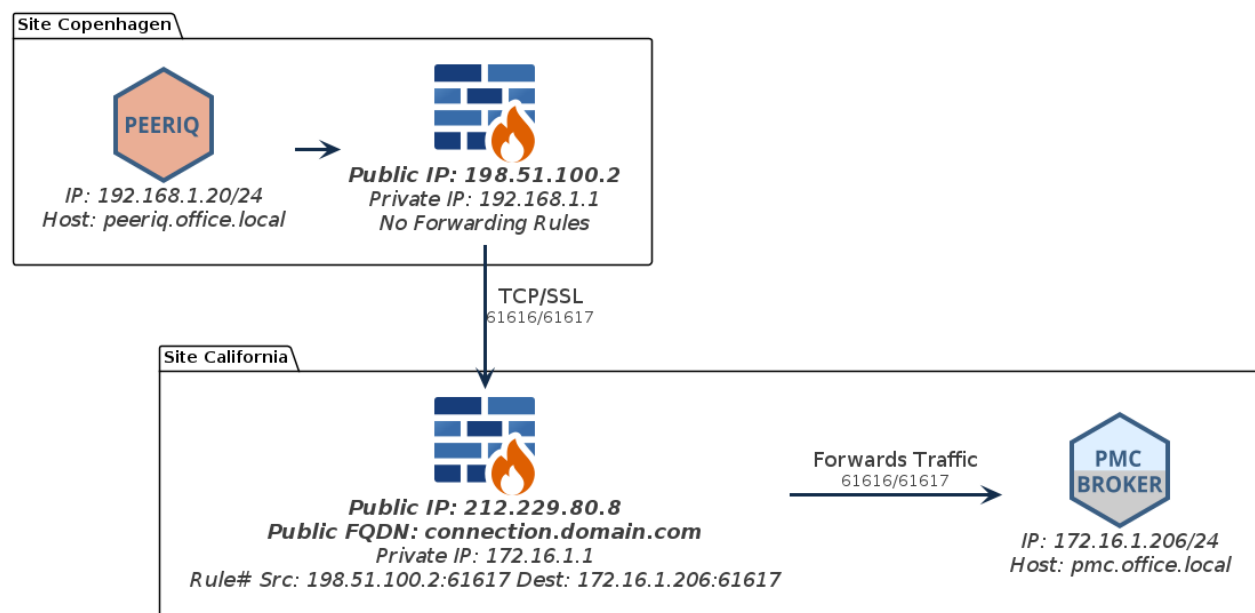
user is trying to connect to the broker at the Paris site, which lacks a direct link to the PMC. Consequently, no data will be transmitted.



Redundant PMC In a redundant PMC configuration, only the primary PMC can be monitored. In the following example, you would connect PeerIQ to the IP address 172.16.1.205 or to the FQDN *pmcprimary.office.local*.



NAT Firewall When connecting PeerIQ to the broker through a NAT firewall, it is essential to configure source and destination rules to forward traffic to the PMC. In the following example, the firewall at the California site is configured to forward all traffic received from IP *198.51.100.2* on port 61617 to the IP address of the broker. In this example, you would connect to the IP address *172.16.1.205* or to the FQDN *connection.domain.local*.

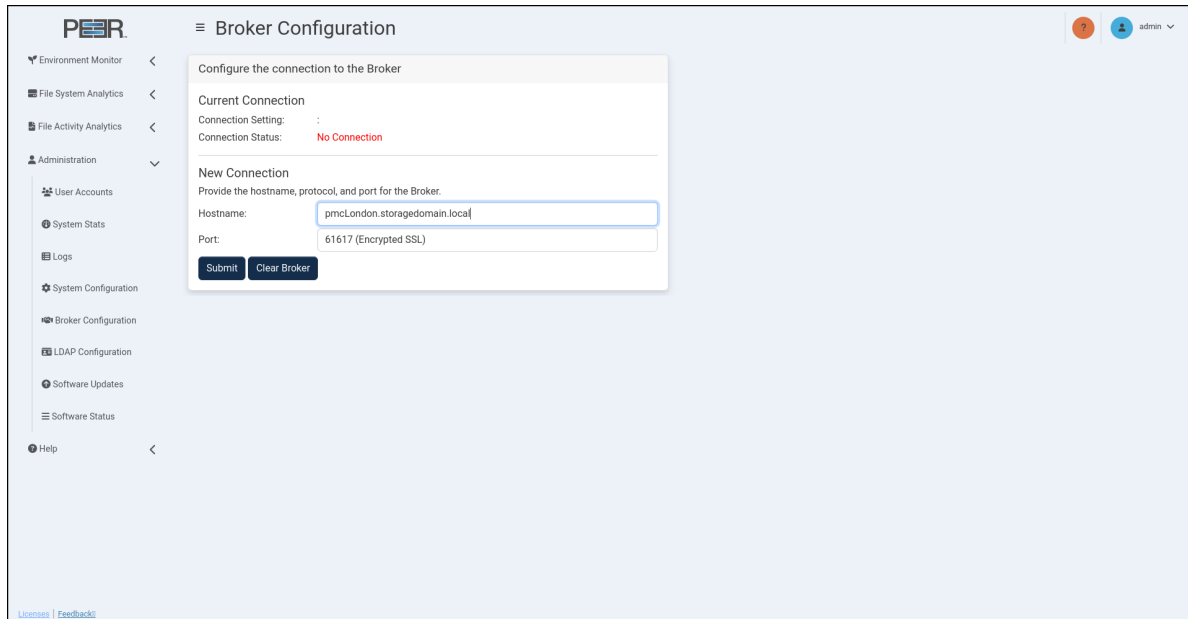


5.1.2 Configuring the Broker Connection

To configure PeerIQ's connection to a broker:

1. Using your Administrator account, open PeerIQ.
2. Select **Broker Configuration** from the menu on the left.

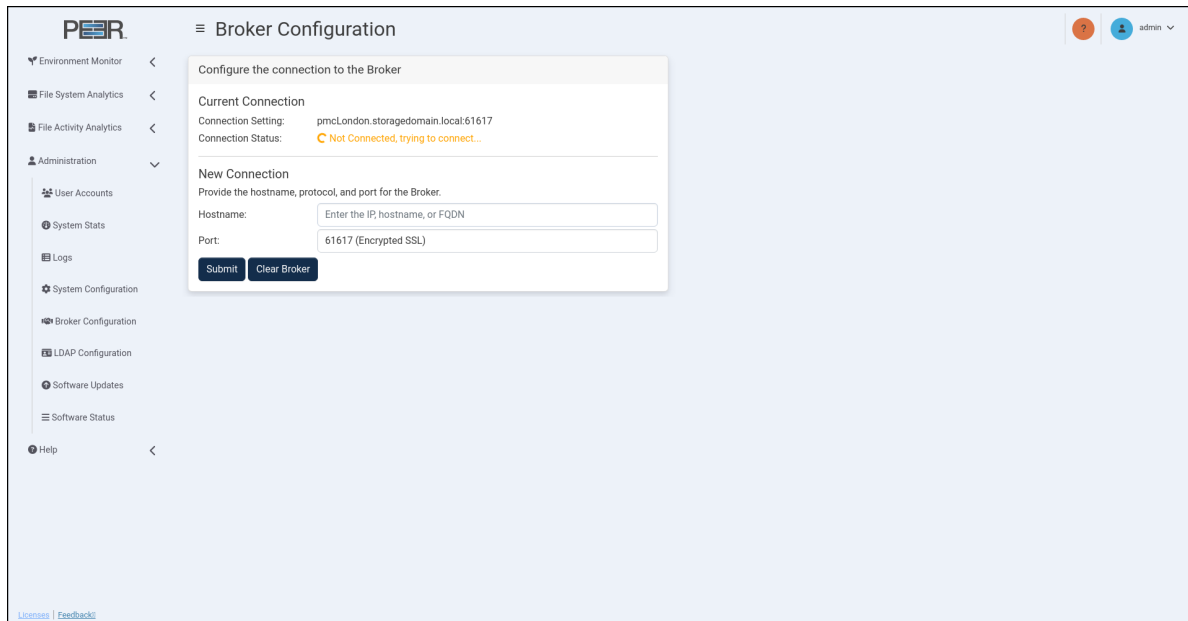
The Broker Configuration page is displayed, showing *No Connection* as the connection status.



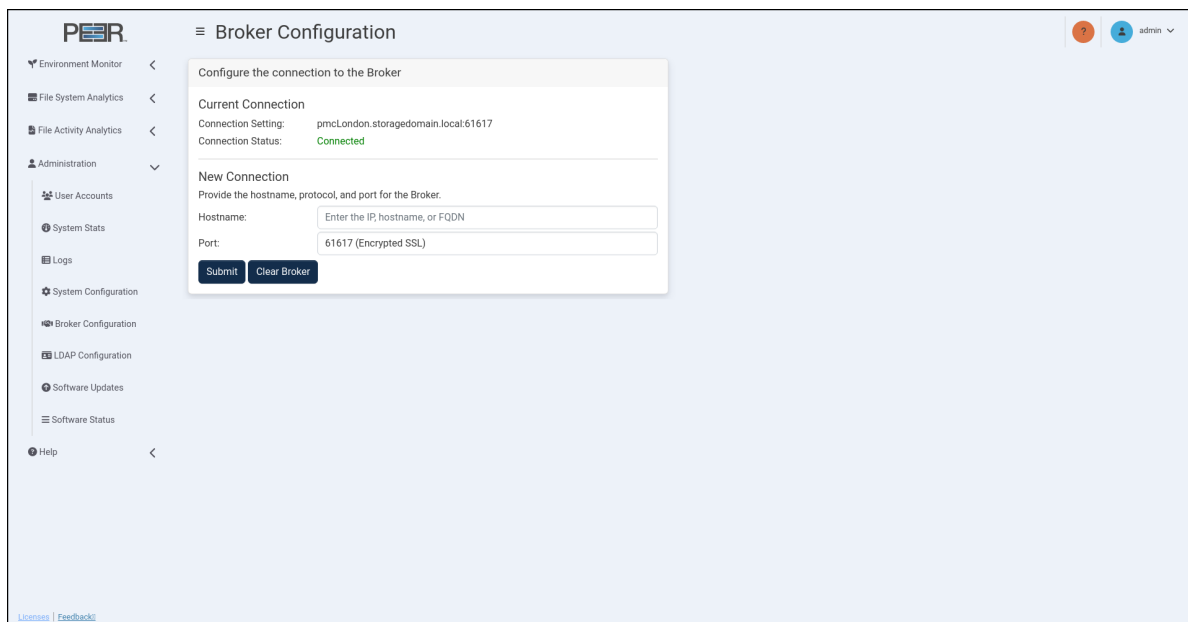
The screenshot displays the PeerIQ web interface's 'Broker Configuration' page. On the left is a navigation menu with options like 'Environment Monitor', 'File System Analytics', 'Administration', 'User Accounts', 'System Stats', 'Logs', 'System Configuration', 'Broker Configuration' (which is selected), 'LDAP Configuration', 'Software Updates', 'Software Status', and 'Help'. The main content area is titled 'Broker Configuration' and contains a form to 'Configure the connection to the Broker'. The form has two sections: 'Current Connection' showing 'Connection Setting: ' and 'Connection Status: No Connection' in red, and 'New Connection' with instructions to 'Provide the hostname, protocol, and port for the Broker.' It includes input fields for 'Hostname:' (containing 'pmcLondon.storagedomain.local') and 'Port:' (containing '61617 (Encrypted SSL)'). At the bottom of the form are 'Submit' and 'Clear Broker' buttons. The top right of the interface shows a user profile for 'admin'.

3. In the **Hostname** field, enter the IP address or the FQDN of the broker.
4. Choose between an encrypted SSL 61617 connection or a standard TCP connection on 61616.
5. Click the **Submit** button.

The connection status changes to *Not Connected, trying to connect...* This status will persist until the connection is established, which can take up to a minute.



Once connected, the status changes to *Connected*.



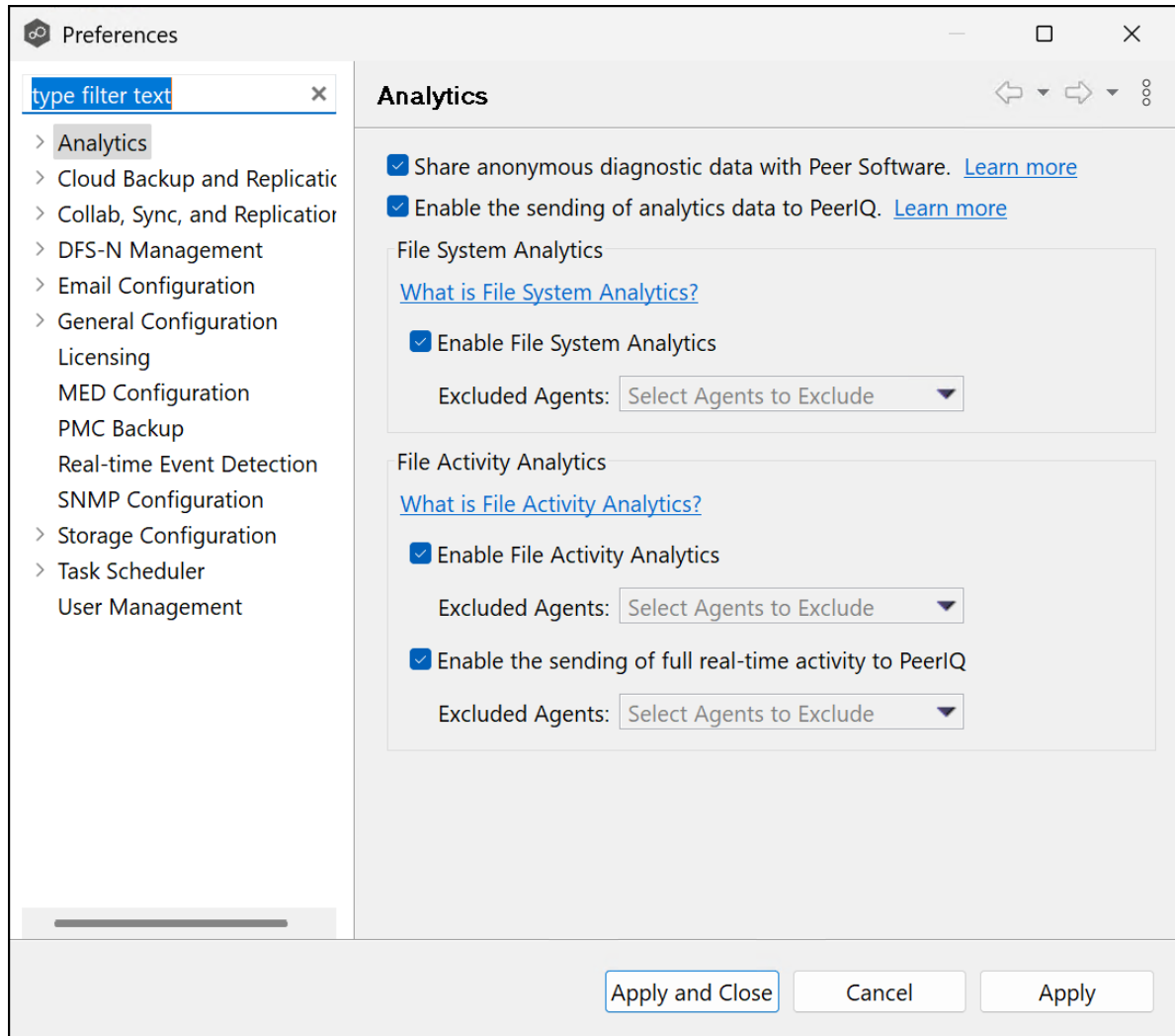
If the status does not change to *Connected*, refer to the Connection Issues section.

5.1.3 Stopping Attempts to Connect to a Broker

To stop connection attempts from PeerIQ to a broker, click the **Clear Broker** button.

3. In the dialog that appears, select the **Enable the sending of analytics data to PeerIQ** checkbox. This option enables the PMC to transmit environmental data to PeerIQ.

Once selected, three additional options become available.



It may take up to 3 minutes for environment data to begin populating in PeerIQ.

4. To enable file system scan data to be sent to PeerIQ, select the **Enable File System Analytics** checkbox.

Enabling this option initiates weekly scans of any volumes associated with jobs in PeerGFS. The scan data will be processed by PeerIQ every Saturday by default. If your use case involves only receiving environmental data analytics, this option is not required.

5. To enable file activity summary data to be sent to PeerIQ, select the **Enable File Activity Analytics** checkbox.

Enabling this option initiates the collection of real-time activity statistics in PeerGFS. These statistics will then be sent to and analyzed by PeerIQ every five minutes. If your use case involves only receiving environmental data analytics, this option is not required.

6. To enable activity data to be sent to PeerIQ, select the **Enable the sending of full real-time activity to PeerIQ** checkbox.

Enabling this option initiates the collection and forwarding of all real-time events detected across running File Collaboration, File Synchronization, and File Replication jobs. > Note: A PeerIQ Advanced License is required to enable the transmission > and logging of real-time activity.

7. To verify that data is being sent correctly, open the **Overview** page in PeerIQ.

The **Data Connection** card displays the status of the connection. When the icon is green and the text says **Good**, data is successfully being sent.

6 Monitoring the PeerGFS Environment

The following section describes the **Environment Monitor** pages. These pages provide details about your PeerGFS environment, including the PMC, Agents, and the jobs.

The seven Environment Monitor pages are:

- Overview
- PMC
- Jobs
- Agents
- Volumes
- Watch Set
- License

6.1 Using the Environment Monitoring Page Controls

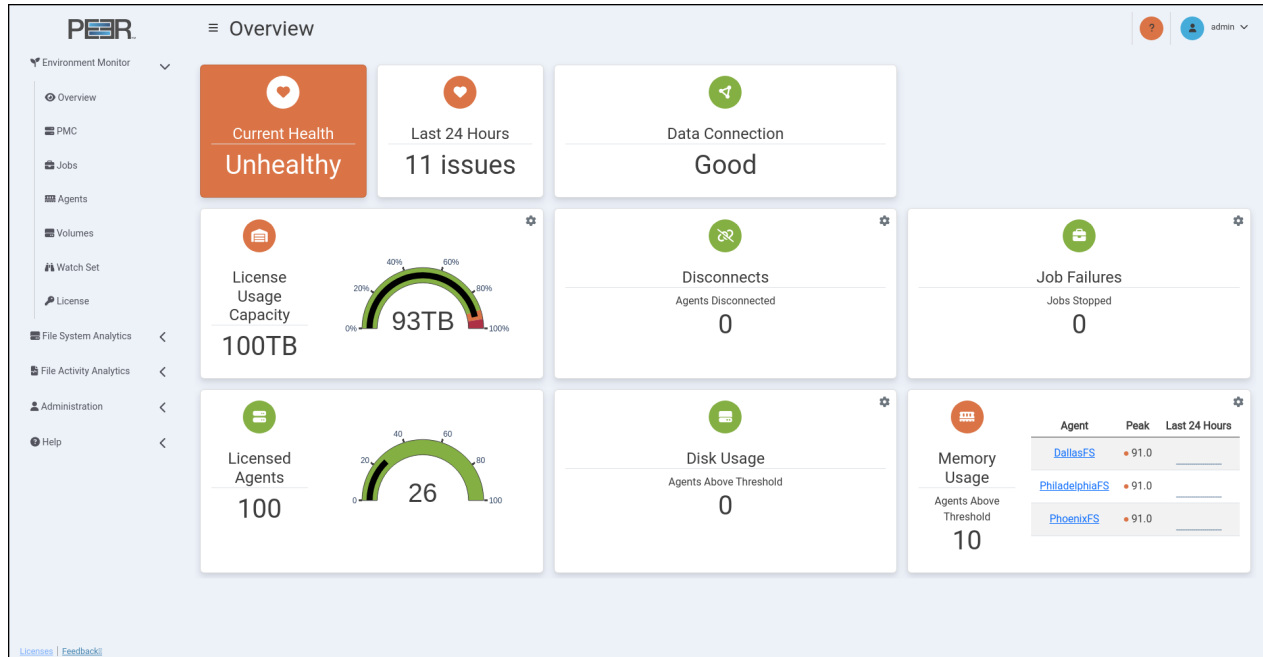
Several pages feature line graphs that depict activity trends over time. Use the controls located in the upper right corner of the page to adjust the date range and refresh rate of the displayed information:

- **Range:** Use this to select the desired time range for the line graphs; options range from 1 hour to 4 weeks.
- **Refresh:** Use this to select the interval at which the line graphs automatically refresh; Options are off (graphs will not refresh) or 1 minute.

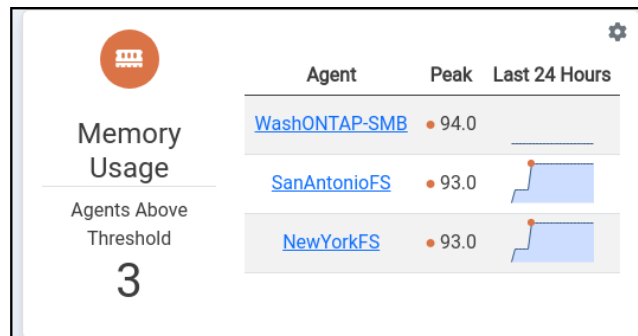


6.2 Overview Page

The **Overview** page is a dashboard displaying the critical aspects of the PeerGFS environment. Each card represents a specific area of health, providing an at-a-glance view of issues from the last 24 hours. The color and status indicator on each card reflects the current health based on detected issues.



When there is an issue, a card displays up to three graphs depicting instances where problems have been encountered. For example, the card below shows memory usage exceeded thresholds on one Agent server. Hover over values to see when the issue occurred. Click the name of an Agent or job for more details.



6.2.1 Overview Page Cards

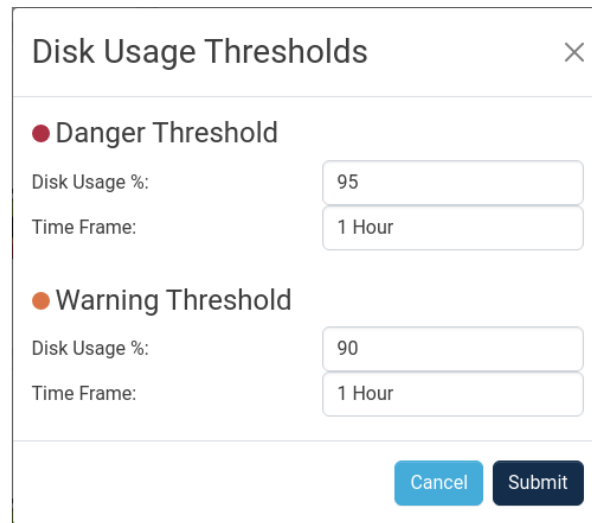
The Overview page contains nine cards:

Card	Description
Current Health	<p>Visually represents the current health of the PeerGFS environment. The presence of an ongoing issue determines the status. The background color and indicator reflect this status:</p> <ul style="list-style-type: none"> • Green: Everything is functioning normally; no current issues detected. Other cards may show different colors, indicating that thresholds were exceeded in the last 24 hours but are now within the allowed limits. • Orange: Indicates that a Warning threshold was exceeded and remains so. The card reflects an Unhealthy state. • Red: Indicates that a Danger threshold was exceeded and the issue is ongoing. The card reflects an Unhealthy state. Exceeding a Danger threshold overrides any warning messages.
Last 24 Hours	<p>Visually represents the overall health of the PeerGFS environment over the last 24 hours. If all other cards show zero issues, the card indicator will be green, reflecting a Healthy status. If any card shows issues, the overall status will turn orange or red, depending on the severity:</p> <ul style="list-style-type: none"> • If any card has an orange indicator, the Last 24 Hours status is Warning, reflecting an unhealthy environment. • If any card has a red indicator, or if multiple cards have orange indicators and at least one is red, the Last 24 Hours status is Danger, reflecting an unhealthy environment.
Data Connection	<p>Displays the results of monitoring environment data reception from PeerGFS, excluding scan and real-time data.</p> <p>A Warning (orange) status is triggered after five minutes of no data, while a Danger (red) status occurs after 30 minutes. The label shows the duration since the last data was received.</p> <p>The status reflects that data reception may still be hindered even with an operational broker link. For example, this can occur if the Enable the sending of analytics data to PeerIQ checkbox was not selected during PMC configuration or if an outdated version of PeerGFS is in use.</p>

Card	Description
License Usage Capacity	<p>Displays the total capacity of the license in terabytes (TB), while the number below the gauge shows the used capacity in TB. The gauge indicates the percentage of the PeerGFS usage allowance that has been utilized. The default thresholds are:</p> <ul style="list-style-type: none">• Danger: Exceeds 95% usage.• Warning: Exceeds 90% usage.
Disconnects	<p>Displays the number of Agents that have been disconnected and identifies those specific Agents. The default thresholds are:</p> <ul style="list-style-type: none">• Danger: Exceeds 10 disconnects in a one-hour period.• Warning: Exceeds 1 disconnect in a one-hour period.
Job Failures	<p>Displays the number of jobs that have failed. The default thresholds are:</p> <ul style="list-style-type: none">• Danger: Exceeds 10 disconnects in a one-hour period.• Warning: Exceeds 1 disconnect in a one-hour period.
Licensed Agents	<p>Displays the number of active Agents in relation to the total number of licensed Agents. The number below Licensed Agents label shows the total number of Agents authorized by the PeerGFS license, while the number below the gauge indicates the number of Agents currently in use.</p>
Disk Usage	<p>Displays the number of Agents that might be utilizing a significant amount of their disk storage. The default thresholds are:</p> <ul style="list-style-type: none">• Danger: Exceeds 95% usage in a one-hour period.• Warning: Exceeds 90% usage in a one-hour period.
Memory Usage	<p>Displays the number of Agents that may have experienced prolonged periods of high memory usage. The default thresholds are:</p> <ul style="list-style-type: none">• Danger: Exceeds 95% usage in a one-hour period.• Warning: Exceeds 90% usage in a one-hour period.

6.2.2 Modifying Thresholds

Preconfigured defaults for the **Danger** and **Warning** thresholds can be modified by Administrators. Using your Administrator account, click the gear icon in the upper right corner of a card to modify its thresholds. In the dialog that appears, set the **Danger** and **Warning** thresholds:



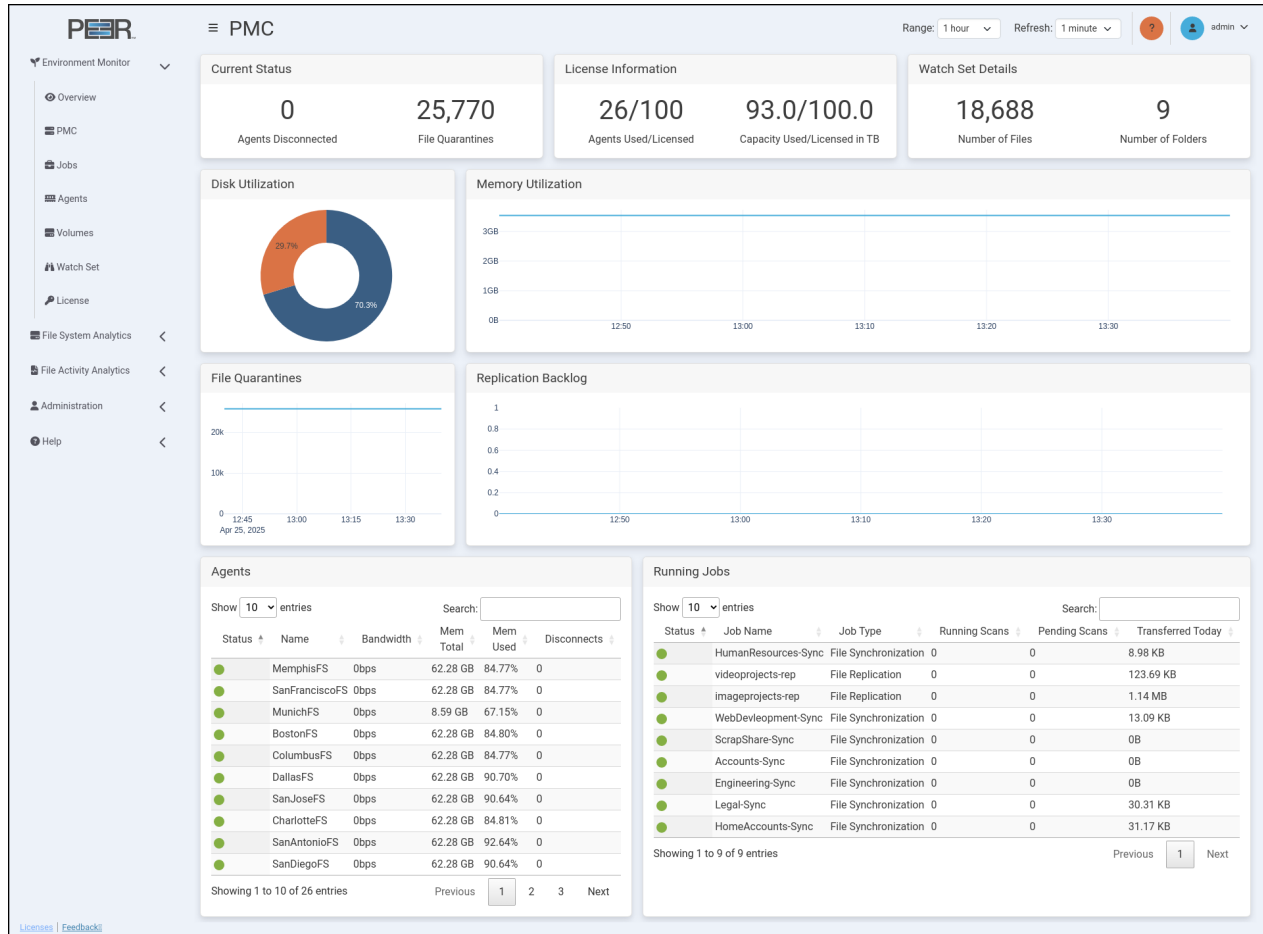
The image shows a dialog box titled "Disk Usage Thresholds" with a close button (X) in the top right corner. The dialog is divided into two sections: "Danger Threshold" and "Warning Threshold". Each section has two input fields: "Disk Usage %" and "Time Frame".

Threshold Type	Disk Usage %	Time Frame
Danger Threshold	95	1 Hour
Warning Threshold	90	1 Hour

At the bottom right of the dialog are two buttons: "Cancel" (light blue) and "Submit" (dark blue).

6.3 PMC Page

The **PMC** page provides an overview of the PMC's environment.

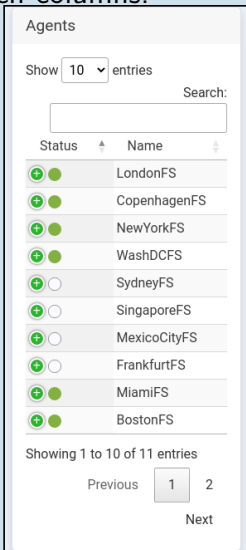


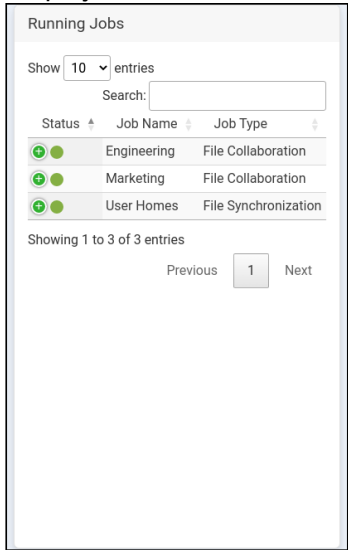
6.3.1 PMC Page Cards

The PMC page contains nine cards:

Card	Description
Current Status	Displays: <ul style="list-style-type: none"> ● Agents Disconnected: The total number of disconnected Agents that the PMC is aware of. ● File Quarantines: The total number of files in quarantine.

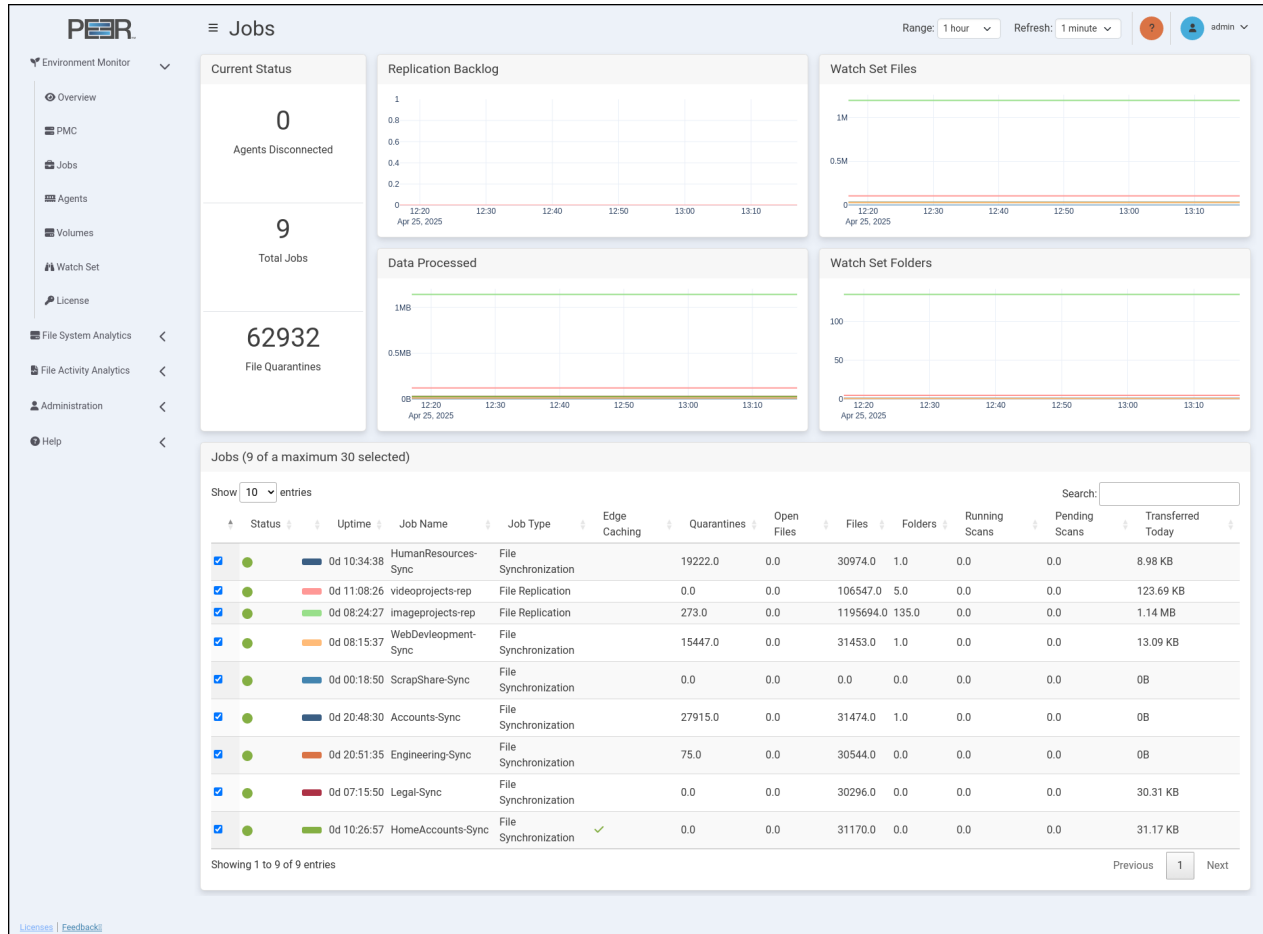
Card	Description
License Information	<p>Displays:</p> <ul style="list-style-type: none">• Agents Used/Licensed: The total number of Agents in relation to the maximum allowed by your license. Agents are counted only if they are associated with at least one job.• Used vs Licensed Capacity in TB: The total capacity used in the environment compared to the maximum licensed capacity.
Watch Set Details	<p>Displays:</p> <ul style="list-style-type: none">• Number of Files: The total number of files in the environment.• Number of Folders: The total number of folders in the environment.
Disk Utilization	<p>Displays a pie chart that compares the total disk space used in the environment (represented in orange) with the available disk space (represented in blue).</p>
Memory Utilization	<p>Displays a line graph that shows the system memory usage of the PMC server over time.</p>
File Quarantines	<p>Displays a line graph that shows the total number of files in quarantine over time.</p>
Replication Backlog	<p>Displays a line graph that shows the total number of files in the replication backlog over time.</p>

Card	Description
Agents	<p>Displays a table listing all Agents in the environment, with each row representing an Agent. For more detailed information about Agents, view the Agents page.</p> <p>The table shows the following information for each Agent:</p> <ul style="list-style-type: none"> • Status: The status of the Agent is indicated by color: <ul style="list-style-type: none"> – Green: Connected – Yellow: Pending – Orange: Disconnected – Black: Disabled – White: Unknown • Name: The name of the Agent. • Bandwidth: The tested bandwidth between the PMC and the Agent. (You must first run Test Agent Bandwidth Speed in the Agents view in the PMC for a value to be displayed.) • Total Mem: The total memory available to the Agent. • Mem Used: The percentage of the total memory currently in use. • Disconnects: The number of disconnects for this Agent. If not all six columns are displayed, click the green plus sign in the Status column to reveal the hidden columns. 

Card	Description
Running Jobs	<p>Displays a table listing all currently running jobs in the environment, with each row representing a job. For more detailed information about all jobs (including jobs that aren't running), view the Jobs page. The table shows the following information for each job:</p> <ul style="list-style-type: none"> • Status: The status of the job is indicated by color: <ul style="list-style-type: none"> – Green: Job is running – Orange: Job isn't running due to an error – White: Job is stopped or has unknown status • Job Name: The name of the job. • Job Type: The type of job. • Running Scans: The total number of currently running scans. • Pending Scans: The total number of currently pending scans. • Transferred Today: The total number of bytes transferred today. To display the number for an Agent, click the green dot to the left of the Agent's status indicator. <p>If not all of the columns are displayed, click the green plus sign in the Status column to display the hidden columns.</p> 

6.4 Jobs Page

The **Jobs** page provides detailed information about PeerGFS jobs in the environment.



6.4.1 Job Page Cards

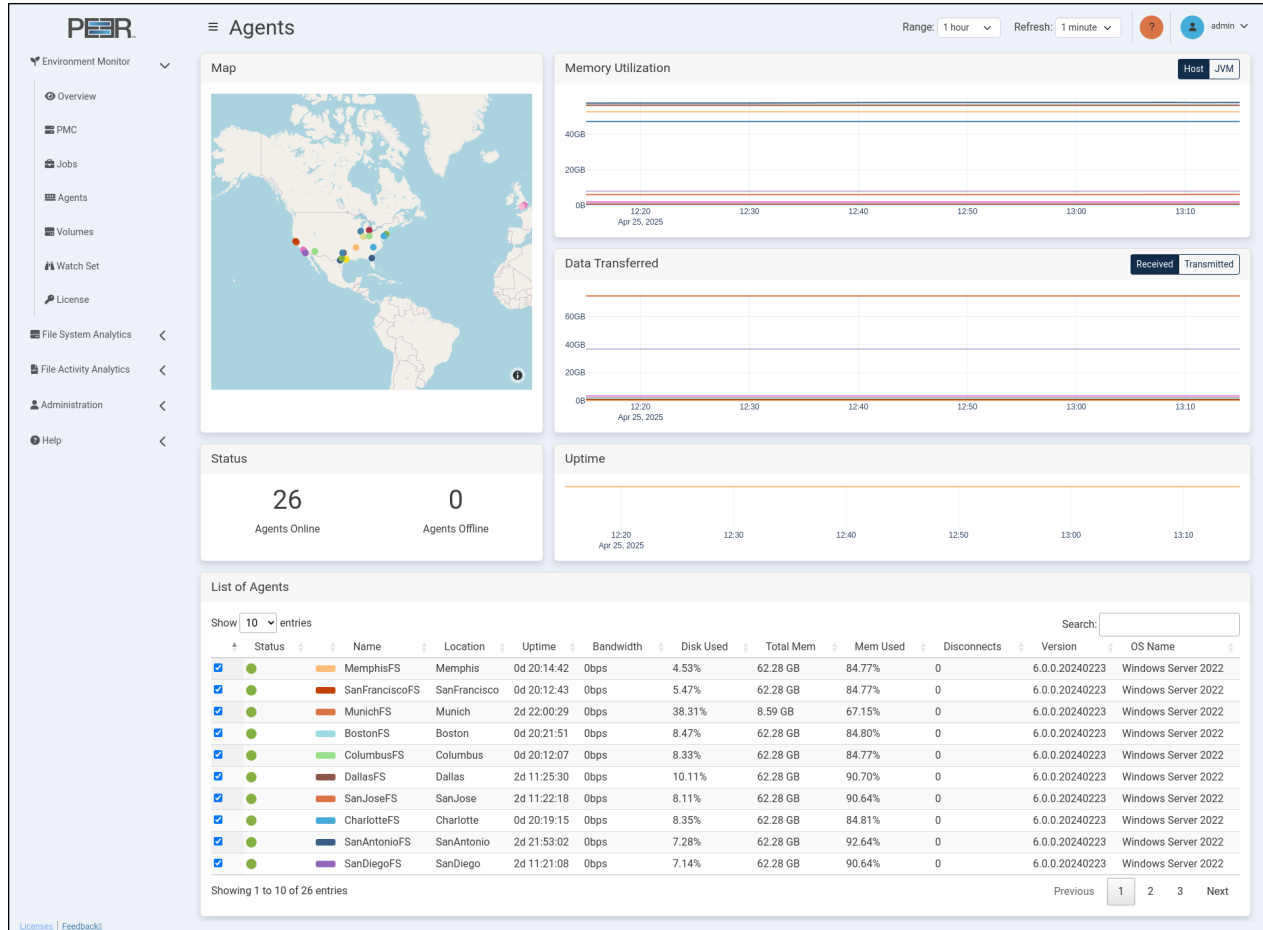
The Jobs page contains six cards:

Card	Description
Current Status	Displays: <ul style="list-style-type: none"> • Agents Disconnected: The total number of disconnected Agents in the environment. • Total Jobs: The total number of jobs in the environment. • File Quarantines: The total number of files currently quarantined.
Replication Backlog	Displays a line graph that shows the total number of files in the replication backlog over time.

Card	Description
Data Processed	Displays a line graph the shows the data processed in bytes over time. The total resets every day.
Watch Set Files	Displays a line graph that shows the total number of files in the environment's watch set over time.
Watch Set Folders	Displays a line graph that shows the total number of folders in the environment's watch set over time.
Jobs	<p>Displays a table listing all the jobs in the environment, with each row representing a job.</p> <p>Toggle the checkbox in the first column to show or hide the graph line representing that job in all graphs on the page.</p> <p>The table displays the following information for each job:</p> <ul style="list-style-type: none"> • Status: The color indicates the status of the job: <ul style="list-style-type: none"> – Green: Running – Orange: Any halted state – White: Stopped or unknown • Color: The color used to identify the corresponding job in the graphs. • Uptime: The total uptime of the job. • Job Name: The name of the job. • Job Type: The type of the job. • Edge Caching: Displays a tick when Edge Caching is enabled for this job. • Quarantines: The total number of files in quarantine for the job. • Open Files: The total number of open files for the job. • Files: The total number of files in the job's watch set. • Folders: The total number of folders in this job's watch set. • Running Scans: The total number of currently running scans. • Pending Scans: The total number of currently pending scans. • Transferred Today: The total number of bytes transferred today.

6.5 Agents Page

The **Agents** page provides an overview of the Agents in the environment.



6.5.1 Agents Page Cards

The Agents page contains six cards:

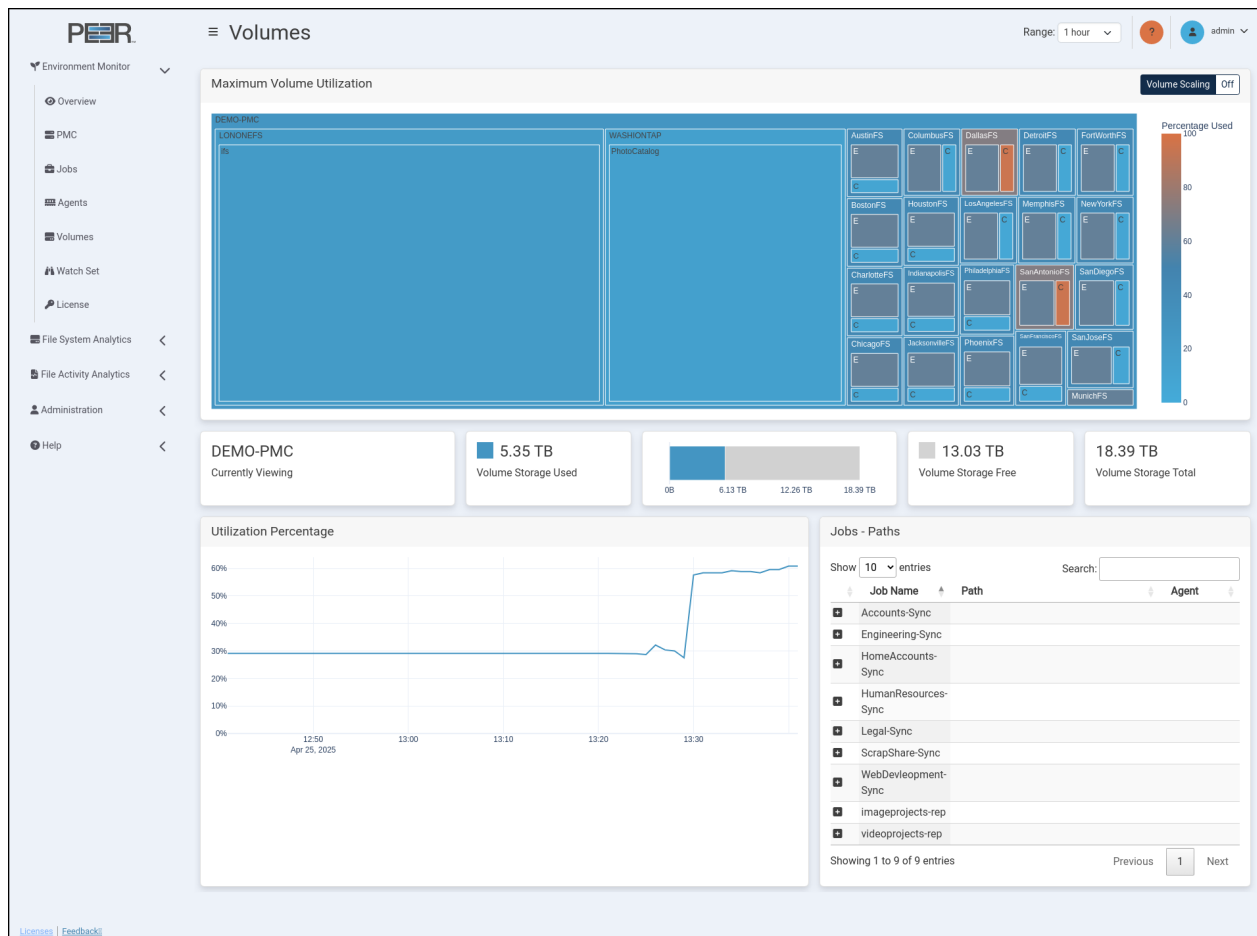
Card	Description
Map	Displays a world map that shows the location of all Agents in the environment. An Agent's latitude and longitude must be configured in the PMC to accurately display its location. If they are not configured, this card is not displayed.

Card	Description
Memory Utilization	<p>Displays a line graph that shows the memory utilization of the Agents in the environment over time. You can view either:</p> <ul style="list-style-type: none">• Host Memory• Java Virtual Machine (JVM) Memory Click the options located in the upper right corner of the card to switch between the two utilization types.
Data Transferred	<p>Displays a line graph that shows the amount of data transferred for the Agents in the environment over time. You can view either:</p> <ul style="list-style-type: none">• Data Received• Data Transmitted Click the options located in the upper right corner of the card to switch between the two transfer types.
Uptime	<p>Displays a line graph that that shows the uptime for the Agents in the environment over time.</p>
Status	<p>Displays:</p> <ul style="list-style-type: none">• Agents Online: The total number of online Agents in the environment.• Agents Offline: The total number of offline Agents in the environment.

Card	Description
List of Agents	<p>Displays a table listing all the Agents in the environment, with each row representing an Agent.</p> <p>Toggle the checkbox in the first column to show or hide the graph line representing that Agent in all graphs on the page. This will also show or hide that Agent in the map.</p> <p>The table shows the following information for each Agent:</p> <ul style="list-style-type: none"> • Status: The color indicates the status of the Agent: <ul style="list-style-type: none"> – Green: Connected – Yellow: Pending – Orange: Disconnected – Black: Disabled – White: Unknown • Color: The color used to identify the corresponding Agent in the graphs and map. • Name: The name of the Agent. • Location: The name of the Agent's location. A location must be configured in the PMC for the location to be displayed. • Uptime: The current uptime of the Agent. • Bandwidth: The results of tested bandwidth between the PMC and the Agent. (You must first run Test Agent Bandwidth Speed in the Agents view in the PMC for a value to be displayed.) • Disk Used: The percentage of the total disk space currently in use. • Total Mem: Total memory available to the Agent. • Mem Used: Percentage of the total memory currently in use. • Disconnects: The number of disconnects for this Agent. • Version: The Agent's current version number. • OS Name: The operating system the Agent is running on.

6.6 Volumes Page

The **Volumes** page provides an overview of all the volumes that are being monitored by a PeerGFS job.



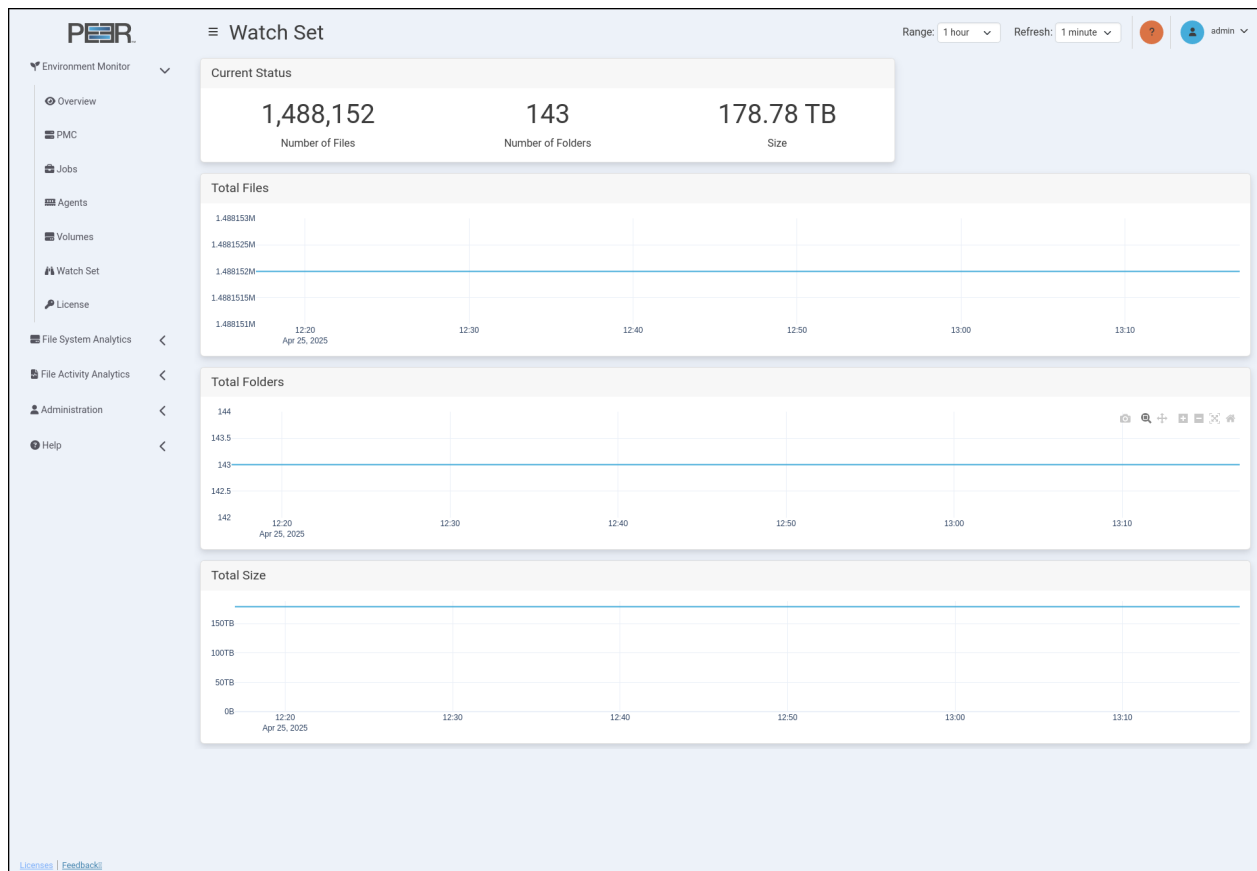
6.6.1 Volumes Page Cards

The Volumes page contains eight cards:

Card	Description
Maximum volume utilization	<p>Displays a treemap of storage devices across the PeerGFS environment and their volumes. The treemap uses nested rectangles, arranged from largest in the top left to smallest in the bottom right, to represent storage volumes. Each nested rectangle represents a volume, with size proportional to the data it represents when the <i>Volume Scaling</i> option is set to <i>On</i>. Otherwise, each volume will be the same size.</p> <p>The colors of the rectangles indicate the percentage of storage used, with the adjacent color scale identifying the percentage. Each storage device in the treemap has its own color.</p> <ul style="list-style-type: none"> • Click a nested rectangle to focus on that storage device or volume. The other cards will be updated to show data only for the selected item. Click again to return to the previous treemap view. • Hover over an element within the treemap to display the total disk space and the percentage used for the current selection.
Currently Viewing	Displays the name of the selected storage device or volume.
Volume Storage Used	Displays the used storage for the selected storage device or volume.
Graph	Displays the used versus available storage for the selected storage device or volume.
Volume Storage Free	Displays the available storage for the selected volume.
Volume Storage Total	Displays the total storage for the selected volume.
Utilization Percentage	Displays a line graph of utilization over time for the selected volume.
Jobs - Paths	<p>Displays a table of all PeerGFS jobs associated with the selected volume, with each row representing a job and the path to its watch set. Expand the plus symbol reveals the path and Agents linked to that volume. When expanded, the other two columns display the path to the watch set and Agent.</p>

6.7 Watch Set Page

The **Watch Set** page provides an overview of all the watch sets in the environment.



6.7.1 Watch Set Page Cards

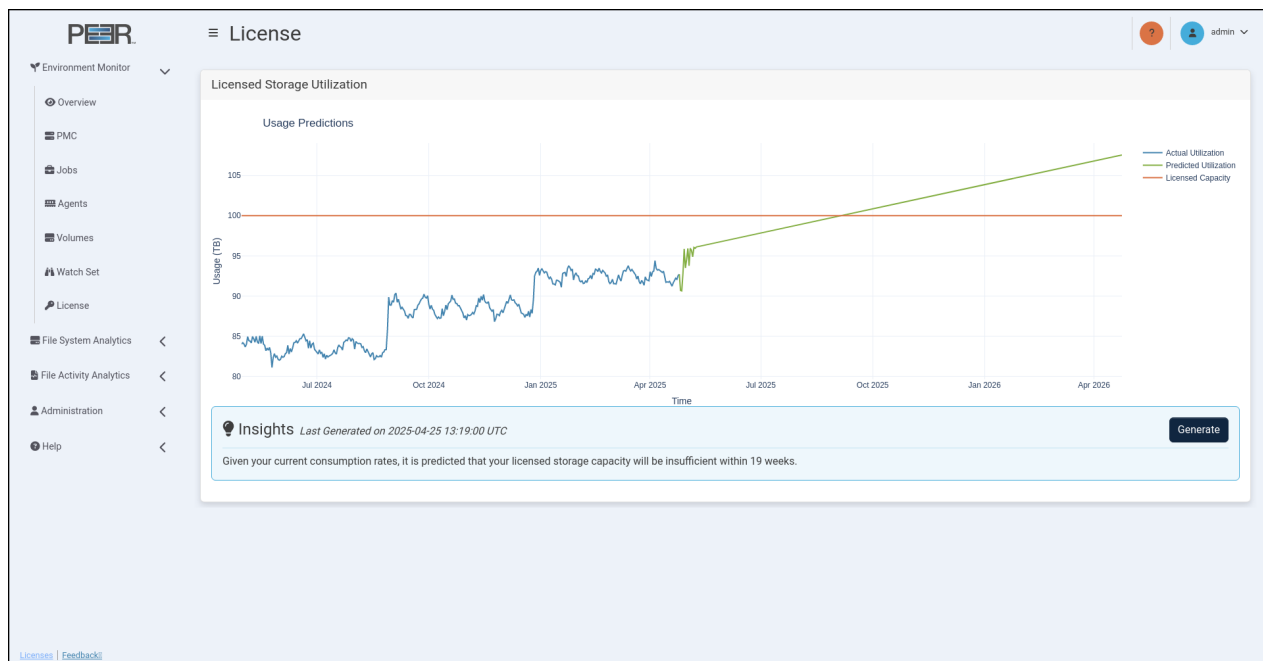
The Watch Set page contains four cards:

Card	Description
Current Status	Displays: <ul style="list-style-type: none"> • Number of Files: The total number of files in the environment's watch sets. • Number of Folders: The total number of folders in the environment's watch sets. • Size: The total size of all files in the environment's watch sets.
Total Files	Displays a line graph that shows the total number of files in the watch sets.
Total Folders	Displays a line graph that shows the total number of folders in the watch sets.

Card	Description
Total Size	Displays a line graph that shows the total size of all files in the watch sets.

6.8 License Page

The **License** page provides an overview of the historical capacity usage of PeerGFS licenses, along with the capability to predict future license utilization. It is important to note that the accuracy of the prediction model improves with the availability of more historical data. To generate a reliable prediction, a minimum of one month of data is required, and the model can project license usage up to a maximum of one year into the future.



6.8.1 License Page Card

The License page contains one card:

Card	Description
Licensed Storage Utilization	<p>Displays:</p> <ul style="list-style-type: none">• Licensed Capacity: The amount of TB licensed for PeerGFS over time.• Actual Utilization: The amount of TB used by PeerGFS over time.• Predicted Utilization: The amount of TB predicted to be used by PeerGFS over time.• Insights: Click the Generate button to generate insights into future license utilization. Once complete, the predicted utilization be updated on the graph. You'll also find an insight that indicates the remaining time until the licensed capacity is insufficient, based on the predicted utilization. We recommend considering additional license capacity from Peer Software to ensure uninterrupted usage of PeerGFS.

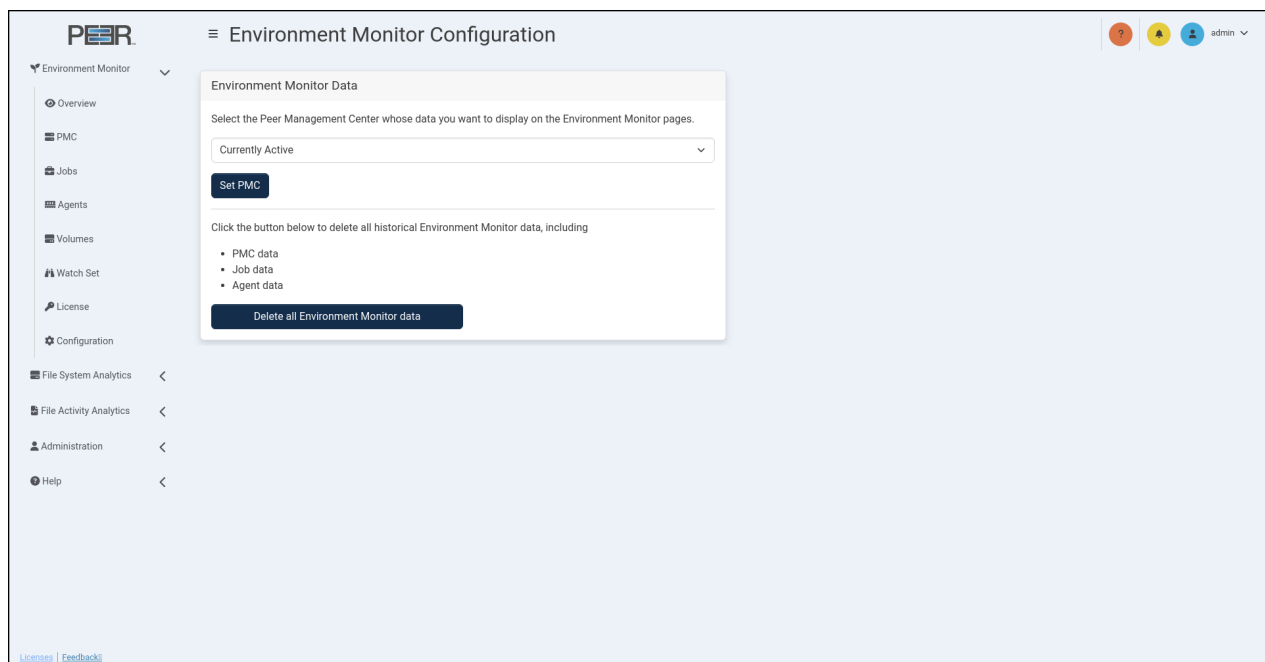
7 Analyzing Your File Systems

The following section describes the **File System Analytics** pages. These pages provide details about the file systems in your PeerGFS environment.

The four File System Analytics pages are:

- **Extensions**
- **Data Aging**
- **Hot Data Analysis**
- **Scans**

7.1 Environment Monitor Configuration



7.1.1 Managing Environment Monitor Data

To manage Environment Monitor data, use the following options on the **Environment Monitor Data** card:

- **Set PMC:** Click this button to choose which PMC is used for the Environment Monitor pages. First, select a PMC or **Currently Active** from the dropdown menu. **Currently Active** will use the PMC that was most recently connected for the first time. Then, click **Set PMC** to apply your selection.

Note: This only applies to having a redundant PMC, PeerIQ cannot be connected to two separate PMC's.

- **Delete all Environment Monitor data:** Click this button to erase all Environment Monitor data, including PMC, job, Agent, and license data.

7.2 Using the FSA Page Controls

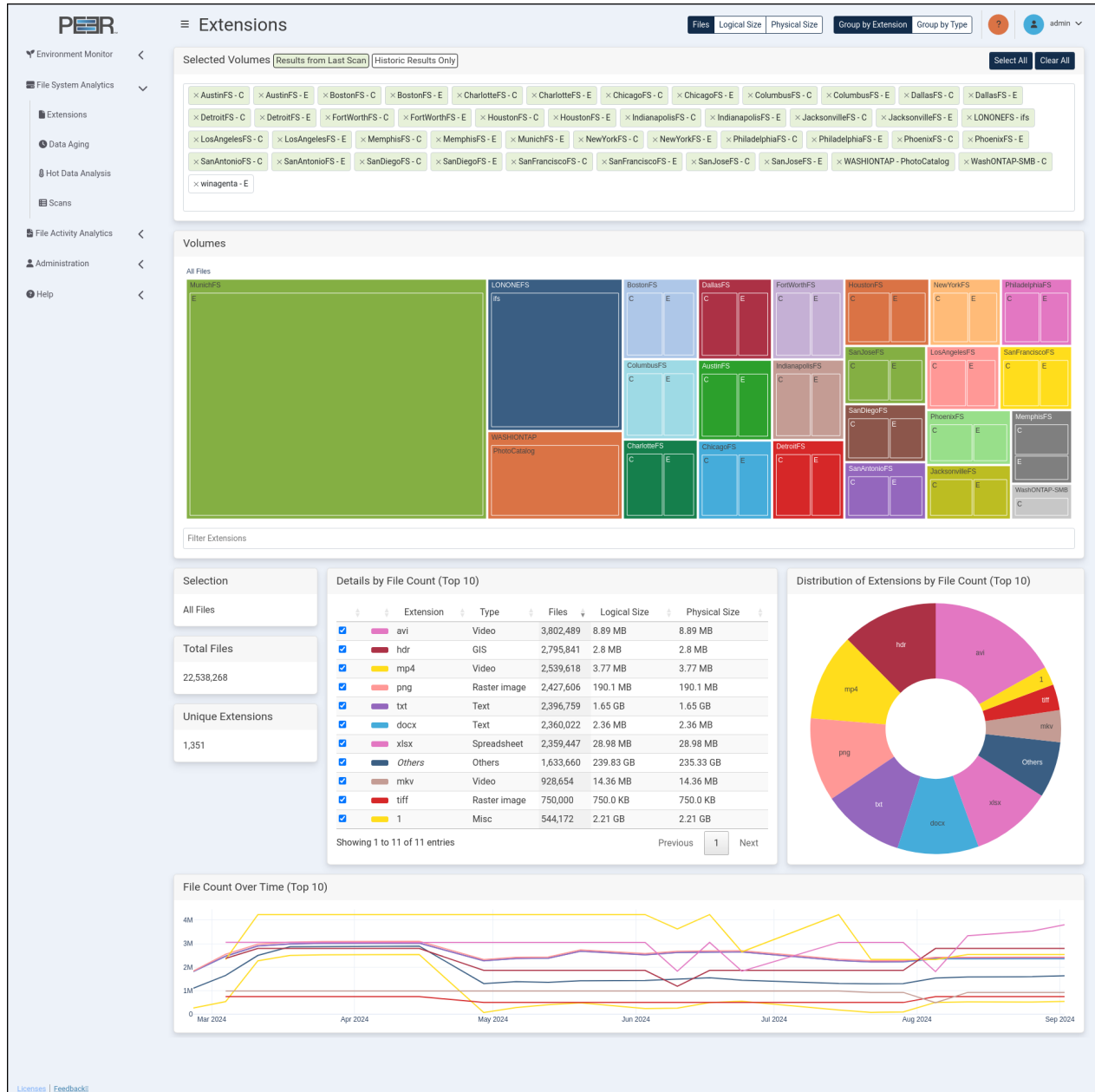
Several of the File System Analytics pages feature data visualizations such as line graphs, pie charts, and treemaps. Use the controls located in the upper right corner of the page to adjust the displayed information:

- **Files/Logical Size/Physical Size:** Select the type of data to display, such as the number of scanned files, the logical size of scanned files, or the physical size on disk of scanned files.
- **Group by Extension/Group by Type:** Select whether to display data grouped by file extension or file type.
- **Modified/Access:** Select whether to display data based on the last modified or last accessed times of each scanned file.

More detailed information is provided on individual pages.

7.3 Extensions Page

The **Extensions Page** displays a breakdown of the file extensions in use across your PeerGFS environment.



7.3.1 Extensions Page Cards

The **Extensions** page contains seven cards:

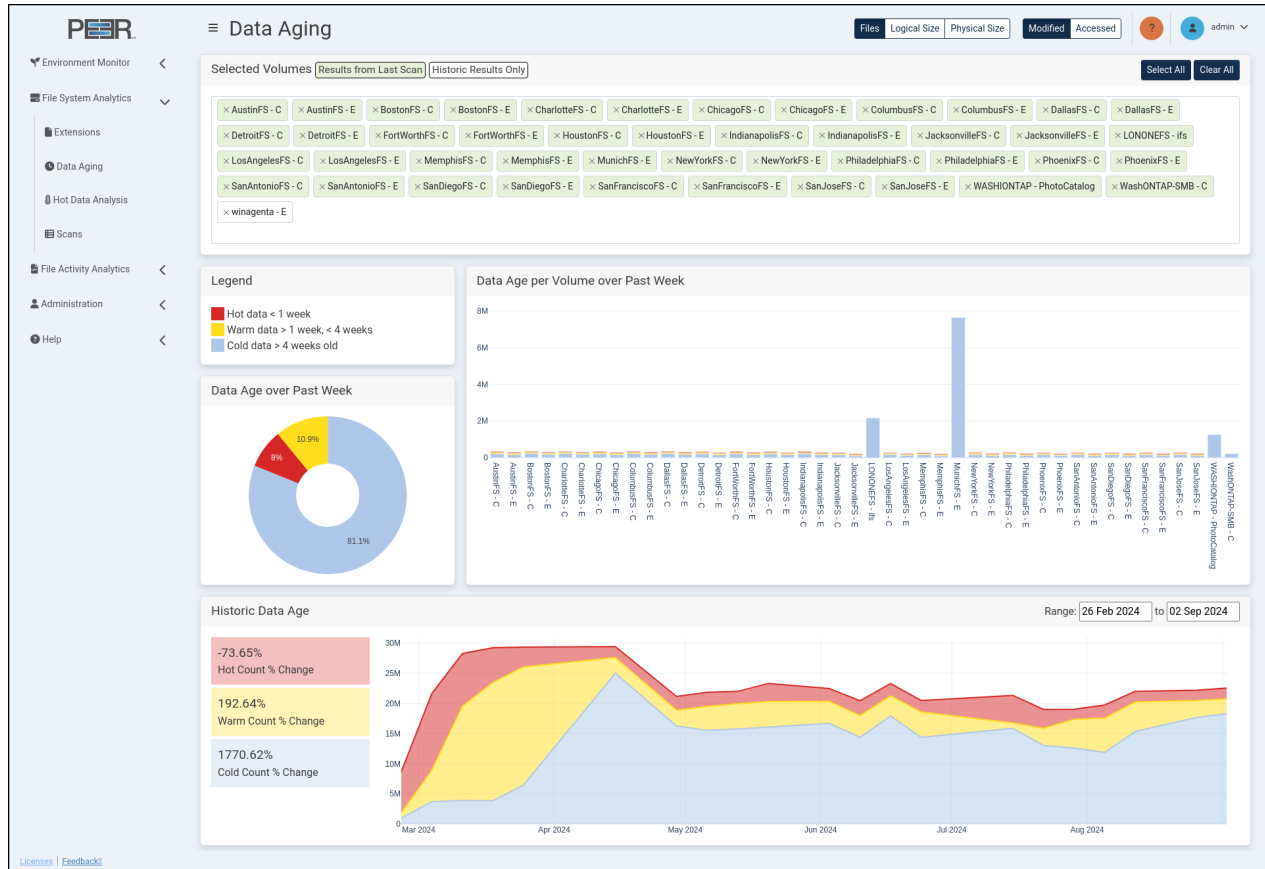
Card	Description
Selected Volumes	<p>This card filters the volumes currently selected for analysis. Selected volumes are sorted into two categories: Results from Last Scan and Historic Results Only. Volumes with recent scans are shown in green, while volumes with no recent scans are shown in white. These white-labeled volumes do not contribute to page elements displaying current data but are included when analyzing historic trends.</p> <p>Use these options to modify which volumes are selected:</p> <ul style="list-style-type: none"> • Select All: Select all available volumes. • Clear All: Deselect all volumes. • Individual Volume Search: Search for and add a volume by typing the name in the Selected Volumes field and selecting the appropriate volume from the drop-down list. • Individual Volume Removal: Click the X next to a volume name to remove that specific volume.
Volumes	<p>Displays a treemap of storage devices across the PeerGFS environment and their volumes. The treemap uses nested rectangles, arranged from largest in the top left to smallest in the bottom right, to visualize storage volumes. Each nested rectangle represents a volume, with size proportional to the data it represents.</p> <p>The size of each volume in the treemap is determined by either the total number of files or the total size of the files, depending on the Group By controls selected at the top of the page.</p> <p>The colors of the rectangles indicate the percentage of storage used, with the adjacent color scale identifying the percentage. Each storage device in the treemap has its own color. If a storage device also hosts an Agent, the color will be consistent across the PeerIQ interface.</p> <ul style="list-style-type: none"> • Click a nested rectangle to focus on that volume. The other cards will be updated to show data only for the selected item. Click again to return to the previous treemap view. • Hover over an element within the treemap to display the total number of files, the total logical size, and the total physical size, and for the current selection. <p>Use the Filters Extensions dropdown below the treemap to filter the data on the page to show only selected file extensions or extension types, based on the controls selected at the top of the page. The dropdown displays all file extensions or extension types present within the PeerGFS environment.</p>

Card	Description
Selection	Identifies which element is selected in the treemap.
Total Files	Displays the total number of files in the current selection.
Unique Extensions or Unique Extension Types	Displays the total number of unique extensions or extension types, based on the Group By controls selected at the top of the page.
Details by File Count (Top 10) or Details by File Logical Size (Top 10) or Details by File Physical Size (Top 10)	<p>Displays a table of the extensions or extension types within the currently selected volumes, based on the Group By controls selected at the top of the page, as well as the Files/Logical Size/Physical Size controls. The table shows the top 10 extensions or extension types when no filter is applied; otherwise, it displays those that match the filter. Click any column heading to sort by that column. Toggle the checkbox in the first column to show or hide the segments in the pie chart and the traces in the line graph. The table displays the following information for each extension or extension type:</p> <ul style="list-style-type: none"> • Color: The color used to identify the corresponding segment in the pie chart and trace in the line graph matching this extension or extension type. • Extension: Displays the file extension. The value <i>Others</i> represents extensions outside of the top 10, and <i>No Extension</i> represents files without a file extension. This column is only shown when Group by Extension is selected. • Type: The file type category. • File: The total number of files for this extension or type. • Size: The total size of the files with this extension or type.

Card	Description
Distribution of Extensions by File Count/File Logical Size/File Physical Size (Top 10) or Distribution of Extension Types by File Count/File Logical Size/File Physical Size (Top 10)	Displays a pie chart showing the distribution of extensions or extension types within the currently selected volumes, based on the Group By controls selected at the top of the page, as well as the Files/Logical Size/Physical Size controls. The colors in the pie chart correspond to those indicated in the Details table.
File Count/File Logical Size/File Physical Size Over Time (Top 10)	Displays a line graph of the top 10 extensions or extension types within the currently selected volumes, based on the Group By controls selected at the top of the page, as well as the Files/Logical Size/Physical Size controls. This chart illustrates trends over time, with line colors corresponding to those indicated in the Details table.

7.4 Data Aging Page

The **Data Aging** page provides a detailed overview of data age within the PeerGFS environment. **Data age** refers to the time that files on your system were last accessed or modified. **Hot data** refers to files that have been recently used, whereas **cold data** refers to files that are infrequently used.



7.4.1 Data Aging Page Cards

The Data Aging page contains five cards:

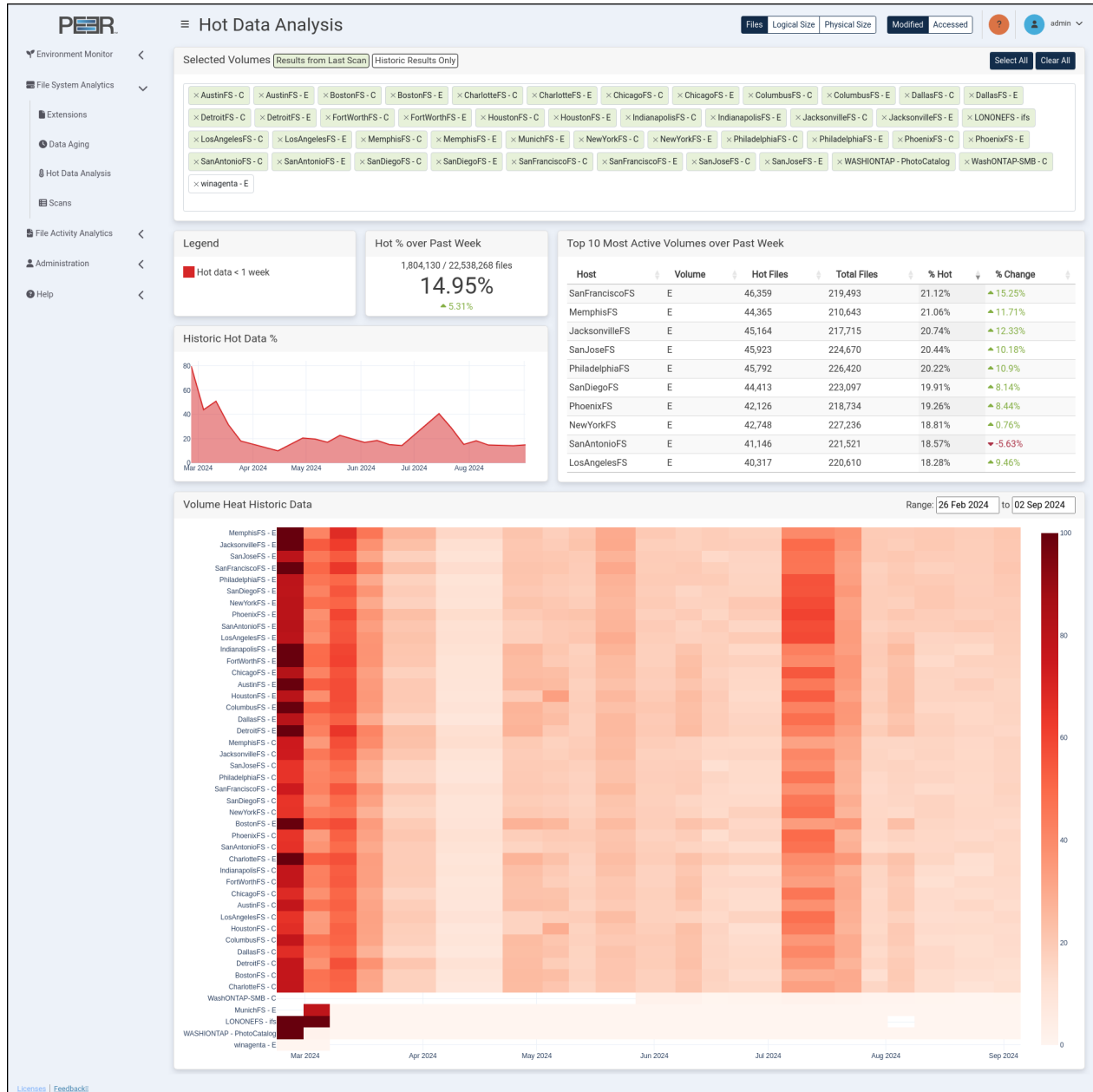
Card	Description
Selected Volumes	<p>This card filters the volumes currently selected for analysis. Selected volumes are sorted into two categories: Results from Last Scan and Historic Results Only. Volumes with recent scans are shown in green, while volumes with no recent scans are shown in white. These white-labeled volumes do not contribute to page elements displaying current data but are included when analyzing historic trends.</p> <p>Use these options to modify which volumes are selected:</p> <ul style="list-style-type: none"> • Select All: Select all available volumes. • Clear All: Deselect all volumes. • Individual Volume Search: Search for and add a volume by typing the name in the Selected Volumes field and selecting the appropriate volume from the drop-down list. • Individual Volume Removal: Click the X next to a volume name to remove that specific volume.
Legend	<p>Illustrates the color associated with each data age range and specifies the corresponding data range.</p>
Data Age per Volume over Past Week	<p>Displays a bar chart where each bar represents a volume in the PeerGFS environment. Each bar is divided into sections corresponding to the data age ranges of the items on that volume. The colors of each section match those in the Legend card.</p> <p>Use the Files/Logical Size/Physical Size controls to adjust the bar chart:</p> <ul style="list-style-type: none"> • Files: When selected, each bar shows the number of files per volume in each data age range. The height of each bar segment reflects the number of files. • Logical Size/Physical Size: When either is selected, each bar shows the size of the files per volume in each data range. <ul style="list-style-type: none"> – Logical Size: The bar chart element size reflects the total size of the files if all files were fully hydrated for each data age range. – Physical Size: The bar chart element size reflects the total size of the files in their current form for each data age range. <p>Use the Modified/Accessed controls to report on the number, logical size, or physical size of files that have been modified or accessed during the week.</p>

Card	Description
Data Age over Past Week	<p>Displays a pie chart representing the percentage of files in each data age range aggregated across all volumes in the PeerGFS environment. Use the Files/Logical Size/Physical Size controls to adjust the pie chart:</p> <ul style="list-style-type: none"> • Files: When selected, each segment represents the number of files across all volumes in each data age range. Provides insight into the distribution and quantity of files across different age ranges. • Logical Size or Physical Size: When either is selected, each segment represents the size of all files across all volumes in each data age range: <ul style="list-style-type: none"> – Logical Size: Represents the total size of files as if they were fully hydrated, meaning the total size if all data were fully present and accessible. Helps in understanding the potential storage requirements if all files were in their complete form. – Physical Size: Represents the actual size of the files in their current form on the storage system. Reflects the real storage space occupied by the files. <p>Use the Modified/Accessed controls to report on the percentage of files that have been modified or accessed during the week.</p>

Card	Description
Historic Data Age	<p>Displays a line graph of files for each data age range over time, aggregated across all volumes. This helps you to identify trends and hot spots in file modification and access. The colors for each section of the line graph match those for each data age range in the Legend card.</p> <p>You can filter the line graph to show results from a specific date range. To do this, click the date input box at the top right of the card, select a start date in the calendar view, and then choose an end date. The graph will update to display data within this range. Additionally, the values to the left of the line graph display the percentage change of hot data for each data age range.</p> <p>Use the Files/Logical Size/Physical Size controls to adjust the line graph:</p> <ul style="list-style-type: none"> • Files: When selected, the graph shows the trend of file modification or access across all volumes in each data age range. Provides insight into the distribution and quantity of files across different age ranges. • Logical Size or Physical Size: When either is selected, each line shows the trend of all file sizes across all volumes in each data range: <ul style="list-style-type: none"> – Logical Size: Represents the trend of file sizes as if all files were fully hydrated. – Physical Size: Represents the trend of file sizes in their current form on the storage system. <p>Use the Modified/Accessed controls to report on the number, logical size, or physical size of files that have been modified or accessed during the week.</p>

7.5 Hot Data Analysis Page

The **Hot Data Analysis** page provides insights into recent file activity within your PeerGFS environment. By focusing on **hot data**—files that have been interacted with recently—this analysis can help you identify files are currently in use or experiencing frequent changes. This information is valuable for various purposes such as resource allocation, performance optimization, and security monitoring.



7.5.1 Hot Data Analysis Cards

The Hot Data Analysis page contains six cards:

Card	Description
Selected Volumes	<p>This card filters the volumes currently selected for analysis. Selected volumes are sorted into two categories: Results from Last Scan and Historic Results Only. Volumes with recent scans are shown in green, while volumes with no recent scans are shown in white. These white-labeled volumes do not contribute to page elements displaying current data but are included when analyzing historic trends.</p> <p>Use these options to modify which volumes are selected:</p> <ul style="list-style-type: none"> • Select All: Select all available volumes. • Clear All: Deselect all volumes. • Individual Volume Search: Search for and add a volume by typing the name in the Selected Volumes field and selecting the appropriate volume from the drop-down list. • Individual Volume Removal: Click the X next to a volume name to remove that specific volume.
Legend	Illustrates the color associated with the data range and specifies the corresponding data range.
Hot % over Past Week	<p>Displays the percentage of files classified as hot during the current week. The colored value below indicates the percentage change compared to the previous week: green with an up arrow for an increase, and red with a down arrow for a decrease. Use the Files/Logical Size/Physical Size controls to adjust the card: Files: When selected, the card shows the percentage of the number of files that are hot during the week.</p> <ul style="list-style-type: none"> • Logical Size or Physical Size: When either is selected, each shows the percentage of the size of files that are hot during the week. <ul style="list-style-type: none"> – Logical Size: Shows the percentage of the size of files as if all were fully hydrated that are hot during the week. – Physical Size: Shows the percentage of the size of files in their current form that are hot during the week. <p>Use the Modified/Accessed controls to report on the percentage of files that have been modified or accessed during the week.</p>

Card	Description
Top 10 Most Active Volumes over Past Week	<p>Displays a table providing a snapshot of the volumes with the highest file activity within your PeerGFS environment.</p> <p>The table shows the following information for each volume:</p> <ul style="list-style-type: none"> • Host: The name of the host where the volume is stored. • Volume: The name of the volume being analyzed. • Hot Files: The number of files that are considered hot on a volume during the week. This column is visible when Files is selected as the control. • Total Files: The total number of files within your environment. This column is visible when Files is selected as the control. • Hot Size: The size of files that are considered hot on a volume during the week. This column is visible when either Logical Size or Physical Size is selected as the control, specifying the type of size being displayed. • Total Size: The size of all files within your environment. This column is visible when Logical Size or Physical Size is selected as the control, specifying the type of size being displayed. • % Hot: The percentage of files on the volume that are considered hot during the week. • % Change: The percentage of overall change in the number of hot files this week compared to the previous week. The value will be green with an up arrow for an increase, and red with a down arrow for a decrease. <p>Use the Files/Logical Size/Physical Size controls to adjust the table:</p> <ul style="list-style-type: none"> • Files: When selected, the table shows the most active volumes based on the number of files, providing insight into file activity and distribution.

Card	Description
Top 10 Most Active Volumes over Past Week (Continued)	<ul style="list-style-type: none"> • Logical Size or Physical Size: When either is selected, the table shows the most active volumes based on the size of files. <ul style="list-style-type: none"> – Logical Size: Represents the total size of files as if they were fully hydrated, meaning the total size if all data were fully present and accessible. – Physical Size: Represents the actual size of the files in their current form on the storage system. <p>Use the Modified/Accessed controls to report on the percentage of file count, logical size, or physical size that has been modified or accessed during the week.</p> <p>The default sorting of the table is determined by the selected control at the top of the page (Files/Logical Size/Physical Size)</p> <p>Click any column header to sort the table by that specific column.</p>
Historic Hot Data %	<p>Displays a line graph showing the percentage of hot files that have been changed over time, aggregated across all volumes in your PeerGFS environment. The graph provides insights into the trend of hot file activity over a historical period, allowing you to track changes and patterns in file usage and modification/access behavior across your system.</p> <p>Use the Files/Logical Size/Physical Size controls to adjust the graph:</p> <ul style="list-style-type: none"> • Files: When selected, the graph shows the trend of the percentage of hot files over time. • Logical Size or Physical Size: When either is selected, the graph shows the trend of the percentage of hot files based on their size. <ul style="list-style-type: none"> – Logical Size: Represents the total size of files as if they were fully hydrated, meaning the total size if all data were fully present and accessible. – Physical Size: Represents the actual size of the files in their current form on the storage system. <p>Use the Modified/Accessed controls to report on the percentage of files that have been modified or accessed during the week.</p>

Card	Description
Volume Heat Historic Data	<p>Displays a heatmap representing each volume in the PeerGFS environment and the percentage of files on those volumes considered hot per week. This information is valuable for identifying trends in hot data totals across all volumes, aiding in the analysis of data usage patterns and resource allocation within your environment.</p> <p>The volumes selected for analysis are identified by labels to the left of the heatmap. The heatmap colors indicate different levels of intensity or frequency, with a color scale to the right of the heatmap explaining what each color represents in terms of data magnitude or intensity.</p> <p>You can filter the heatmap to show results from a specific date range. To do this, click the date input box at the top right of the card, select a start date in the calendar view, and then choose an end date. The heatmap will update to display data within this range.</p> <p>Use the Files/Logical Size/Physical Size controls to adjust the graph:</p> <ul style="list-style-type: none"> • Files: When selected, the heatmap shows the trend of the percentage of hot files over time. • Logical Size or Physical Size: When either is selected, the heatmap shows the trend of the percentage of hot files based on their size. <ul style="list-style-type: none"> – Logical Size: Represents the total size of files as if they were fully hydrated, meaning the total size if all data were fully present and accessible. – Physical Size: Represents the actual size of the files in their current form on the storage system. <p>Use the Modified/Accessed controls to report on the percentage of files that have been modified or accessed during the week.</p>

7.6 Scans Page

The **Scans** page provides detailed information about the File System Analytics scans received by PeerIQ from the connected PMC. It is accessible only to Administrator accounts.

Scans

Received File System Analytics Scans

Period	Hosts	Volumes	Last Scan
2024-06-03 - Week 23	23	43	06-06-2024 14:59:30 UTC
2024-05-20 - Week 21	23	43	22-05-2024 11:44:06 UTC
2024-05-13 - Week 20	23	43	17-05-2024 19:05:51 UTC
2024-05-06 - Week 19	23	43	10-05-2024 18:06:12 UTC
2024-04-29 - Week 18	23	43	05-05-2024 23:59:24 UTC
2024-04-15 - Week 16	23	43	18-04-2024 14:43:10 UTC
2024-03-25 - Week 13	23	43	28-03-2024 18:48:14 UTC
2024-03-18 - Week 12	23	43	20-03-2024 19:30:46 UTC
2024-03-11 - Week 11	23	43	17-03-2024 23:59:57 UTC
2024-03-04 - Week 10	23	43	10-03-2024 23:59:52 UTC
2024-02-26 - Week 09	25	46	01-03-2024 19:28:56 UTC

Showing 1 to 11 of 11 entries

Previous 1 Next

Service Status

Refreshing Views

Latest Scan

06-06-2024 15:59:31 UTC

7.6.1 Scans Page Cards

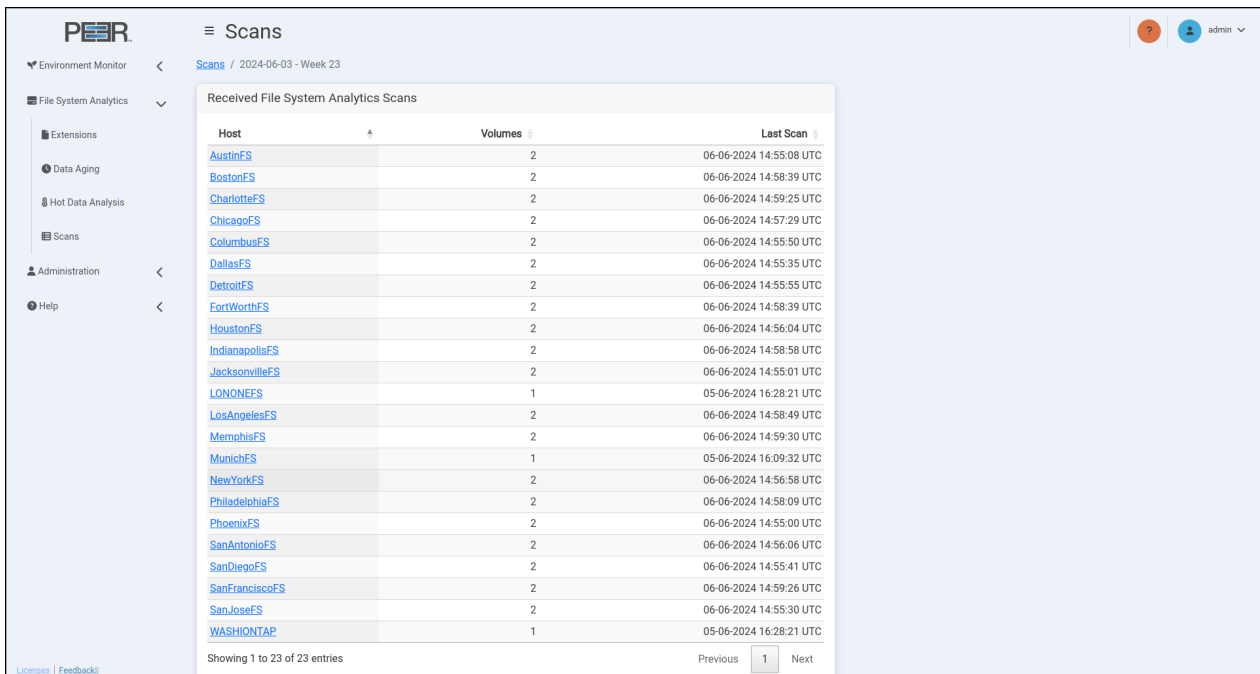
The Scans page contains three cards:

Card	Description
Received File System Analytics Scans	<p>Displays a table listing the last ten scans received by PeerIQ and includes the following information for each scan:</p> <ul style="list-style-type: none"> • Period: The time period (in weekly increments) during which the scan occurred. • Hosts: The number of hosts that sent scan data during this period. • Volumes: The number of volumes that were scanned during this period. • Last Scan: The time and date when the last scan was received for this period. <p>This table is sorted by scan period by default, with the most recent period at the top. Click any column header to sort the table by that column.</p> <p>To view more detailed information about a scan, click its date range in the Period column.</p>

Card	Description
Service Status	<p>Displays the current status of the scan service. The status can be:</p> <ul style="list-style-type: none"> • Ingesting: Scan data is currently being ingested by PeerIQ. • Refresh Queued: A refresh of the File System Analytics pages is pending. • Refreshing Views: A refresh of the File System Analytics pages is in progress. • Idle: No File System Analytics scan data is being processed. • Errors: There is a problem with processing the scan data.
Latest Scan	Displays the data and time of the latest scan.

7.6.2 Viewing Detailed Scan Information

To view more detailed information about a scan, click its date range in the **Period** column. This action displays a table with additional details about the scan, including each host that participated in the scan during this period.



The screenshot shows the PeerIQ interface with the 'Scans' section selected. A modal window titled 'Received File System Analytics Scans' is displayed, showing a table of scan data. The table has three columns: Host, Volumes, and Last Scan. The data is as follows:

Host	Volumes	Last Scan
AustinFS	2	06-06-2024 14:55:08 UTC
BostonFS	2	06-06-2024 14:58:39 UTC
CharlotteFS	2	06-06-2024 14:59:25 UTC
ChicagoFS	2	06-06-2024 14:57:29 UTC
ColumbusFS	2	06-06-2024 14:55:50 UTC
DallasFS	2	06-06-2024 14:55:35 UTC
DetroitFS	2	06-06-2024 14:55:55 UTC
FortWorthFS	2	06-06-2024 14:58:39 UTC
HoustonFS	2	06-06-2024 14:56:04 UTC
IndianapolisFS	2	06-06-2024 14:58:58 UTC
JacksonvilleFS	2	06-06-2024 14:55:01 UTC
LONGNEFS	1	05-06-2024 16:28:21 UTC
LosAngelesFS	2	06-06-2024 14:58:49 UTC
MemphisFS	2	06-06-2024 14:59:30 UTC
MunichFS	1	05-06-2024 16:09:32 UTC
NewYorkFS	2	06-06-2024 14:56:58 UTC
PhiladelphiaFS	2	06-06-2024 14:58:09 UTC
PhoenixFS	2	06-06-2024 14:55:00 UTC
SanAntonioFS	2	06-06-2024 14:56:06 UTC
SanDiegoFS	2	06-06-2024 14:55:41 UTC
SanFranciscoFS	2	06-06-2024 14:59:26 UTC
SanJoseFS	2	06-06-2024 14:55:30 UTC
WASHINGTONTAP	1	05-06-2024 16:28:21 UTC

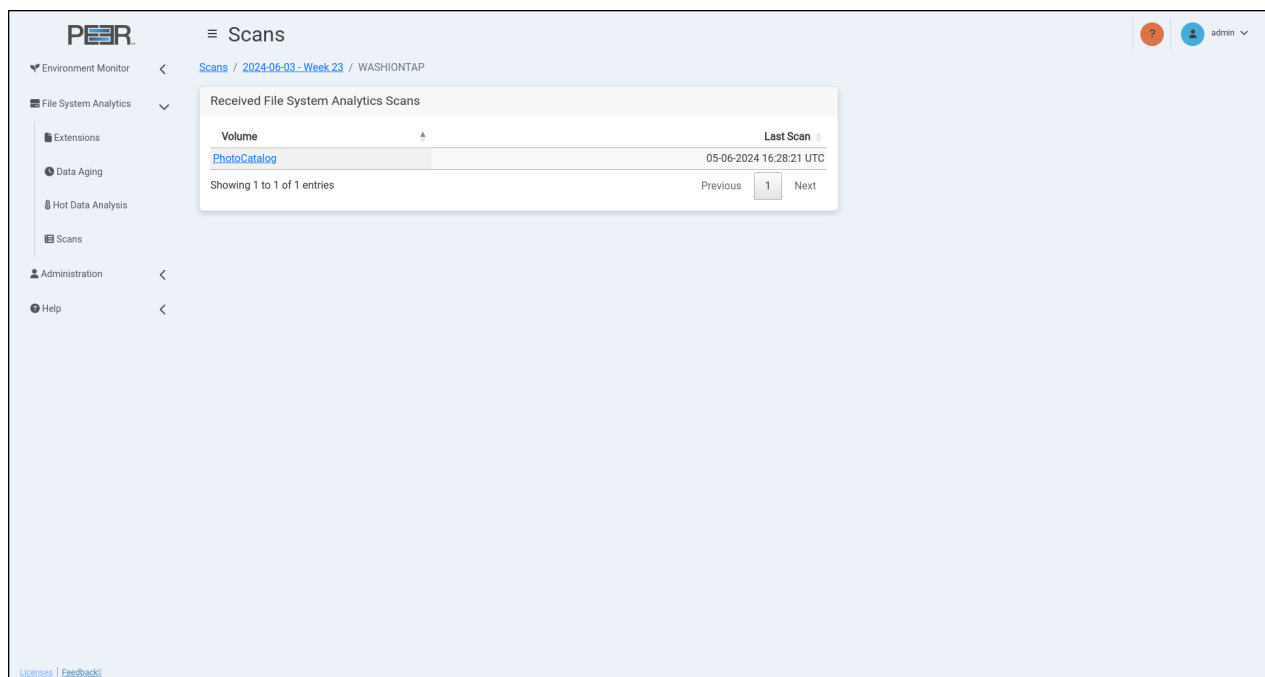
The table shows 23 entries in total. The current view shows 1 to 23 of 23 entries. Navigation buttons for 'Previous' and 'Next' are visible at the bottom of the table.

The table has the following columns:

Column	Description
Host	Displays the name of the host. To view more detailed information about a host, click its name.
Volumes	Displays the number of volumes that were scanned during this time period.
Last Scan	Displays the time and date when the last scan was received for this time period.

7.6.3 Viewing Detailed Host Information

To view more detailed information about a host, click its name in the **Host** column. This action displays a table with additional details about the host, including each volume associated with that host.

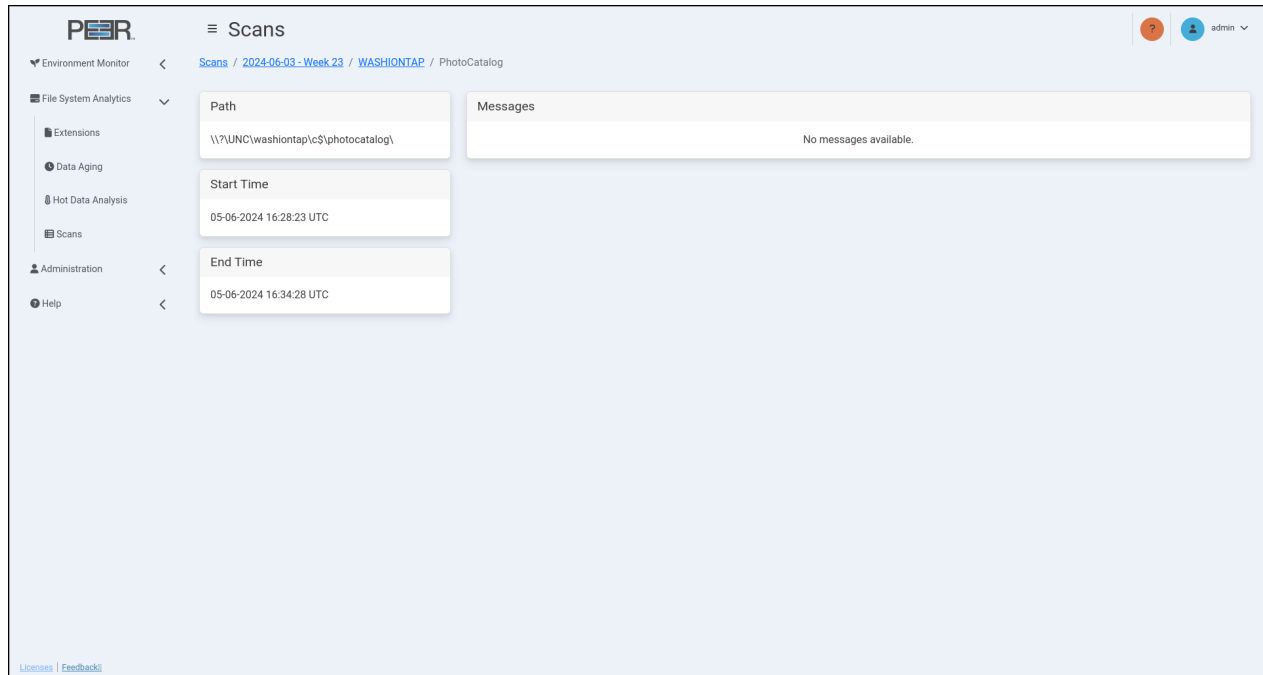


The table has the following columns:

Column	Description
Volume	Displays the name of the volume. To display more detailed information about a volume, click its name.
Last Scan	Displays the time and date when the last scan was received for this time period.

7.6.4 Viewing Detailed Volume Information

To view more detailed information about a volume, click its name in the **Volume** column. This action displays a page with cards that provide a detailed breakdown of scan information for that volume.

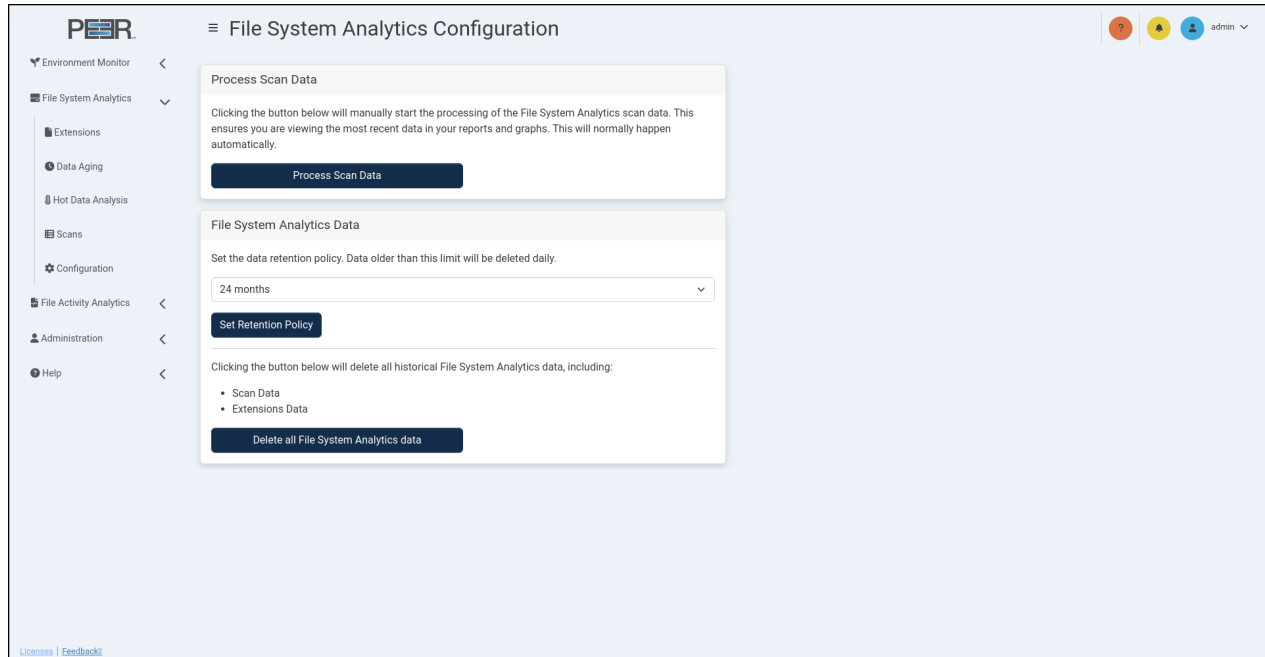


This page contains four cards:

Card	Description
Path	Displays the path of the volume being scanned.
Start Time	Displays the start time of the scan for this volume.
End Time	Displays the end time of the scan for this volume.
Messages	Displays any log entries generated for this volume during the scan.

7.7 File System Analytics Configuration

The **File System Analytics Configuration** page enables Administrators to manage file system data collected from PeerGFS agents. These settings control how long historical scan information is stored, when processing occurs, and how to clear all accumulated File System Analytics data when necessary.



7.7.1 Process Scan Data

Agents in your PeerGFS environment routinely scan file system volumes associated with active jobs. This scan data is sent to PeerIQ for processing and used throughout the File System Analytics pages.

If processing is ever interrupted, click **Process Scan Data** to manually restart processing. This ensures that the analytics pages reflect the most recent scan data. Under normal circumstances, processing occurs automatically.

7.7.2 File System Analytics Data Retention

The **File System Analytics Data** card controls how long PeerIQ retains the processed scan data used throughout the **Extensions**, **Data Aging**, **Hot Data Analysis**, and **Scans** pages.

Use the dropdown menu to select the maximum amount of historical scan data PeerIQ should store. Options range from **1 month** to **24 months**. Any scan data older than the configured limit is automatically removed during daily maintenance.

After selecting a retention period, click **Set Retention Policy** to apply it.

Note: Reducing the retention period permanently deletes all File System Analytics data older than the new limit. Increasing the retention period does not restore previously deleted data.

You may also delete all File System Analytics data at any time by clicking **Delete all File System Analytics data**. This action removes all scanned analytics history, including: - **Scan Data** - **Extensions Data**

Note: This action is irreversible. Once deleted, the data cannot be recovered.

8 Analyzing File Activity

The following section describes the **File Activity Analytics** pages, which enable you to analyze file activity by users/clients accessing the file systems in your PeerGFS environment.

File Activity Analytics has three pages:

- **Users**
- **Clients**
- **Activity**

8.1 Users Page and Clients Page

The following section of documentation applies to both the Users and Clients page.

The Users Page and Clients Page provides an overview of user and client activity across volumes monitored by PeerGFS. They summarize key file and folder operations, helping you track how data is being accessed and modified. The following activity is tracked:

Activity Type	Description
Total	The sum of all file and folder activities.
File Attribute	Indicates that a file's attributes have been changed. For example, changing a document to read-only.
File Close	Indicates that a file is closed after being accessed or edited. For example, closing a Word document.
File Create	Indicates that a new file has been created. For example, saving a new file called "notes.txt".
File Delete	Indicates that a file has been removed. For example, deleting "old.document.docx".
File Open	Indicates that a file has been opened. For example, opening "budget.xlsx".
File Read	Indicates that a file's contents have been read. For example, viewing "report.pdf".
File Rename	Indicates that a file has been renamed. For example, renaming "draft.docx" to "final.docx".

Activity Type	Description
File Security	Indicates that a file's permissions have been changed. For example, changing access rights to a document.
File Write	Indicates that file's contents have been changed. For example, editing and saving "slides.pptx".
Folder Attribute	Indicates that a folder's attributes have been changed. For example, setting a folder to hidden.
Folder Create	Indicates that a folder has been created. For example, creating a folder named "Projects".
Folder Delete	Indicates that a folder has been removed. For example, deleting the folder "Old_Backups".
Folder Security	Indicates that a folder's permissions have been changed. For example, changing access rights to a folder.
Folder Rename	Indicates that a folder has been renamed. For example, renaming "Photos_2024" to "ProductPics".

8.1.1 Client Hostname or IP Address

PeerGFS normally records the hostname of the client performing an operation. However, in certain cases, this information may not be available.

Windows File Server Local Access When a job is configured to work with a Linux File Server, PeerGFS cannot associate activity with a specific client hostname. This limitation exists regardless of the file being accessed via NFS or locally. In these cases, activity is shown as `localhost`.

Linux File Server When a job is configured to work with a Linux File Server, PeerGFS cannot associate activity with a specific client hostname. This limitation exists regardless of the file being accessed via NFS or locally. In these cases, activity is shown as `localhost`.

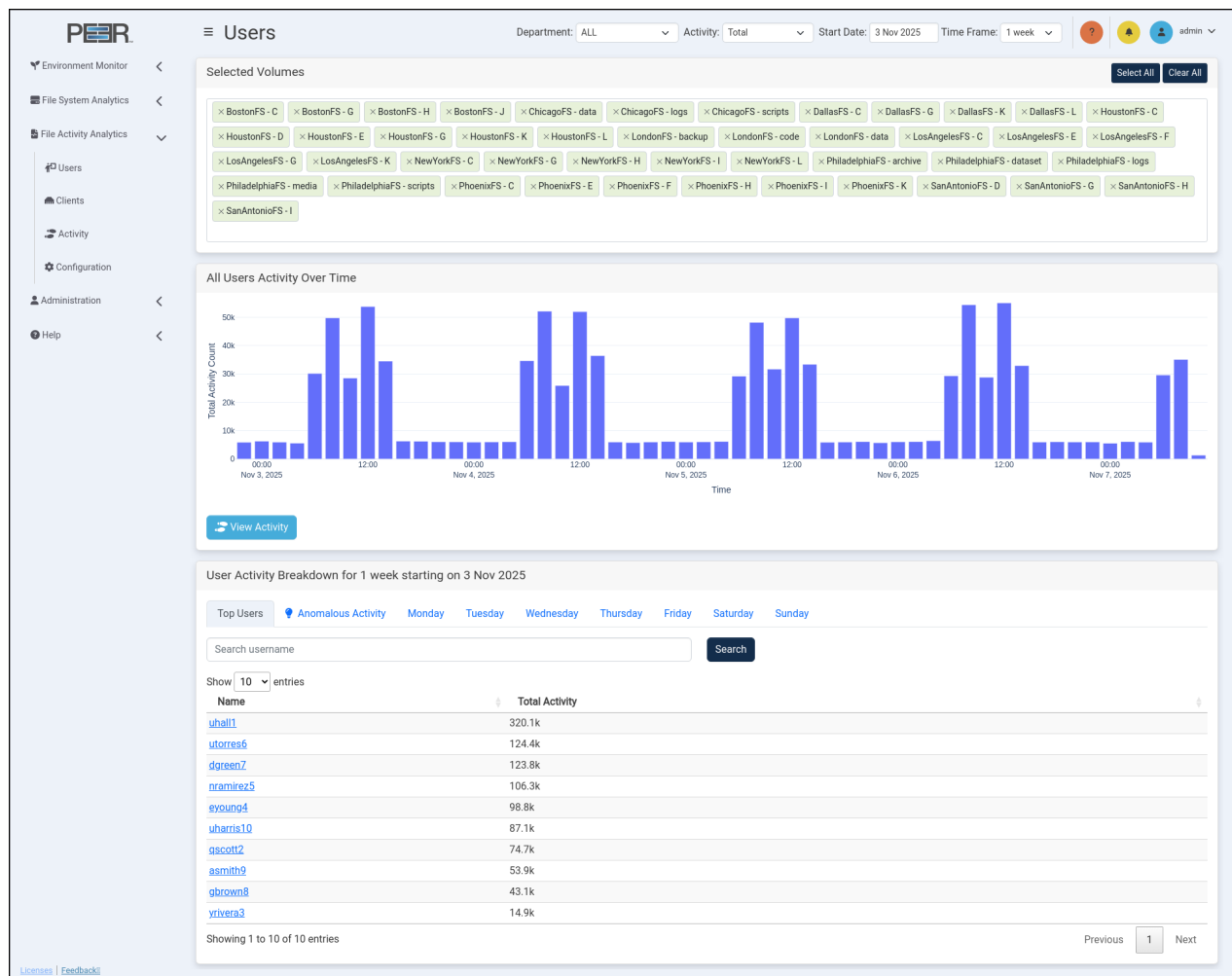
8.2 Using the FAA Page Controls

You can customize the data displayed on the Users/Clients page using the controls at the top-right of the page:

- **Department:** Filter the displayed data based on a user's department. This requires that your

LDAP environment contains the 'department' attribute and that the Resolve LDAP Information option is enabled in PeerIQ's LDAP configuration. > *Note: This filtering applies only to Users, not Clients.*

- **Activity:** Filter the displayed data to show specific activity types. See the list of tracked activities above.
- **Start Date:** Select the date from which to begin displaying data. For daily views, any date is valid. For weekly or monthly views, only Mondays can be selected.
- **Time Frame:** Define the period of data to display, starting from the selected Start Date.



8.2.1 Users Page and Clients Page Cards

The Users page and Clients page includes several cards that provide a summarized view of user and client activity:

8.2.2 Selected Volumes

This card filters the volumes currently selected for analysis. Selected volumes are sorted into two categories: Recent Activity and No Recent Activity.

Recent Activity includes volumes with data from the most recent set of real-time statistics and are shown in green.

No Recent Activity includes volumes with no activity in the latest real-time statistics and are shown in white.

Modifying Volume Selection Use these options to modify which volumes are selected:

Select All: Select all available volumes.

Clear All: Deselect all volumes.

Individual Volume Search: Search for and add a volume by typing the name in the Selected Volumes field and selecting the appropriate volume from the drop-down list.

Individual Volume Removal: Click the X next to a volume name to remove that specific volume.

8.2.3 All Users/Clients Activity Over Time

This card displays a trend chart showing user or client activity over time, based on the selected filters. The chart visualizes total activity across all monitored volumes and highlights fluctuations in user or client interactions within the selected time frame.

Hover over a data point to display detailed metrics for that specific interval, including the timestamp and corresponding activity count. This visualization helps identify patterns in usage, peak activity periods, and potential irregularities in user or client behavior.

View Activity Clicking this button opens the **Activity** page with all filters preconfigured based on the current selections, providing a visual way to access the detailed activity view.

8.2.4 Users/Clients Activity Breakdown

This section provides a breakdown of user or client activity and includes multiple tabs for viewing filtered data. Each tab features a search box for locating a specific user or client. Enter part or all of a username or hostname and click Search to display matching entries. The table below updates automatically to reflect the filtered results.

Selecting a name from the table opens a detailed view for that specific user or client, allowing deeper analysis of activity trends and behaviors.

Top Users/Clients The Top Users/Clients tab displays the most active users or clients based on the applied filters. Activities are ranked by total activity count, providing quick insight into which users or clients are generating the highest volume of file and folder operations.

Anomalous activity The Anomalous Activity tab lists users or clients whose activity patterns deviate significantly from their normal behavior. Each entry includes an anomaly score, a numerical value indicating the degree of deviation. A higher score represents more unusual activity.

Note: A minimum of one month of historical data is required for any anomaly detection results. The more data available, the more precise the scoring becomes. Anomalous activity represents behavior that is statistically irregular but not necessarily indicative of a problem.

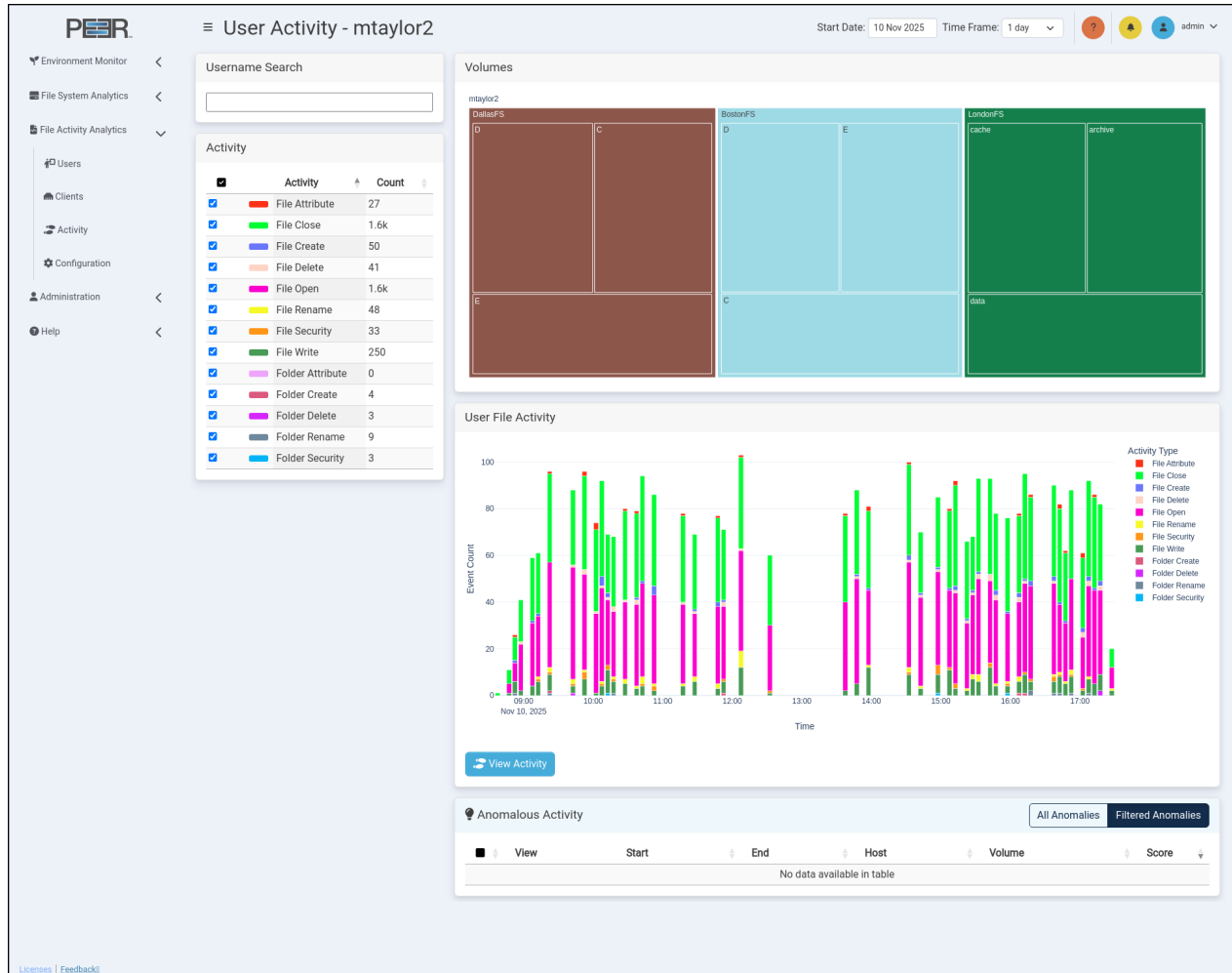
Top Users/Clients per break down This view displays the top active users or clients according to the selected time frame.

- In a 4-week view, tabs display weekly user/client activity.
- In a 1-week view, tabs display daily user/client activity.
- In a 1-day view, tabs display 4-hour user/client activity blocks.

This hierarchical breakdown allows you to analyze user and client activity trends at varying levels of granularity.

8.3 User Activity Page and Client Activity Page

The **User Activity Page** and **Client Activity Page** provide a detailed analysis of activity performed by a specific user or client on volumes monitored within PeerGFS.



8.3.1 User Activity Page and Client Activity Page Cards

The User Activity Page and Client Activity Page contain five cards.

Username/Client Search Provides a search field for selecting a user or client. Begin typing a username, hostname, or IP to see matching results. You can select a user/client from the drop-down list or enter the full username, hostname, or IP and press Enter. *Note:* If a user or client has no trackable activity on volumes being monitored by PeerGFS, they will not appear in the search results.

Volumes Displays a treemap of volumes and shares that the selected user has accessed. If no user is selected, the card will indicate that no data is available. The treemap uses nested rectangles to represent volumes and shares, arranged from largest to smallest based on access. Each rectangle's size is proportional to the amount of file activity it represents.

- Click a nested volume or folder within the treemap to focus on that volume or folder. The page will update to show file activity for the selected item.
- Click again on the same volume or folder to return to the previous treemap view.



Activity Lists all activity types tracked for the selected user. You can toggle activity types on or off to adjust the data shown in other cards.

User/Client File Activity Events Shows a bar chart of the selected user's or client's activity at the selected treemap level. The chart breaks down the number of events over the selected time frame. If no user or client is selected, this card shows **"No Data Available."**

View Activity Clicking this button opens the **Activity** page with all filters preconfigured based on the current selections, providing a visual way to access the detailed activity view.

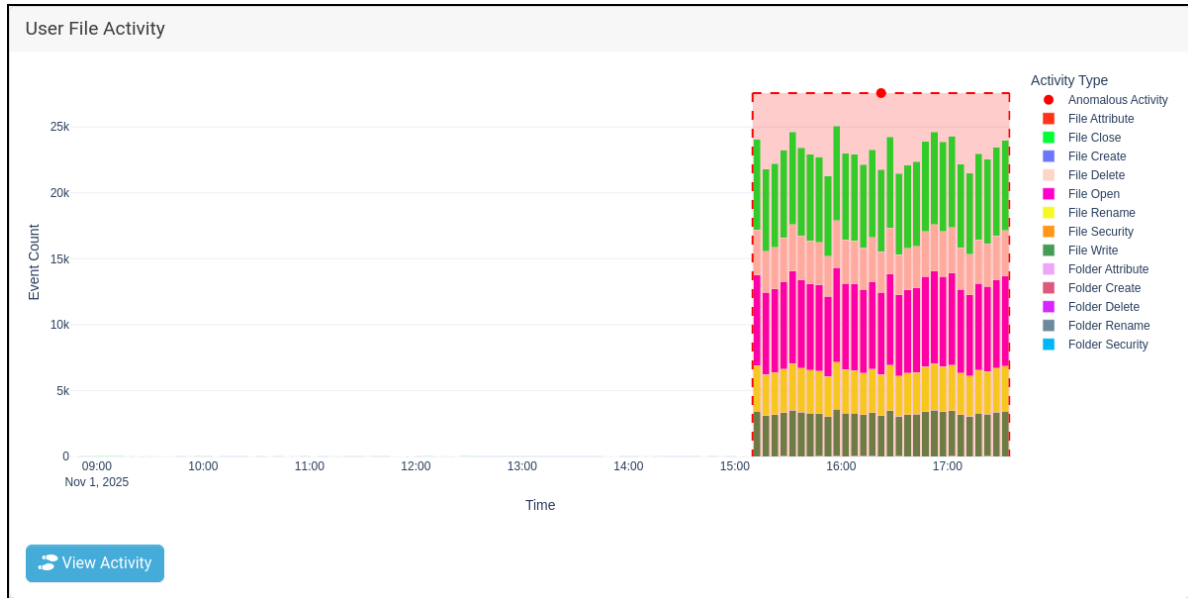
Anomalous Activity The **Anomalous Activity** tab identifies users or clients whose file activity patterns deviate significantly from their typical behavior. This enables administrators to quickly detect unusual or potentially suspicious activity across monitored volumes. While anomalies highlight unusual behavior, they may result from legitimate user actions such as bulk file transfers, maintenance operations, or software updates.

Note: The Anomalous Activity tab is available only with a PeerIQ Advanced license. If your installation does not include this license, the table will appear empty.

Anomalous Activity							All Anomalies	Filtered Anomalies
<input checked="" type="checkbox"/>	View	Start	End	Host	Volume	Score		
<input checked="" type="checkbox"/>	 	2025-11-01 15:10:00 UTC	2025-11-01 17:35:00 UTC	BostonFS	C	183.07		

Each entry in the Anomalous Activity table includes the following information:

- **View:** Clicking the magnifying glass icon updates the **User File Activity** graph and the Volumes treemap to display the selected anomaly in detail. The highlighted anomaly is outlined with a red dashed box and marked by a red circle, as shown in the example below.



- **Footprints:** Clicking the footprints icon automatically applies all related filters to generate a detailed activity report. This report provides a full breakdown of all file and folder operations that occurred during the anomaly window.
- **Start and End Time:** Indicates the time range of the anomaly. An anomaly can last for any duration, with a minimum of five minutes.
- **Host and Volume:** Displays the host system and volume where the anomalous activity was detected.
- **Anomaly Score:** Represents the numerical deviation from normal user or client behavior. Higher scores indicate a greater degree of unusual activity.

The page contains two tabs that determine which anomalies are displayed:

- **Filtered Anomalies:** Displays anomalies that match the currently applied filters and controls at the top of the page.
- **All Anomalies:** Displays the top 10 anomalies recorded for the selected user or client, regardless of applied filters.

9 Activity Page

The **Activity** page allows users to create, view, and download detailed reports of file and folder activity across monitored systems. Reports can be customized using filters for time range, users, clients, storage, files and folders, and activity types. Each report includes both high-level summaries and a full chronological event log.

Note: The Activity page is available only with a PeerIQ Advanced license. If your installation does not include this license, the Generate Report buttons will remain inactive.

Unsaved Reports

Expiring	Size	Status	Generation Time	Events
6 hours	286.7 kB	Expiring	8.3s	857
22 hours	278.5 kB	Expiring	14.6s	5
4 hours	286.7 kB	Expiring	9.2s	747

Showing 1 to 3 of 3 entries

Saved Reports

Name	Size	Generation Time	Events
File Creates Engineering Dept Audit LondonFS 2025	6.0 MB	5.0s	42.5k
PNG File analysis 01 2025	57.8 MB	24.4s	417.4k
File Rename Security Changes 2025-10-23	286.7 kB	2.3s	750
Operation Trend By User Boston FS 04	286.7 kB	8.9s	840

Showing 1 to 4 of 4 entries

9.1 Overview

The Activity page is accessible to all users. Any report generated, whether saved or unsaved, is visible to all users. Reports can be created for short-term review or saved for long-term reference. Each report provides both aggregate totals (such as event counts per user or storage host) and full event-level detail.

9.2 Filters

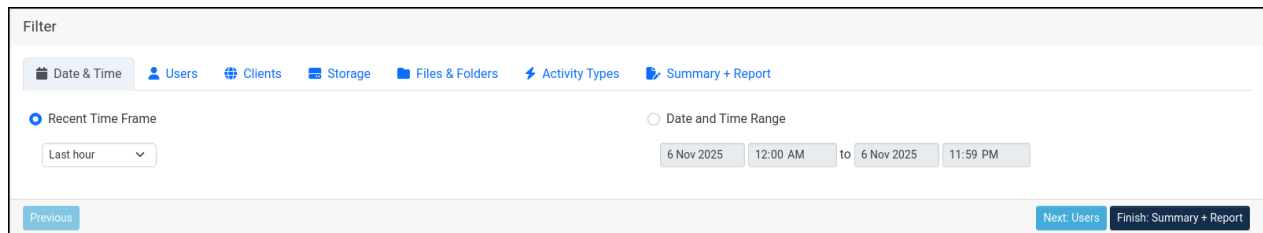
The top portion of the Activity page functions as a **guided wizard**, allowing users to configure their report step-by-step. Each tab in the filter row corresponds to a category, and you can progress by

selecting **Next** or click directly on a tab to adjust specific criteria. You may return to previous tabs at any time using the **Previous** button or by selecting a tab directly.

The available filter tabs are:

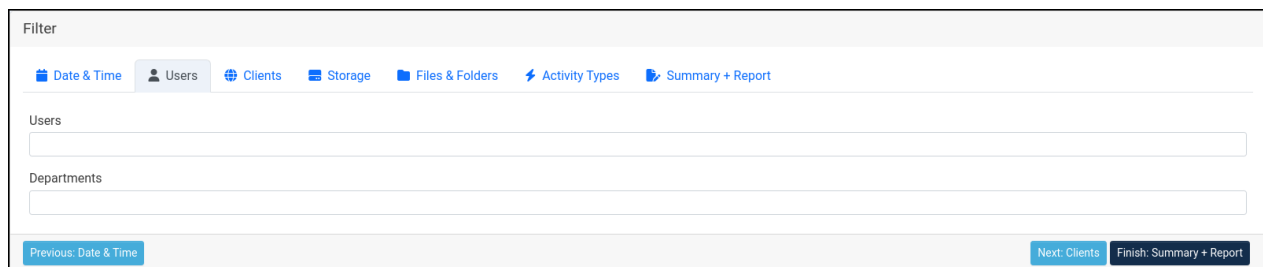
9.2.1 Date & Time

Defines the time range for captured activity. Users may select a **Recent Time Frame** (for example, *Last hour*) or specify a custom **Date and Time Range**.



9.2.2 Users

Filters by user accounts. The **Users** and **Departments** fields support **type-ahead search**, as you begin typing, PeerIQ displays matching users or departments automatically.



9.2.3 Clients

Filters by connected client systems. The **Clients** field also supports **type-ahead search** for quick selection. Depending on network configuration, both **IPv4** and **IPv6** addresses are supported. CIDR address ranges are supported in standard notation, for example 10.10.10.1/24. In cases where applications are performing file operations locally on a monitored file server, loopback addresses such as 127.0.0.1 or ::1 will appear.

The screenshot shows the 'Filter' interface with the 'Clients' tab selected. The navigation bar includes 'Date & Time', 'Users', 'Clients', 'Storage', 'Files & Folders', 'Activity Types', and 'Summary + Report'. Below the navigation bar, there is a 'Clients' input field. At the bottom, there are three buttons: 'Previous: Users', 'Next: Storage', and 'Finish: Summary + Report'.

9.2.4 Storage

Filters activity by storage hosts and volumes. Both **Storage Hosts** and **Volumes** fields support **type-ahead search**. Begin typing to see matching names or identifiers.

The screenshot shows the 'Filter' interface with the 'Storage' tab selected. The navigation bar includes 'Date & Time', 'Users', 'Clients', 'Storage', 'Files & Folders', 'Activity Types', and 'Summary + Report'. Below the navigation bar, there are two input fields: 'Storage Hosts' and 'Volumes'. At the bottom, there are three buttons: 'Previous: Clients', 'Next: Files & Folders', and 'Finish: Summary + Report'.

9.2.5 Files & Folders

Specifies which files or folders are included. The **Folders**, **Files**, and **Extensions** fields all support **type-ahead search**. The **File Name** and **Extension** filters are mutually exclusive—only one may be active at a time.

Selecting **Include temp files in suggestions** expands the filter to include system and application-generated temporary file patterns such as:

`*.tmp`, `~$*`, `~*.*`, `*.$$$$`, `*.ac$`, `*.sv$`, `._*`, `atmp*`.

This is useful for analyzing activity involving creating or modifying temporary working files (for example, Microsoft Office save operations).

The screenshot shows the 'Filter' interface with the 'Files & Folders' tab selected. The navigation bar includes 'Date & Time', 'Users', 'Clients', 'Storage', 'Files & Folders', 'Activity Types', and 'Summary + Report'. Below the navigation bar, there is a 'Folders' input field. Below that, there are two radio buttons: 'Files' (selected) and 'Extensions'. Below the 'Files' radio button, there is an 'Include temp files in suggestions' checkbox. At the bottom, there are three buttons: 'Previous: Storage', 'Next: Activity Types', and 'Finish: Summary + Report'.

9.2.6 Activity Types

Determines which categories of file and folder events are included.

File activity: Open, Close, Create, Delete, Rename, Write, Attribute, and Security. **Folder activity:** Create, Delete, Rename, Attribute, and Security.

Selecting **All File Activity** or **All Folder Activity** includes every respective event type.

Filter

[Date & Time](#)
[Users](#)
[Clients](#)
[Storage](#)
[Files & Folders](#)
[Activity Types](#)
[Summary + Report](#)

☒ All File Activity
 ☒ All Folder Activity

☒ Open
 ☒ Close
 ☒ Create
 ☒ Delete
 ☒ Rename
 ☒ Write
 ☒ Attribute
 ☒ Security

☒ Coalesce Events

[Previous: Files & Folders](#)
[Next: Summary + Report](#)
[Finish: Summary + Report](#)

Coalesced Events When enabled, **Coalesce Events** simplifies repetitive or system-generated activity sequences into a single, meaningful event. PeerIQ identifies patterns, such as those produced by Microsoft Office—and converts them into a more readable form.

For example, saving a Word document generates the following raw events:

Event	File
FILE_CREATE	~WRD0002.tmp
FILE_WRITE	~WRD0002.tmp
FILE_SECURITY	~WRD0002.tmp
FILE_RENAME	manual.docx -> ~WRL0003.tmp
FILE_RENAME	~WRD0002.tmp -> manual.docx
FILE_ATTRIBUTE	~WRL0003.tmp
FILE_DELETE	~WRL0003.tmp

With **Coalesce Events** enabled, these are condensed into:

Event	File
FILE_WRITE	manual.docx

This makes the resulting report easier to interpret by showing the actual user action rather than

low-level application IO. Because coalescing requires additional pattern analysis, enabling this option can increase the time required to generate reports, especially in environments with a high volume of Microsoft Office document activity.

9.3 Summary + Report

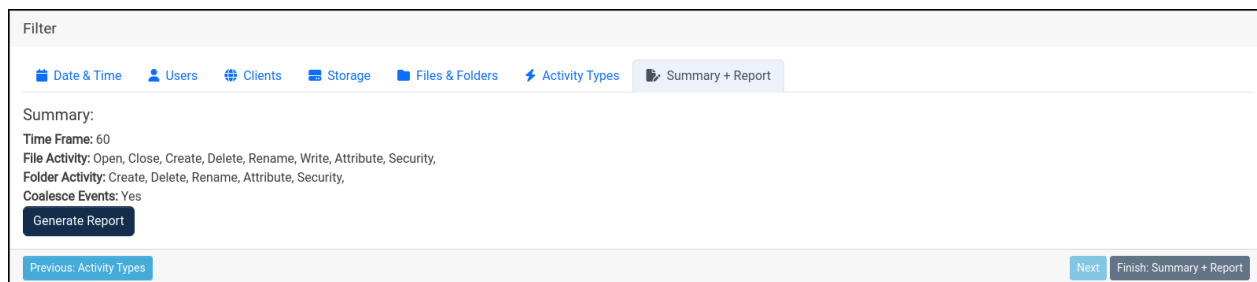
The final step in the wizard is the **Summary + Report** tab. This tab displays an overview of all filters selected during setup, including:

- Time Frame
- File Activity and Folder Activity settings
- Coalesce Events configuration

From here, users can review their selections before generating a report.

Click **Generate Report** to begin report creation. Large reports—particularly those covering broad time ranges or multiple users, volumes, or storage hosts—may take **over an hour to generate**. To minimize generation time and improve clarity, it is recommended to use the most **precise and narrow filters possible**.

Once generation begins, a new entry will appear in the **Unsaved Reports** table showing its progress.



9.4 Unsaved and Saved Reports

Below the filter section, two tables display available reports: **Unsaved Reports** and **Saved Reports**. Both share common controls:

- The **bin icon** deletes a report.
- The **eye icon** opens a report for viewing.

9.4.1 Unsaved Reports

- Contain reports in progress or temporarily stored.
- Reports in progress show one of three statuses: *Generating*, *Coalescing*, or *Building Views*.
- Reports that are still processing do not display an expiration time.
- Once finished, unsaved reports automatically expire **24 hours** after completion.
- To preserve a report, click the **Save** (disk) icon, this moves it to the **Saved Reports** table.
- Click the **eye** icon to view the report.

9.4.2 Saved Reports

- Contain reports explicitly saved by a user.
- Saved reports do **not** expire and remain available until deleted.
- Each record shows the report's **Name**, **Size**, **Generation Time**, and **Event Count**.
- Click the **eye** icon to view the report or the **bin** icon to delete it.

10 File Activity Report

The **File Activity Report** page displays the results of a report generated from the **Activity** page. Reports can be accessed directly after creation or opened later from either the **Unsaved Reports** or **Saved Reports** tables.

Each report provides a static snapshot of user and client file activity based on the filters defined in the Activity page wizard. The selected filters are shown at the top of the report for easy reference.

File Activity Report

Time Frame: 60
 Download Delete Save This report expires in 22 hours

File Activity: Open, Close, Write, Create, Delete, Rename, Security, Attribute
 Folder Activity: Create, Delete, Rename, Security, Attribute
 Coalesce Events: Yes

Users & Clients

User	Events	Clients
vallen6	6	192.168.1.6
kwilson4	4	192.168.1.4
system1	4	fe80::1:1
utaylor9	3	fe80::1:9
sroberts7	2	fe80::1:7

Showing 1 to 5 of 6 entries

Storage Hosts & Volumes

Storage Host	Events	Volumes
LondonFS	10	data, archive, cache
BostonFS	8	E, C, D
DallasFS	2	C

Showing 1 to 3 of 3 entries

Files & Folders

Storage Host	Volume	File	Events
BostonFS	E	docs/Floor Plan Sample.dwg	3
LondonFS	archive	docs/document.pptx	2
LondonFS	cache	docs/excel.doc.xlsx	2
LondonFS	archive	docs/Presentation1.pptx	2
BostonFS	C	docs/document.pptx	2

Showing 1 to 5 of 12 entries

Events

Show 10 entries

Time	User	Client	Storage Host	Volume	Folder	File	Event
2025-11-11 15:56:38 UTC	sroberts7	fe80::1:7	LondonFS	cache	docs	excel.doc.xlsx	FILE_CREATE
2025-11-11 15:56:46 UTC	sroberts7	fe80::1:7	LondonFS	cache	docs	excel.doc.xlsx	FILE_WRITE
2025-11-11 16:02:56 UTC	kwilson4	192.168.1.4	BostonFS	E	docs	Floor Plan Sample.dwg → Floor Plan Sample.bak	FILE_RENAME
2025-11-11 16:02:56 UTC	kwilson4	192.168.1.4	BostonFS	E	docs	Floor Plan Sample.dwg	FILE_CREATE
2025-11-11 16:02:56 UTC	kwilson4	192.168.1.4	BostonFS	E	docs	Floor Plan Sample.dwg	FILE_WRITE
2025-11-11 16:05:09 UTC	mtaylor2	192.168.1.2	LondonFS	data	docs	file1.txt	FILE_WRITE
2025-11-11 16:10:09 UTC	kwilson4	192.168.1.4	BostonFS	D	docs	Presentation1.pptx	FILE_WRITE
2025-11-11 16:17:56 UTC	vallen6	192.168.1.6	DallasFS	C	docs	file1.txt	FILE_WRITE
2025-11-11 16:24:45 UTC	utaylor9	fe80::1:9	LondonFS	data	docs	newword1.docx	FILE_WRITE
2025-11-11 16:28:49 UTC	vallen6	192.168.1.6	BostonFS	C	docs	document.pptx	FILE_CREATE

Showing 1 to 10 of 20 entries

This report was created in 5.08 seconds

[Licenses](#) | [Feedback](#)

10.1 Overview

The File Activity Report organizes activity into related categories, including users, clients, storage hosts, volumes, files, folders, and events. Each card on the page presents a different aspect of the report. All displayed data represents the state at the time of report generation and does not update dynamically.

The report header displays the configured time frame, active filters, and available actions. The following buttons are shown:

- **Download:** Exports the complete report data as a compressed ZIP file. The ZIP archive contains individual CSV files for each section of the report, including:

```
clients.csv
events.csv
files.csv
folders.csv
hosts_volumes.csv
users.csv
```

Each CSV file corresponds to one of the cards described below.

- **Delete:** Permanently removes the report.
- **Save:** Opens a dialog box allowing the user to assign a name to the report. Once saved, the report is moved to the **Saved Reports** table and no longer expires.

If the report remains unsaved, a message displays the remaining time until expiration. Unsaved reports automatically expire 24 hours after creation, as described in the **Activity Page** section.

10.1.1 Viewing truncated values with the eye icon

Many columns will shorten long values and display an ellipsis to fit the table. Clicking the **eye icon** reveals the full contents of the truncated field. For example, in the **Clients** column of the **Users & Clients** table, a user may have activity from many IP addresses that do not fit in the cell. In that case, the column shows an ellipsis, and the eye icon will display the complete list. The eye icon behaves this way anywhere long values are truncated.

10.2 Users & Clients

The **Users & Clients** card lists all users and clients involved in file or folder activity during the selected time frame. This section provides the total number of events per user and the associated client systems from which the activity originated.

10.3 Storage Hosts & Volumes

The **Storage Hosts & Volumes** card summarizes the distribution of activity across all monitored storage systems. Two tabs are available:

- **Hosts:** Displays each storage host and the total number of recorded events.
- **Volumes:** Shows the corresponding volumes for each host and the event count per volume.

These two views help identify where activity was most concentrated within the environment.

10.4 Files & Folders

The **Files & Folders** card lists the individual files and folders associated with events in the report. Two tabs are available:

- **Files:** Lists all files where activity occurred, along with their storage host, volume, and number of events.
- **Folders:** Lists the affected folders using the same structure.

This information allows users to quickly identify which specific files or directories experienced notable activity during the report period.

10.5 Events

The **Events** card presents the full chronological record of actions captured within the report. Each row represents a single file or folder event and includes the following details:

- **Time:** The timestamp of the event.
- **User:** The user account that initiated the action.
- **Client:** The client system associated with the activity.
- **Storage Host:** The host where the event occurred.
- **Volume:** The volume on the storage host.
- **Folder:** The folder path where the file resides.
- **File:** The file name involved in the event.
- **Event:** The specific file or folder action, such as FILE_CREATE, FILE_WRITE, or FILE_DELETE.

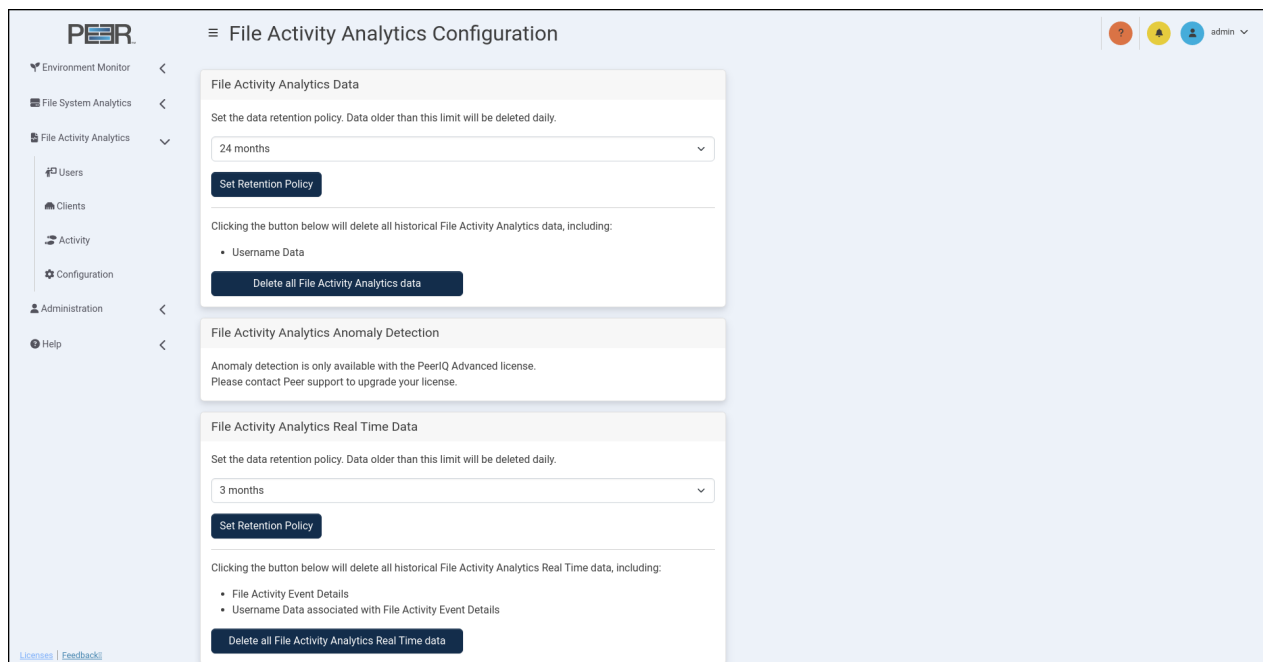
The events listed in this table reflect all filters applied at report generation time. The report footer displays the total time required to generate the report.

10.6 Exported Data

When the **Download** button is selected, the system compiles the contents of all report sections into a ZIP file containing CSV exports. Each CSV file matches its respective on-screen table, preserving column order and data structure. These files can be imported into external analysis tools for further review or integration with third-party reporting systems.

10.7 File Activity Analytics Configuration

The **File Activity Analytics Configuration** page enables Administrators to manage how long PeerIQ retains activity data, control anomaly-detection settings, and delete historical data when necessary. These settings apply to all file and folder activity collected from the PeerGFS environment.



10.7.1 File Activity Analytics Data Retention

The **File Activity Analytics Data** card controls retention of the aggregated data used by the **Users**, **Clients**, and **Activity** pages.

Use the dropdown menu to select the maximum amount of historical data PeerIQ should store. Options range from **1 month** to **24 months**. Any data older than the configured limit is automatically removed during daily maintenance.

After selecting a retention period, click **Set Retention Policy** to apply it.

Note: Reducing the retention period permanently deletes all File Activity Analytics data that exceeds the new limit. Increasing the retention period does not restore previously deleted data.

You may also delete all File Activity Analytics data at any time by clicking **Delete all File Activity Analytics data**. This action removes all stored analytics history, including **Username Data** associated with that history.

Note: This action is irreversible. Once deleted, the data cannot be recovered.

10.7.2 File Activity Analytics Anomaly Detection

The **File Activity Analytics Anomaly Detection** option enables automatic analysis of user and client file behavior. When enabled, PeerIQ uses anomaly models that are refreshed daily. New real-time statistics are analyzed every 5 minutes to detect activity patterns that deviate from normal usage.

To enable or disable anomaly detection, select or clear the **Enable Anomaly Detection** checkbox, then click **Save** to apply the change.

Note: Disabling anomaly detection pauses the generation of new anomaly scores and prevents new anomalies from being identified until the feature is re-enabled.

If the PeerIQ installation does not include an Advanced license, this feature is unavailable. In this case, the following message is displayed instead of the configuration controls:

Note: Anomaly detection is only available with the PeerIQ Advanced license. Please contact Peer Software to upgrade your license.

10.7.3 File Activity Analytics Real-Time Data

The **File Activity Analytics Real-Time Data** card allows administrators to manage the lifecycle of real-time activity records collected by PeerIQ. This includes deleting all stored real-time data and configuring a **data retention policy**. Use the dropdown menu to specify how long PeerIQ should retain real-time event information. Available options include **1 month**, **2 months**, and **3 months**. Any real-time activity data older than the selected retention period is automatically removed during daily maintenance.

After selecting a retention period, click **Set Retention Policy** to apply it.

Note: Reducing the retention period immediately deletes any real-time activity data older than the new limit. Restoring a longer retention period later does not recover previously deleted data.

Clicking **Delete all File Activity Analytics Real-Time data** permanently deletes all stored information associated with real-time file activity, including:

- **File Activity Event Details**
- **Username Data** associated with File Activity Event Details

This operation clears all historical data from the real-time analytics components.

Note: This action is irreversible. Once deleted, the data cannot be recovered.

11 Administering PeerIQ

The following section describes the **Administration** pages, which can be accessed only when using your Administrator account. These pages enable you to manage users, configure the connection to the broker, configure PeerIQ, and manage PeerIQ logs, and other diagnostic information.

The nine Administration pages are:

- Broker Configuration
- Email Configuration
- LDAP Configuration
- Logs
- Software Status
- Software Updates
- System Configuration
- System Stats
- User Accounts

11.1 Broker Configuration Page

For information about the Broker Configuration page, see the section Setting Up Communication between the PMC and PeerIQ. The section first explains how the broker facilitates information exchange between PeerIQ and Peer Management Center, and then provides instructions on configuring a connection to the broker.

11.2 Email Configuration Page

The **Email Configuration** page allows administrators to define the settings used by PeerIQ to send system-generated email notifications, such as alerts or user messages.

11.2.1 Overview

PeerIQ supports email delivery through an external SMTP server. The configuration includes the SMTP host and port, encryption type, authentication method, and sender address.

After entering the necessary information, click **Save** to store the settings.

The configuration can be verified using the **Test Email Configuration** card at the bottom of the page.

11.2.2 SMTP Configuration Fields

Field	Description
SMTP Server	The hostname or IP address of the mail server used for sending email.
SMTP Port	The port number used by the mail server (for example, 25, 465, or 587).

Field	Description
Encryption	Select the encryption type for email transmission. Options include None , SSL , and STARTTLS .
From Address	The email address used as the sender for PeerIQ notifications.

11.2.3 Authentication Methods

PeerIQ supports three types of authentication: **None**, **Basic**, and **OAuth 2.0**.

None Select **None** when your SMTP server does not require authentication. Only the basic SMTP server, port, encryption, and **From Address** fields are needed.

Basic Authentication Select **Basic** to connect using a username and password.

The screenshot displays the PeerIQ web interface for Email Configuration. The left sidebar shows a navigation menu with options like Environment Monitor, File System Analytics, File Activity Analytics, Administration, User Accounts, System Stats, Logs, System Configuration, Broker Configuration, LDAP Configuration, Email Configuration (selected), Software Updates, Software Status, and Help. The main content area is titled 'Email Configuration' and contains the following fields:

- SMTP Server**: Text input field.
- SMTP Port**: Text input field.
- Encryption**: Dropdown menu with 'None' selected.
- Authentication**: Dropdown menu with 'Basic' selected.
- SMTP Username**: Text input field.
- SMTP Password**: Text input field.
- From Address**: Text input field with 'example@example.com' entered.

Below these fields is a 'Save' button. Underneath is a 'Test Email Configuration' section with a 'To address' field (containing 'example@example.com') and a 'Test' button. The bottom left corner of the interface has links for 'Licenses' and 'Feedback'.

When this method is chosen, the following additional fields appear:

Field	Description
SMTP Username	The username for the SMTP account.
SMTP Password	The password associated with the SMTP account.

After completing all fields, click **Save** to apply the configuration.

OAuth 2.0 Authentication (Office 365) Select OAuth 2.0 when using Microsoft 365 (Office 365) or Exchange Online. This method applies to all cloud-hosted mailboxes authenticated through Microsoft Entra ID. This method provides secure, token-based authentication instead of storing user credentials.

The screenshot shows the PeerIQ 'Email Configuration' page. On the left is a navigation menu with options like Environment Monitor, File System Analytics, File Activity Analytics, Administration (expanded), User Accounts, System Stats, Logs, System Configuration, Broker Configuration, LDAP Configuration, Email Configuration (selected), Software Updates, Software Status, and Help. The main content area is titled 'Email Configuration' and contains several input fields: SMTP Server, SMTP Port, Encryption (set to None), Authentication (set to OAuth 2.0), Provider (set to Office 365), Redirect URI (https://nginx/config/oauth2/office/callback), Client ID, Client Secret, Tenant ID, and From Address (example@example.com). A 'Save' button is at the bottom of this section. Below it is a 'Test Email Configuration' section with a 'To address' field (example@example.com) and a 'Test' button. The top right corner shows a user profile icon and the name 'admin'.

Additional fields appear when **OAuth 2.0** is selected:

Field	Description
Provider	Choose Office 365 .
Redirect URI	This value is automatically generated and must match the redirect URI registered in Microsoft Entra ID.

Field	Description
Client ID	The application (client) ID from your Microsoft Entra ID registration.
Client Secret	The client secret created during app registration.
Tenant ID	The directory (tenant) ID for your organization in Entra ID. This can be tied to either an Azure or Microsoft 365 (Office 365) subscription.
From Address	The email address used as the sender for PeerIQ notifications.

11.2.4 Example: Office 365 Configuration

When connecting PeerIQ to **Office 365** using OAuth 2.0, the recommended settings are as follows:

Field	Value
SMTP Server	smtp.office365.com
SMTP Port	587
Encryption	STARTTLS
Authentication	OAuth 2.0
Provider	Office 365

These values ensure compatibility with Microsoft's secure mail relay and token- based authentication.

11.2.5 Configuring Office 365 / OAuth 2.0 in Microsoft Entra ID

Before PeerIQ can send email using Office 365 with OAuth 2.0, an application must be registered in **Microsoft Entra ID** (formerly Azure AD).

Step 1 – Navigate to App Registrations

1. Navigate to Microsoft Entra admin center → Microsoft Entra ID → App registrations > Note:
At document creation the URL is
https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade/q
2. Select **New Registration**.

Step 2 – Create the Application

1. Enter a descriptive name such as *PeerIQ Email Integration*.
2. Under **Supported Account Types**, choose **Accounts in this organizational directory only**.
3. In **Redirect URI**, select **Web** and enter the Redirect URI displayed in your PeerIQ configuration page (for example, `https://<your_peeriq_host>/config/oauth2/office/callback`).
4. Click **Register**.

Step 3 – Gather App Details After registration, copy the following from the application overview page:

- **Application (Client) ID**
- **Directory (Tenant) ID**

In PeerIQ, these values must be entered in the **Client ID** and **Tenant ID** fields under the **Email Configuration** page when **OAuth 2.0** and **Office 365** are selected.

Step 4 – Generate a Client Secret

1. In the left menu, select **Certificates & Secrets**.
2. Under **Client Secrets**, click **New Client Secret**.
3. Provide a description and expiration duration.
4. Copy the **Value** of the secret immediately, this must be entered in the **Client Secret** field within the PeerIQ **Email Configuration** page.

Note: Once you leave this page in Entra, the Client Secret value will no longer be visible. If lost, you will need to generate a new one.

Step 5 – Assign API Permissions

1. In the left menu, select **API Permissions > Add a Permission**.
2. Choose **Microsoft Graph > Delegated Permissions**.
3. Add the following permissions:
 - Mail.Send
 - SMTP.Send
 - offline_access
 - User.Read
4. Click **Grant admin consent for your organization**.

If the **Grant admin consent** button appears **greyed out**, you may not have sufficient administrative privileges in your Microsoft Entra ID. Contact your Microsoft Entra ID administrator to complete this step.

Step 6 – Complete PeerIQ Configuration Return to the PeerIQ **Email Configuration** page and enter the following:

PeerIQ Field	Microsoft Entra ID
Client ID	Application (Client) ID
Tenant ID	Directory (Tenant) ID
Client Secret	Secret Value generated in Step 4
Redirect URI	Must match the URI used during registration
Provider	Office 365

In the **From Address** field, enter the email address of the account used to authenticate during the Microsoft 365 sign-in process.

By default, this must match the authorized Office 365 account. If your organization has granted “Send As” or “Send on Behalf” rights, you may use another address that the authenticated account is permitted to send from.

Click **Save** to apply the configuration.

11.2.6 Authorization and Redirect

After clicking **Save**, a Microsoft sign-in window will appear. Use the same Office 365 account that corresponds to the **From Address** entered in the configuration.

Once you sign in, Microsoft will ask you to grant the application permission to send email on your behalf. Approve the request to complete the OAuth 2.0 authorization process.

Upon successful authorization, PeerIQ displays a confirmation screen:

Authorization succeeded. The page will automatically redirect back to PeerIQ, confirming that the OAuth credentials have been securely stored and validated.

11.2.7 Testing the Configuration

After successful authorization, it is recommended to verify that PeerIQ can send emails using the configured account.

1. In the **Test Email Configuration** section, enter a valid destination email address in the **To Address** field.

2. Click **Test**.

PeerIQ will attempt to send a test message using the configured SMTP settings.

If successful, you will receive an email with the subject line:

This is a test email sent by PeerIQ.

Receiving this message confirms that your Office 365 configuration and authorization are functioning correctly.

11.3 LDAP Configuration

You can manage LDAP access on the **LDAP Configuration** page.

PeerIQ LDAP Configuration page. The page displays configuration options for LDAP, including fields for Active Directory, Server URL, Authentication, Service Domain, Service Username, Service Password, and User Search Base. It also includes a 'Resolve LDAP Information' section with a checkbox for resolving user and departmental information.

The LDAP Configuration page contains two cards:

Card	Description
LDAP Configuration	Use this card to configure a connection to an LDAP server.
Resolve LDAP Information	Use this card to enable user name resolution using NFS UIDs and SIDs, as well as retrieving department information from AD servers.

11.3.1 Configuring Access for LDAP Users

To enable LDAP support within PeerIQ, use the **LDAP Configuration** card. The process to enable LDAP access involves two steps:

1. Configuring LDAPS
2. Configuring the Connection to the LDAP Server

Configuring LDAPS LDAPS (Lightweight Directory Access Protocol over SSL) secures directory information exchange over an encrypted connection, ensuring data confidentiality and integrity between your server and client applications. This section provides instructions for setting up LDAPS with PeerIQ using trusted certificates.

Prerequisites:

- Ensure you have SSH and SCP tools available for this configuration process.
- Ensure you have a supported LDAP server. PeerIQ supports the following:
 - Microsoft Windows Active Directory (2016 and newer)
 - OpenLDAP
 - Red Hat Identity Management

LDAPS establishes TLS connections using the certificates present in PeerIQ's host trust store. Use one of the following methods to include certificates in the trust store.

Method 1: Using a Certificate from a Certificate Authority If you have a certificate from a certificate authority that is valid for any FQDN in the domain *.examplecompany.org, and you're using this certificate for your internal servers (e.g., adhost.examplecompany.org), the certificate will be valid. In this case, the LDAPS connection will be successful, and no further action is required.

Method 2: Using Self-Signed Certificates LDAPS will not connect using self-signed certificates unless the certificate has been imported into PeerIQ's trust store.

To import a self-signed certificate:

1. Export the certificate from the Windows AD server or copy from the Linux LDAP server as a Base-64 encoded X.509 (.CER) certificate.

2. Rename the exported file to have a .crt extension.
3. Use SCP to transfer the file onto your PeerIQ host. By default, the PeerIQ host username is peersoftware and the password is password. For example:

```
scp ./example.crt peersoftware@\<peeriq_ip\>:/tmp/example.crt
```

4. Access your PeerIQ host using SSH:

```
ssh peersoftware@\<peeriq_ip\>
```

5. Copy the .crt file to your certificate import location. Locations Below:

OS	Certificate import location
Red Hat or Rocky Linux	/etc/pki/ca-trust/source/anchors/
Ubuntu Virtual Appliance	/usr/local/share/ca-certificates/

For example for the Ubuntu Virtual Appliance:

```
sudo cp /tmp/example.crt /usr/local/share/ca-certificates/example.crt
```

6. Run the certificate import command to inform the system about the new certificate:

OS	Certificate import command
Red Hat or Rocky Linux	update-ca-trust extract
Ubuntu Virtual Appliance	update-ca-certificates

For example for the Ubuntu Virtual Appliance:

```
sudo update-ca-certificates
```

7. For the Ubuntu Virtual Appliance you can now exit the SSH console. For Red Hat/ Rocky Linux a reboot of the host running the PeerIQ software is required.

Note: LDAPS will not connect using self-signed certificates unless the certificate is imported into PeerIQ's trust store. If you encounter an error, it will be displayed as Failed to open socket within the User Interface next to the **Test** button.

Active Directory

Server URL

Authentication

LDAPS ▼

Service Domain

Service Username

Service Password

Save Test Failed to open socket

Additionally, navigating to the *Logs* from the left menu will show the error:

LDAP Socket Open Error: ("('socket ssl wrapping error: [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: unable to get local issuer certificate (_ssl.c:1131)'),")

Show 10 entries

Export to CSV

Search:

Tag	Time	Priority	Message
OverviewLogger:	2023-08-31 08:25:50	error	LDAP Socket Open Error: ("('socket ssl wrapping error: [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: unable to get local issuer certificate (_ssl.c:1131)'),")

Showing 1 to 3 of 3 entries

Previous 1 Next

Configuring the Connection to the LDAP Server Use the LDAP Configuration card to configure the connection to your Active Directory or OpenLDAP server.

The screenshot shows the PeerIQ LDAP Configuration interface. On the left is a sidebar with navigation links: Environment Monitor, File System Analytics, File Activity Analytics, Administration (expanded), User Accounts, System Stats, Logs, System Configuration, Broker Configuration, LDAP Configuration, Software Updates, Software Status, and Help. The main panel is titled 'LDAP Configuration' and contains a form. The form has a dropdown menu set to 'Active Directory'. Below it are text input fields for 'Server URL' (containing 'ldaps://dc.example.com:636'), 'Authentication' (a dropdown set to 'LDAP'), 'Service Domain' (containing 'example.com'), 'Service Username' (containing 'admin'), 'Service Password' (empty), and 'User Search Base' (a dropdown set to 'Service Domain'). At the bottom of the form are 'Save' and 'Test' buttons. Below the form is a section titled 'Resolve LDAP Information' containing a checked checkbox 'Resolve user and departmental information from the LDAP server for File Activity Analytics data views.' and a 'Save' button. The top right of the interface shows a user profile icon and the name 'admin'.

To configure the connection:

1. Using your Administrator account, open the **User Accounts** page.
2. In the **LDAP Configuration** card, select either **Active Directory** or **OpenLDAP** in the first field.
3. Fill out the remaining fields based on your selection:

For Active Directory:

- **Server URL:** The URL of the LDAP server (e.g., ldap://dc.london.local:389).
- **Authentication:** The authentication type for the LDAP connection.
- **Service Domain:** The domain for the service user account.
- **Service Username:** The username for the service user account.
- **Service Password:** The password for the service user account.
- **User Search Base:** This setting defines the starting point in the Active Directory (AD) tree where searches for user objects will begin. Selecting Service Domain will search at the start of the domain specified in the “Service Domain” field. Selecting UPN Suffix will use the search base, derived from the portion of the username following the “@” symbol, to search the domain. For example, assume your Service Domain is set to example.com. If a user’s login name is fred@management.example.com and the User Search Base is set to use the Service Domain, the search will start at DC=example,DC=com, not DC=management,DC=example,DC=com. If the User Search Base is set to use UPN Suffix, the search will start at DC=management,DC=example,DC=com.

For Open LDAP / Red Hat Identity Management (IdM) :

- **Server URL:** The URL of the LDAP server (e.g., ldap://dc.london.local:389).
 - **Service Domain:** The domain for the service user account.
 - **Service Username:** The username for the service user account.
 - **Service Password:** The password for the service user account.
 - **User Object Class:** The unique identifier for the user's object class.
 - **Username Attribute:** The unique attribute for identifying a username.
 - **User Search Base:** The root domain where users are configured.
4. Click **Test** to perform a test connection to the LDAP server.
 5. Click **Save**.

11.3.2 Resolving NFS Usernames using the Resolve LDAP Information option

The usernames displayed on File Activity Analytics pages depend on your environment's configuration. Windows-based Agents automatically resolve Security Identifiers (SIDs) to usernames for SMB client activity. However, Linux-based Agents do not automatically resolve User Identifiers (UIDs) or SIDs. PeerIQ can resolve usernames for Linux-based Agents if the UIDs and SIDs are properly mapped to usernames via LDAP or Active Directory (AD).

This section guides you through verifying your environment and configuring PeerIQ for username resolution.

Prerequisites

- An LDAP or AD server is used for user authentication.
- Users accessing NFS exports authenticate against the same LDAP/AD server used by PeerIQ.
- Linux clients must use UIDs and Group Identifiers (GIDs) provided by the LDAP/AD server.
- If using AD, ensure Unix attributes are configured.

Configuring PeerIQ for Username Resolution

Step 1: Verify LDAP Credentials in PeerIQ

1. Log in to the PeerIQ dashboard.
2. Navigate to **Administration > LDAP Configuration**.
3. Confirm that LDAP/AD server credentials are correct.

Step 2: Enable Username Resolution

1. Within the LDAP Configuration page, check **Resolve LDAP Information**.
2. Click **Save**.

Verifying Environment Configuration

Active Directory: Verifying Unix Attributes AD users must have Unix attributes configured. Verify this with the following PowerShell command:

```
Get-ADUser -Identity "User1" -Properties uidNumber, gidNumber, loginShell,
unixHomeDirectory, msSFU30NisDomain |

Select-Object uidNumber, gidNumber, loginShell, unixHomeDirectory,
msSFU30NisDomain
```

Correct output example:

```
uidNumber : 1001
gidNumber : 1001
loginShell : /bin/bash
unixHomeDirectory : /home/User1
msSFU30NisDomain : nisdomain
```

- Ensure that PeerIQ and your NFS clients belong to either the same Active Directory (AD) domain or to domains within the same AD forest that have established trust relationships.

OpenLDAP and Red Hat Identity Management Considerations Ensure that PeerIQ and all clients authenticate against the same LDAP server. If multiple LDAP servers are used, synchronize user data to maintain consistent UIDs and GIDs across the environment.

Linux Client Configuration

Verify Linux clients use LDAP/AD-provided UIDs and GIDs by checking `/etc/sss/sss.conf`:

1. Open the file:

```
sudo nano /etc/sss/sss.conf
```

2. Ensure the `[domain/default]` section includes:

```
ldap_id_mapping = False
```

3. Restart the SSSD service:

```
sudo systemctl restart sssd
```

This configuration ensures that the system directly utilizes UIDs and SIDs provided by LDAP or Active Directory (AD).

11.3.3 Resolving Active Directory (AD) Departments using the Resolve LDAP Information option

The **Department** filter shown on the File Activity Analytics pages is dependent on your environment's LDAP configuration.

This guide explains how to verify your environment settings and configure PeerIQ to resolve user departments using LDAP.

Prerequisites Ensure the following before proceeding:

- An Active Directory (AD) server configured for user authentication.
- Users authenticate using the same AD server configured in PeerIQ.
- Users have their **Department** attribute configured in the AD server. Verify this by running the following PowerShell command on the AD server:

```
Get-ADUser -Identity "jdoe" -Properties Department | Select-Object Name, Department
```

Configuring PeerIQ for Department Resolution

Step 1: Verify LDAP Credentials

1. Log into the PeerIQ dashboard.
2. Navigate to **Administration > LDAP Configuration**.
3. Confirm that your AD server credentials are valid.

Step 2: Enable Department Resolution

1. On the **LDAP Configuration** page, select the **Resolve LDAP Information** checkbox.
2. Click **Save** to apply your changes.

11.4 Logs Page

The **Logs** page displays a table of log entries and enables you to send diagnostics to Peer Software Support. It is accessible only to Administrator accounts.

The screenshot shows the PeerIQ Logs interface. On the left is a sidebar with various system monitoring and configuration options. The main panel is titled 'Logs' and features a search bar and several filter controls. At the top, there are input fields for 'Start Date' and 'End Date' (both in mm/dd/yyyy format), a 'Select log levels' button, and a 'Submit' button. To the right of these are buttons for 'Send Diagnostics', 'Save Diagnostics', and 'Download'. Below the filters, there's a 'Show 10 entries' dropdown and a search input field. The log table has four columns: Tag, Time, Priority, and Message. It lists ten log entries, all from 'OverviewLogger:' at '2025-04-25 13:18:51 UTC' with an 'info' priority and the message 'Example log message.'. At the bottom of the table, it says 'Showing 1 to 10 of 257 entries' and provides pagination links: Previous, 1, 2, 3, 4, 5, ..., 26, Next.

The Log table displays the most recent 5,000 log entries. You can:

- **Filter** the log table using the date fields and log levels.
- **Change** the number of entries displayed in the table.
- **Export** the current log view to a CSV file by clicking **Export to CSV**.
- **Search** for specific log entries within the current view.
- **Send** diagnostic information to Peer Software support.

11.4.1 Filtering Log Contents

Use the date and log level filters to refine the data displayed in the Log table.

To filter the log data:

1. Open the **Logs** page.
2. Select a start date and end date.
3. Click **Select log level**, and then select the types of log entries to be displayed.
4. Click **Submit** to enable the filters.

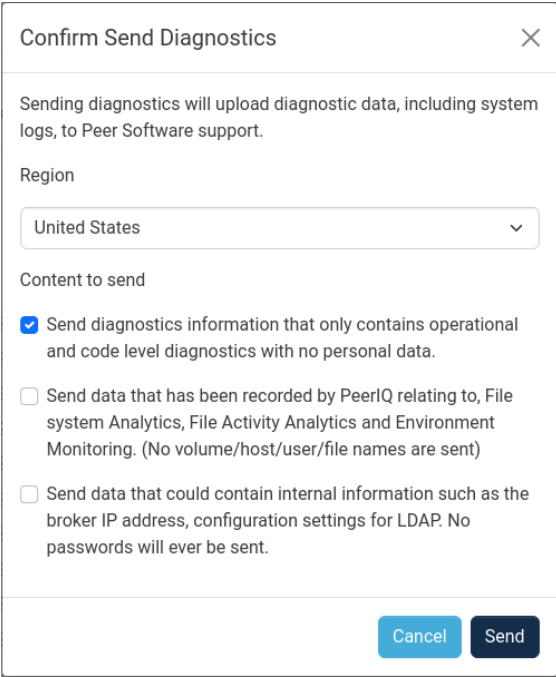
11.4.2 Sending Diagnostics

You can send a diagnostics file to Peer Software support. A connection to the internet is required for a successful upload.

To send the diagnostics file:

1. Open the **Logs** page.
2. In the **Send Diagnostics** card, click the **Send** button.

The **Confirm Send Diagnostics** dialog opens.



The dialog box titled "Confirm Send Diagnostics" contains the following elements:

- A close button (X) in the top right corner.
- A message: "Sending diagnostics will upload diagnostic data, including system logs, to Peer Software support."
- A "Region" section with a dropdown menu currently showing "United States".
- A "Content to send" section with three radio button options:
 - ☒ Send diagnostics information that only contains operational and code level diagnostics with no personal data.
 - ☐ Send data that has been recorded by PeerIQ relating to, File system Analytics, File Activity Analytics and Environment Monitoring. (No volume/host/user/file names are sent)
 - ☐ Send data that could contain internal information such as the broker IP address, configuration settings for LDAP. No passwords will ever be sent.
- At the bottom right, there are two buttons: "Cancel" and "Send".

3. Select the region closest to the PeerIQ appliance for faster uploads.
4. In the **Content to send** section, select the levels of diagnostic data to send Peer Software Support:
 - Operation and code level diagnostics (if using the Ubuntu-based PeerIQ virtual appliance, this will also include system logs)
 - File System Analytics and Environment Monitoring
 - Configuration settings information

Note: No passwords will be included in the diagnostic logs sent to Peer Software Support.

Upon completion, a success message is displayed, and the diagnostics file is stored in the selected region.

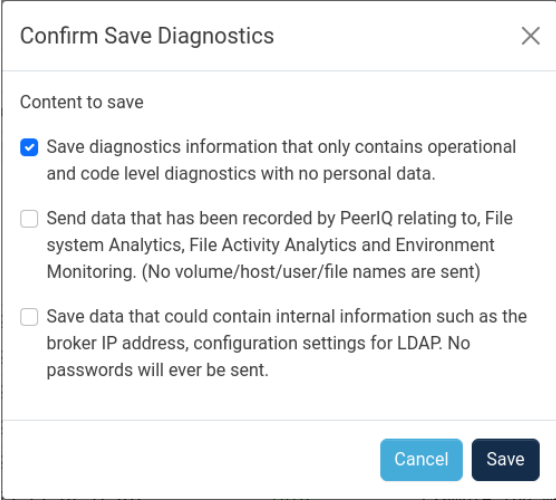
11.4.3 Saving Diagnostics

You can save a diagnostics file for your own records or to send it to Peer Software Support if PeerIQ is unable to establish an internet connection.

To save the diagnostics file:

1. Open the **Logs** page.
2. In the **Save Diagnostics** card, click **Save**.

The **Confirm Save Diagnostics** dialog opens.

A dialog box titled "Confirm Save Diagnostics" with a close button (X) in the top right corner. The dialog contains a section titled "Content to save" with three radio button options. The first option is selected and is labeled "Save diagnostics information that only contains operational and code level diagnostics with no personal data." The second option is labeled "Send data that has been recorded by PeerIQ relating to, File system Analytics, File Activity Analytics and Environment Monitoring. (No volume/host/user/file names are sent)". The third option is labeled "Save data that could contain internal information such as the broker IP address, configuration settings for LDAP. No passwords will ever be sent." At the bottom right of the dialog are two buttons: "Cancel" and "Save".

Confirm Save Diagnostics

Content to save

☒ Save diagnostics information that only contains operational and code level diagnostics with no personal data.

☐ Send data that has been recorded by PeerIQ relating to, File system Analytics, File Activity Analytics and Environment Monitoring. (No volume/host/user/file names are sent)

☐ Save data that could contain internal information such as the broker IP address, configuration settings for LDAP. No passwords will ever be sent.

Cancel Save

3. In the **Content to save** section, select the levels of diagnostic data to save:
 - Operation and code level diagnostics (if using the Ubuntu-based PeerIQ virtual appliance, this will also include system logs)
 - File System Analytics and Environment Monitoring
 - Configuration settings information
4. Click **Save**.

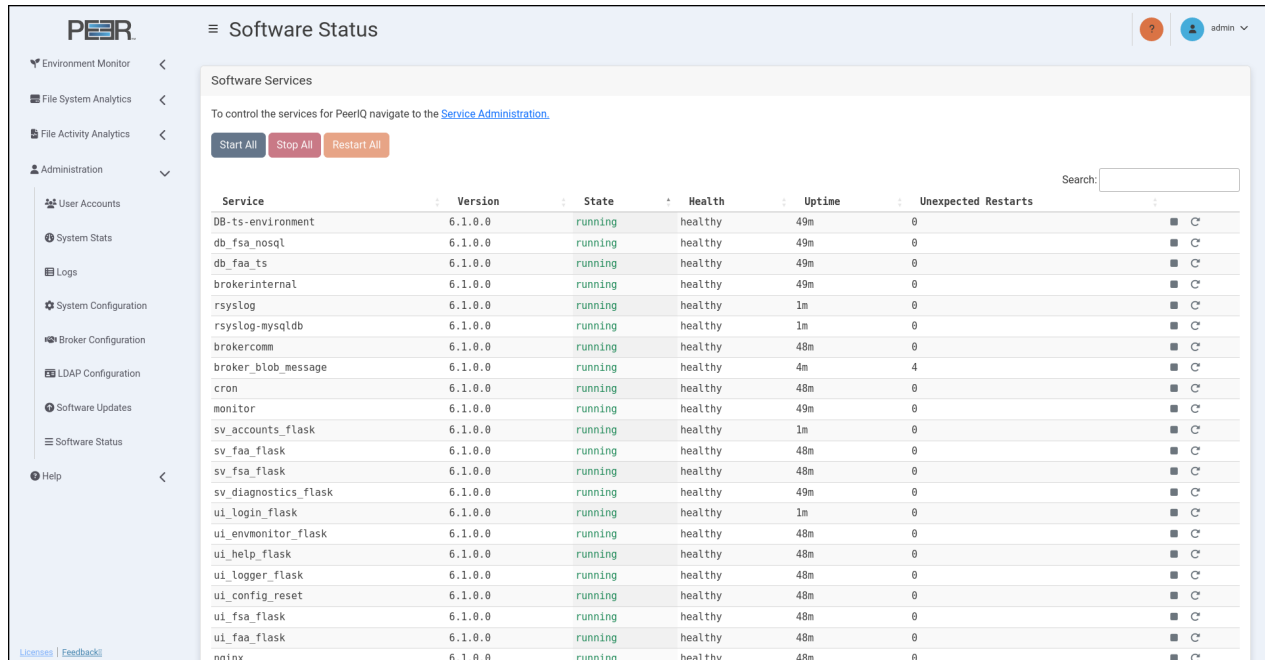
Note: No passwords will be included in the downloaded diagnostic logs.

Upon completion, a success message is displayed. The file will be in a compressed tar.gz format; uncompress it to access the logs in CSV format. Depending on the level of content saved, other diagnostic files in JSON format will be in folders named after their corresponding PeerIQ component.

11.5 Software Status Page

The **Software Status** page provides information about PeerIQ containers, and controls for starting, stopping and restarting PeerIQ containers.

The page must be accessed from the **Service Administration** for the container controls to be activated.



Software Services

To control the services for PeerIQ navigate to the [Service Administration](#).

[Start All](#) [Stop All](#) [Restart All](#)

Service	Version	State	Health	Uptime	Unexpected Restarts
DB-ts-environment	6.1.0.0	running	healthy	49m	0
db_fsa_nosql	6.1.0.0	running	healthy	49m	0
db_faa_ts	6.1.0.0	running	healthy	49m	0
brokerinternal	6.1.0.0	running	healthy	49m	0
rsyslog	6.1.0.0	running	healthy	1m	0
rsyslog-mysqldb	6.1.0.0	running	healthy	1m	0
brokercomm	6.1.0.0	running	healthy	48m	0
broker_blob_message	6.1.0.0	running	healthy	4m	4
cron	6.1.0.0	running	healthy	48m	0
monitor	6.1.0.0	running	healthy	49m	0
sv_accounts_flask	6.1.0.0	running	healthy	1m	0
sv_faa_flask	6.1.0.0	running	healthy	48m	0
sv_fsa_flask	6.1.0.0	running	healthy	48m	0
sv_diagnostics_flask	6.1.0.0	running	healthy	49m	0
ui_login_flask	6.1.0.0	running	healthy	1m	0
ui_envmonitor_flask	6.1.0.0	running	healthy	48m	0
ui_help_flask	6.1.0.0	running	healthy	48m	0
ui_logger_flask	6.1.0.0	running	healthy	48m	0
ui_config_reset	6.1.0.0	running	healthy	48m	0
ui_fsa_flask	6.1.0.0	running	healthy	48m	0
ui_faa_flask	6.1.0.0	running	healthy	48m	0
nginx	6.1.0.0	running	healthy	48m	0

Card	Description
Software Services	Provides controls for stopping, starting, and restarting all services. Each service represents a container. The table displays a list of all running services, along with their individual version, state, health, uptime, and the total number of unexpected restarts. Controls are provided to start, stop, and restart individual services.

11.6 Software Updates Page

The **Software Updates** page provides options and information for upgrading to new PeerIQ versions, including release notes and compatibility details.

PeerIQ Updates

Current Version **6.0.0.1** ([details](#))

Select Major Version: **6.0**

Available Minor Versions and Patches:

PeerIQ Version	Upgradeable from	Compatible PMC Versions
<input checked="" type="radio"/> 6.0.0.47	5.2	5.2.0.20220814 6.0.0.20240524
<input type="radio"/> 6.0.0.37	5.2	5.2.0.20220814 6.0.0.20240524
<input type="radio"/> 6.0.0.36	5.2	5.2.0.20220814 6.0.0.20240524
<input type="radio"/> 6.0.0.35	5.2	5.2.0.20220814 6.0.0.20240524
<input type="radio"/> 6.0.0.34	5.2	5.2.0.20220814 6.0.0.20240524
<input type="radio"/> 6.0.0.20	5.2	5.2.0.20220814 6.0.0.20240524

[Update](#)

Release Notes:

—Release 6.0.0.47.

- Added a new Data Aging page under File System Analytics to get an understanding of the age of data.
- Added a new Hot Data Analysis page under File System Analytics to get an understanding of hot data.
- Added a new Scans page under File System Analytics to see which scans have run against which file servers.
- Added the ability to use previous license key data to help with usage predictions.
- Added the ability to set the time zone of the displayed data.
- Added links from the Environment Overview page to affected jobs or agents.
- Added a current health card to the Environment Overview page.
- Fixed data sorting order in tables.
- Fixed Agent selection when changing graph tabs.
- Fix to scans where 0 byte files are accessed or modified and do not change in size.

11.6.1 Software Updates Page Cards

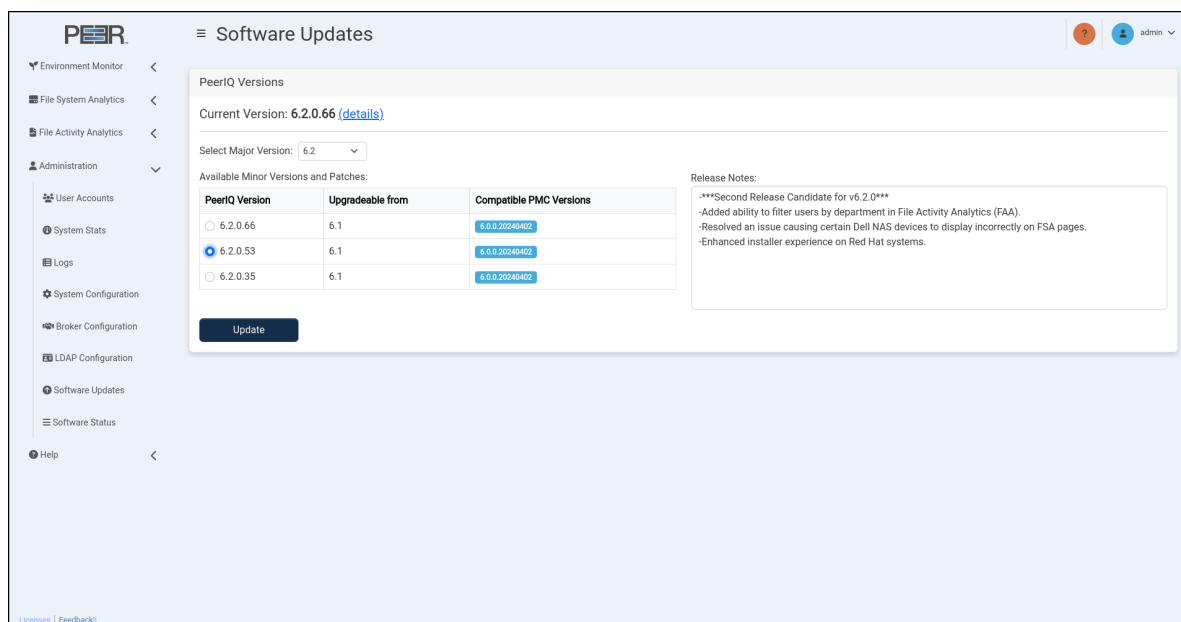
The **Software Updates** page contains one card:

Card	Description
Software Updates	<p>Displays information about available PeerIQ upgrades.</p> <ul style="list-style-type: none"> • Current Version: Shows the PeerIQ version currently in use. Click the details hyperlink to access the Peer Software website for additional information about your current version. • Select Major Version: Use the dropdown box to choose the major PeerIQ version you want to upgrade to. • Release Notes: Lists release notes for the selected minor version or patch. • Available Minor Versions and Patches: Displays the following information: <ul style="list-style-type: none"> – PeerIQ Version: You can select the desired PeerIQ version for the update by clicking the radio button next to the version name. – Upgradable From: Indicates the lowest PeerIQ version that can be upgraded to this version. – Compatible PMC Versions: Lists PMC versions compatible with this PeerIQ version.

11.6.2 Updating PeerIQ

To update PeerIQ, follow these steps:

1. Choose the PeerIQ version to update to.

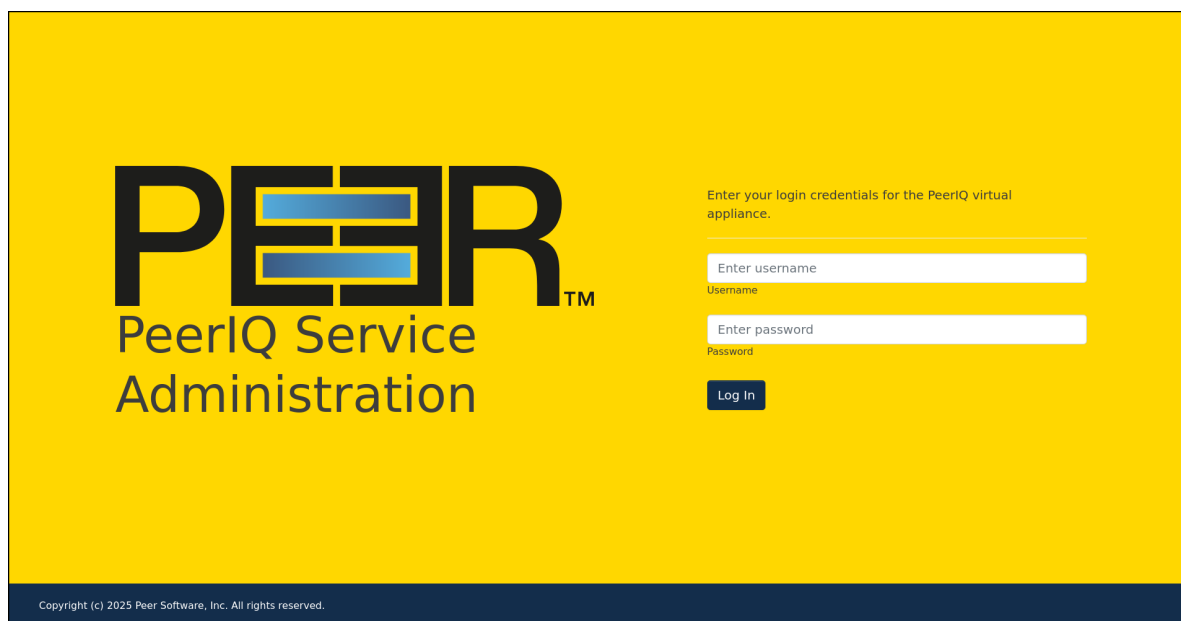


2. Click the **Update Button** to start the update process.

A dialog prompting you to confirm the update will appear.

3. Click **Proceed** to open a new login screen for the software.

The PeerIQ Service Administration login page has a yellow background and a different title from the standard PeerIQ web console. It can be accessed directly via `https://<peeriqIP>:4443`.

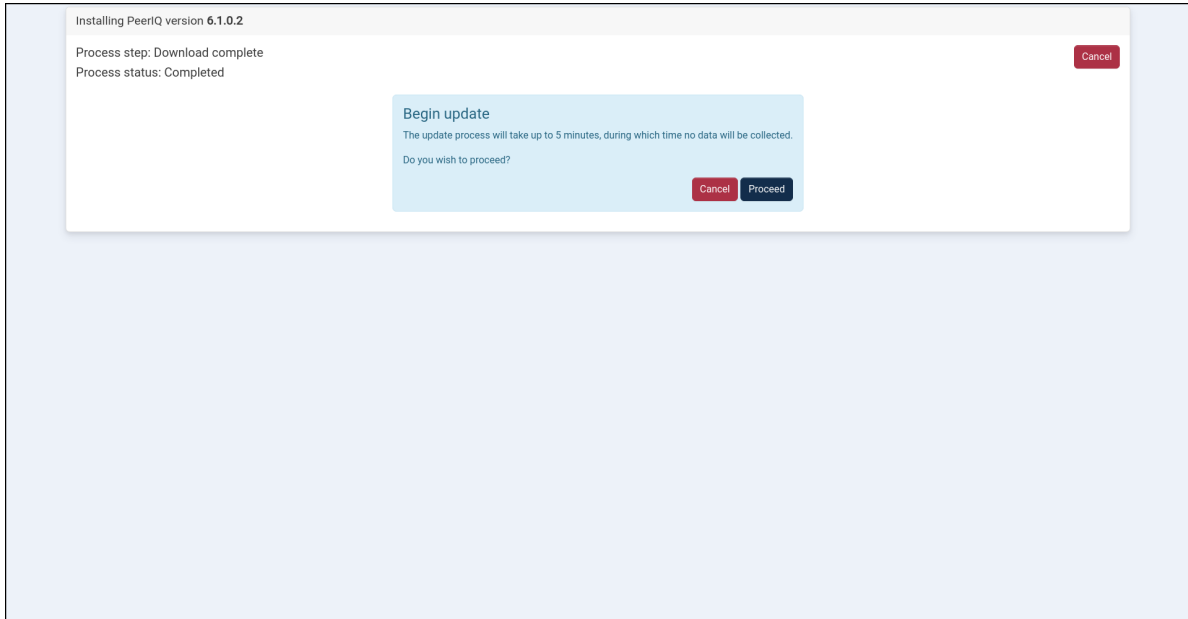


4. Log in to the PeerIQ Service Administration portal. The download for the selected PeerIQ version will begin automatically.

Note: The credentials required for accessing PeerIQ Service Administration differ from those used for the PeerIQ web console. For Virtual Appliances, use the same credentials that are used to log in via the virtual appliance console or through SSH. The default credentials are:

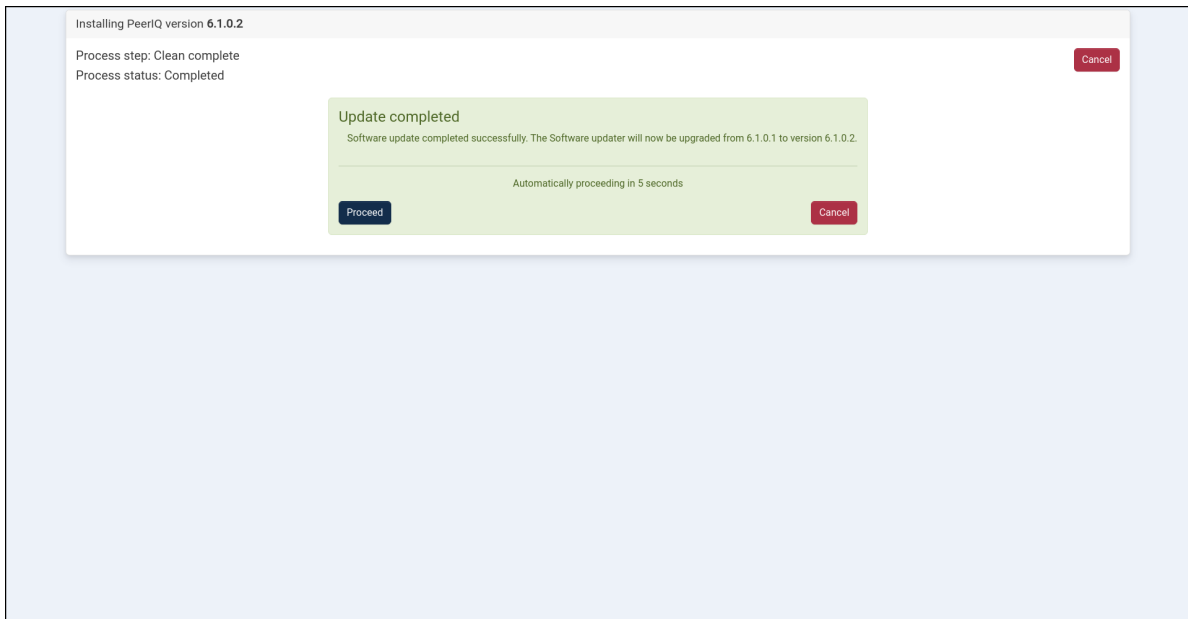
Username: peersoftware, Password: password. These defaults are typically updated during the initial deployment of the virtual appliance. For Red Hat installs, you may use the same credentials that were used during the installation of PeerIQ, or any user account that has sudo privileges.

5. Confirm the update by clicking **Yes** once the download completes.



PeerIQ will be updated to the selected version.

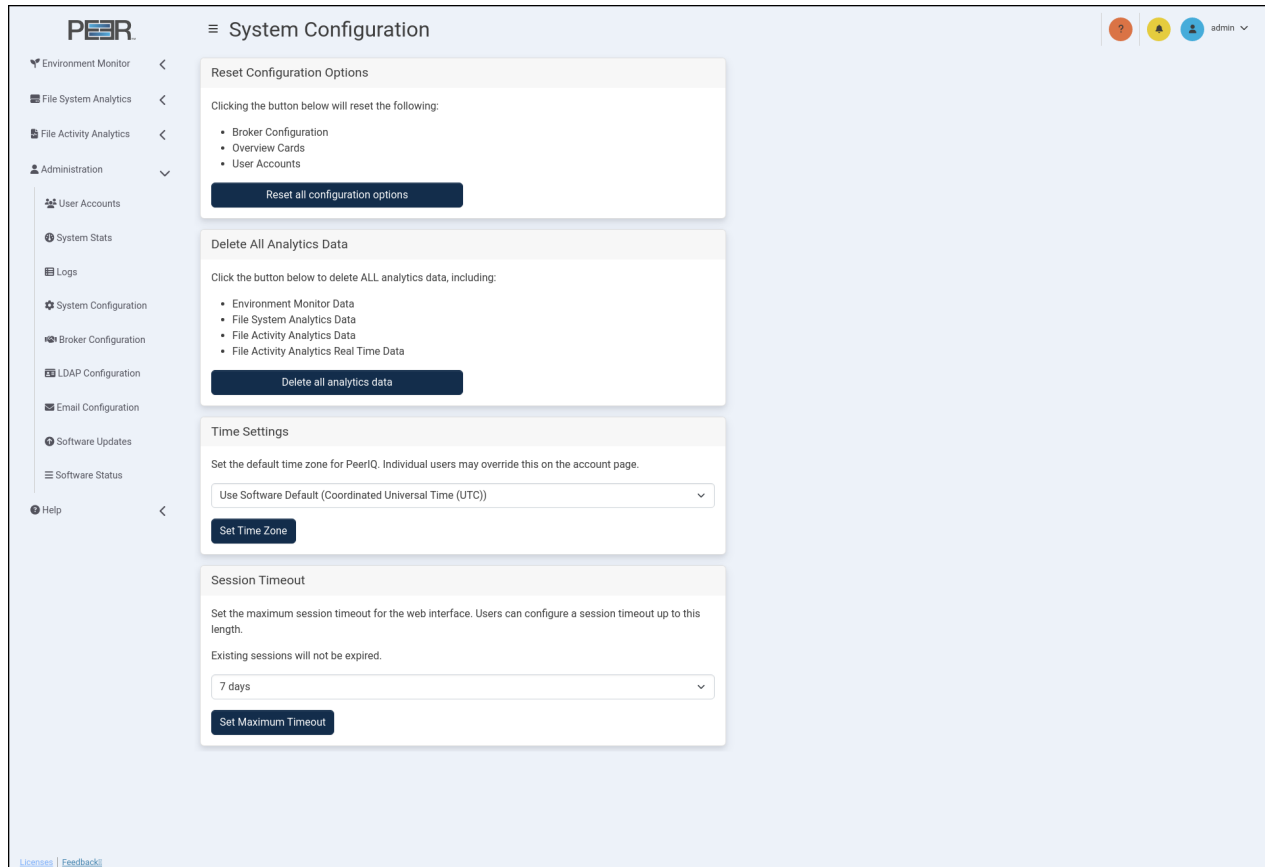
6. After updating PeerIQ, a notice to update the service container will appear. If no action is taken within five seconds, the service container update is automatically performed. Clicking **Cancel** during that five second window will skip the service container update.



After installation, the PeerIQ login page is redisplayed.

11.7 System Configuration Page

The **System Configuration** page allows an Administrator to perform a complete reset, which includes erasing configuration parameters such as usernames and passwords, as well as clearing any data that has been collected from the PMC. Once the data has been erased, it cannot be recovered.



The System Configuration page has four cards:

11.7.1 Resetting Configuration Options

This **Reset Configuration Options** card enables you to revert all parameters to the default settings, as initially configured when the product was first deployed. This includes:

- **Broker configuration:** The existing broker connection will be stopped.
- **Overview cards:** All customizations made to Warning and Danger thresholds will be restored to the default values.
- **User accounts:** All LDAP configurations will be deleted, including all user accounts and their associated settings (such as time zone). This will restore the default credentials:

- **Username:** admin
- **Password:** password

After resetting the configuration options, you will be logged out of the PeerIQ system.

11.7.2 Delete All Analytics Data

Clicking **Delete All Analytics Data** permanently removes all data collected by the PeerIQ system.

Note: This action is irreversible. Once deleted, the data cannot be recovered.

11.7.3 Managing Time Zone Settings

The **Time Settings** card enables you to set the default time zone that is used by all users on all pages within the PeerIQ user interface. You can set the time zone using the drop-down menu options to display page elements in either Coordinated Universal Time (UTC) or the time zone of each web browser accessing the pages. While this global setting is the default for all users of the system, each user can set their own time settings after logging in to PeerIQ.

Note: Downloaded logs and reports will always be in UTC format.

11.7.4 Session Timeout

The **Session Timeout** setting defines how long a user session remains active in the PeerIQ web interface before automatic expiration. Administrators can select the maximum allowed duration from the drop-down menu.

Setting a timeout ensures inactive sessions do not remain open indefinitely, improving overall security for the web interface.

11.7.5 Configuration

From the drop-down list, choose one of the available timeout options:

- **7 days**
- **1 day**
- **6 hours**

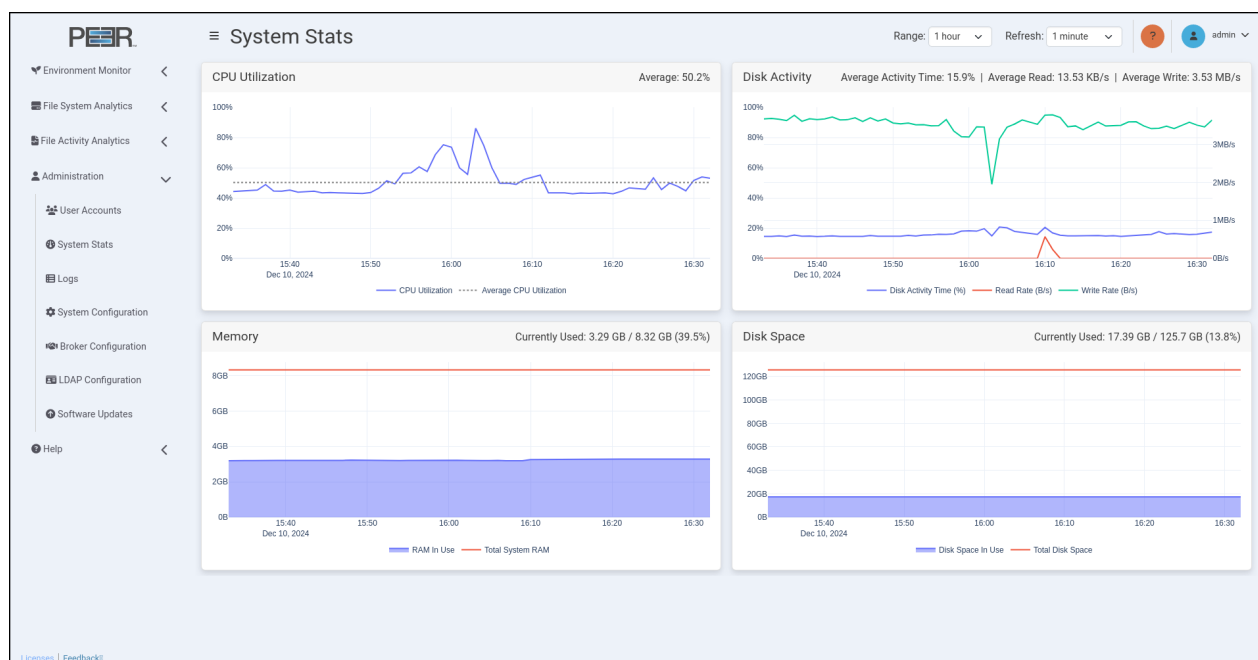
- 1 hour
- 30 minutes
- 10 minutes

Once a value is selected, click **Set Maximum Timeout** to apply the change.

Note: Updating the timeout affects only new sessions. Existing sessions will remain active until they naturally expire or the user signs out.

11.8 System Stats Page

The **System Stats** page provides an overview of the virtual appliance where PeerIQ is deployed. It enables you to analyze overall performance and monitor the appliance's health. Use this page to identify potential performance issues affecting PeerIQ and gain insights into how the appliance is operating. This page is accessible to Administrators only.



11.8.1 Using the System Stats Page Controls

This page features line graphs that depict activity trends over time. Use the controls located in the upper right corner of the page to adjust the date range and refresh rate of the displayed information:

- **Range:** Use this to select the desired time range for the line graphs; options range from 1 hour to 4 weeks.

- **Refresh:** Use this to select the interval at which the line graphs automatically refresh; Options are off (graphs will not refresh) or 1 minute.

11.8.2 System Stats Page Cards

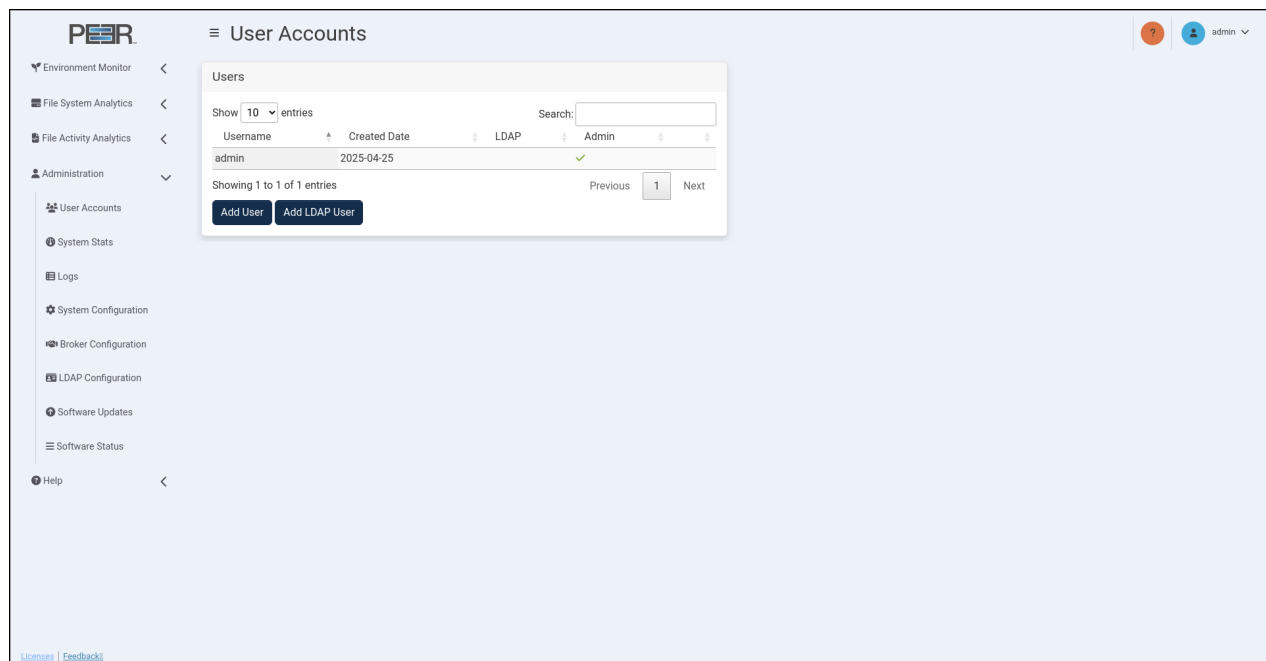
The **System Stats** page contains four cards:

Card	Description
CPU Utilization	<p>Displays a line graph illustrating CPU usage over time, reflecting the selected time range. The graph shows the percentage of CPU used and the average CPU utilization for that period. The average utilization percentage is displayed in the top right of the card.</p> <p>Hover over a data point to view its date and time, as well as the interval it represents, which depends on the range setting. For example, if the range setting is 1 week or longer, the hover box will display "(60 minute average)" below the date and time.</p>
Disk Activity	<p>Displays a line graph showing total disk activity as a percentage over time, reflecting the selected time range. It also shows Bytes per second (B/s) for both disk read and write speeds. The average disk activity time, as a percentage, and the average read and write speeds for the selected time range are shown in the top right of the card.</p> <p>Hover over a data point to view its date and time, as well as the interval it represents, which depends on the range setting. For example, if the range setting is 1 week or longer, the hover box will display "(60 minute average)" below the date and time.</p>
Memory	<p>Displays a line graph representing memory usage over time, with the total amount of memory assigned to the virtual appliance. The graph reflects the selected time range, with current memory usage displayed as both a fraction and a percentage in the top right of the card.</p> <p>The graph displays point measurements rather than averages, regardless of the range option selected.</p> <p>The Currently Used values in the headers reflect the most recent data point in the database, rather than just the most recent point in the plot. For example, if the range is set to 1 week, the last point in the Memory plot will be from the most recent hour (on the hour), but the header will display the memory in use as of the most recent minute.</p>

Card	Description
Disk Space	<p>Displays a line graph depicting disk space usage over time, reflecting the selected time range. It includes the total amount of disk space assigned to the virtual appliance. Current disk space usage is shown as both a fraction and a percentage in the top right of the card.</p> <p>The graph displays point measurements rather than averages, regardless of the range option selected.</p> <p>The Currently Used values in the headers reflect the most recent data point in the database, rather than just the most recent point in the plot. For example, if the range is set to 1 week, the last point in the Memory plot will be from the most recent hour (on the hour), but the header will display the memory in use as of the most recent minute.</p>

11.9 User Accounts Page

You can manage user accounts on the **User Accounts** page.



The User Accounts page contains one card:

Card	Description
Users	Use this card to view and delete all local users and add LDAP users.

11.9.1 Adding and Removing Users

Use the **Users** card on the **User Accounts** page to add, view, and remove users.

Adding a Local User Adding a local user will allow that user to log in to PeerIQ using the specified username and password.

To add a local user:

1. Using your Administrator account, open the **User Accounts** page.
2. Click the **Add User** button in the **Users** card.
3. Fill out the fields in the **Add User** dialog:
 - **Username:** Enter the username for the new user.
 - **Password:** Enter the password for the new user. The user can change this later.
 - **Role:** Assign a role to the user within PeerIQ. Roles define what users can do in terms of configuring PeerIQ as well as viewing data and reports. Administrators have full access to PeerIQ, while non-Administrators have limited access to data and reports, and cannot make configuration changes.

The image shows a modal dialog box titled "Add User" with a close button (X) in the top right corner. Inside the dialog, there are three input fields: "Username", "Password", and "Role". The "Role" field is a dropdown menu with "User" selected. At the bottom right of the dialog, there are two buttons: "Close" (light blue) and "Add User" (dark blue).

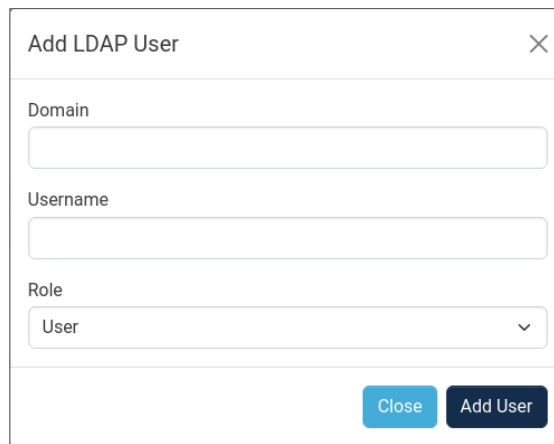
4. Click **Add User**.

Adding an LDAP User Before you can add an LDAP user, you must configure the connection to the LDAP Server. For details, see the section [Configuring Access for LDAP Users](#).

Adding an LDAP user will allow that user to login to PeerIQ using their LDAP login credentials.

To add an LDAP user:

1. Using your Administrator account, open the **User Accounts** page.
2. Click the **Add LDAP User** button in the **Users** card.
3. Fill out the fields in the **Add LDAP User** dialog:
 - **Domain:** Enter the domain to which the user belongs.
 - **Username:** Enter the user's username within the specified domain. Do not include the domain in this field.
 - **Role:** Assign a role to the user within PeerIQ. Roles define what users can do in terms of configuring PeerIQ as well as viewing data and reports. Administrators have full access to PeerIQ, while non-Administrators have limited access to data and reports, and cannot make configuration changes.



The screenshot shows a modal dialog titled "Add LDAP User" with a close button in the top right corner. Inside the dialog, there are three input fields: "Domain", "Username", and "Role". The "Role" field is a dropdown menu with "User" selected. At the bottom right of the dialog, there are two buttons: "Close" and "Add User".

4. Click **Add User**.

The newly added user will log in using their username, followed by the @ symbol, followed by their domain (e.g., johnsmith@london.local).

Removing a User To remove a user from the system, follow this step:

1. Using your Administrator account, open the **User Accounts** page.
2. Click the red trash icon at the end of row of the user you want to delete.

Note: The default user cannot be deleted.