notifi

Are You In Control of Your Application Environments?

PERFORMANCE MONITORING SOFTWARE FOR YOUR APPLICATIONS

VERSION 1.2

Kreativ LLC

Contents

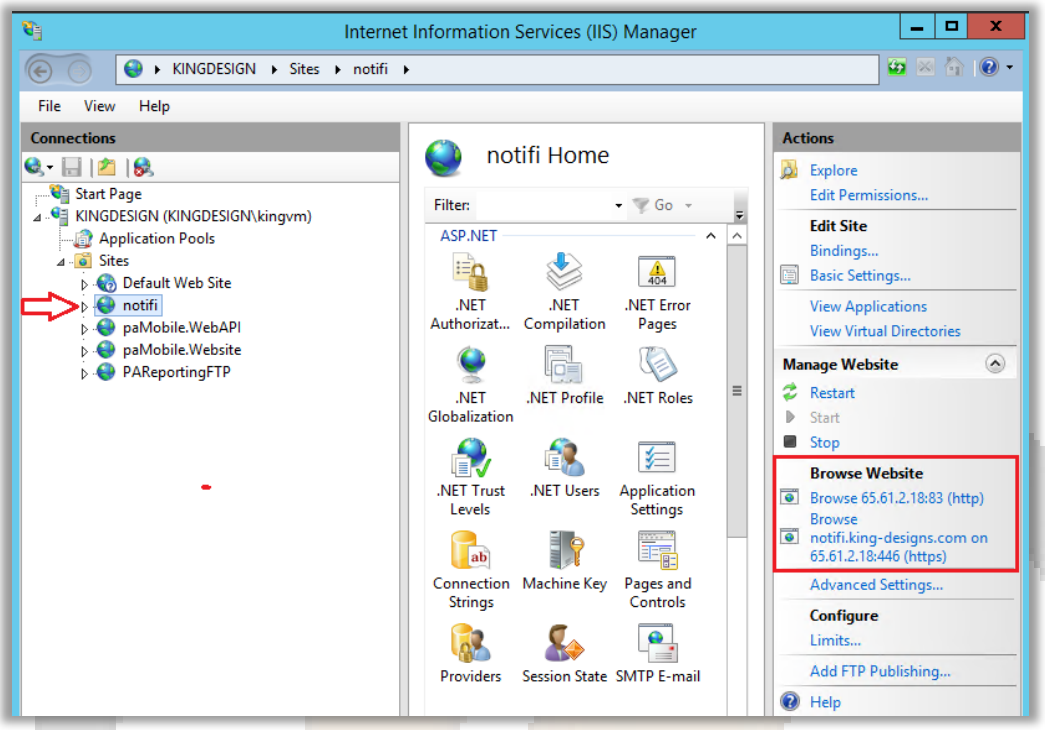
Summary

notifi© is an application monitoring software that advances support resources from reactive to proactive. Stop waiting for users to call you when a problem occurs and get ahead. notifi© monitors text based log files and SQL tables and quickly and efficiently identifies issues. Notification/Alert rules are used to allow generic or detailed definitions that identify issues and provide information to team resources to simplify their application support.

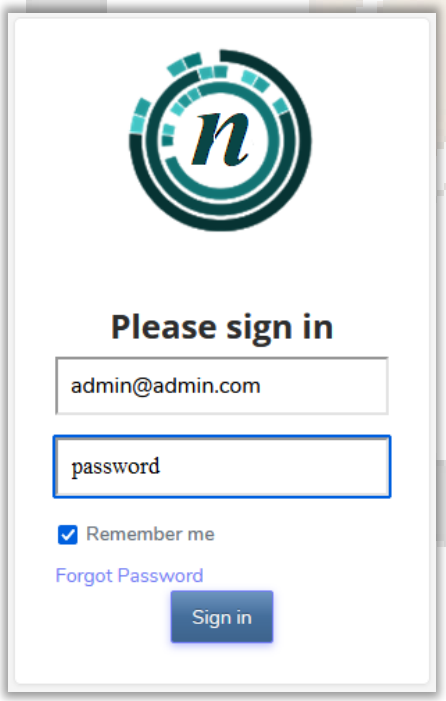
notifi© provides a SQL metric/KPI monitoring interface that will send SMS and/or email notifications/alerts to support personnel using individual resource information or user groups. Rules can be used to capture and catalog issues or have one or more alerts to almost unlimited monitoring and management.

After Installation

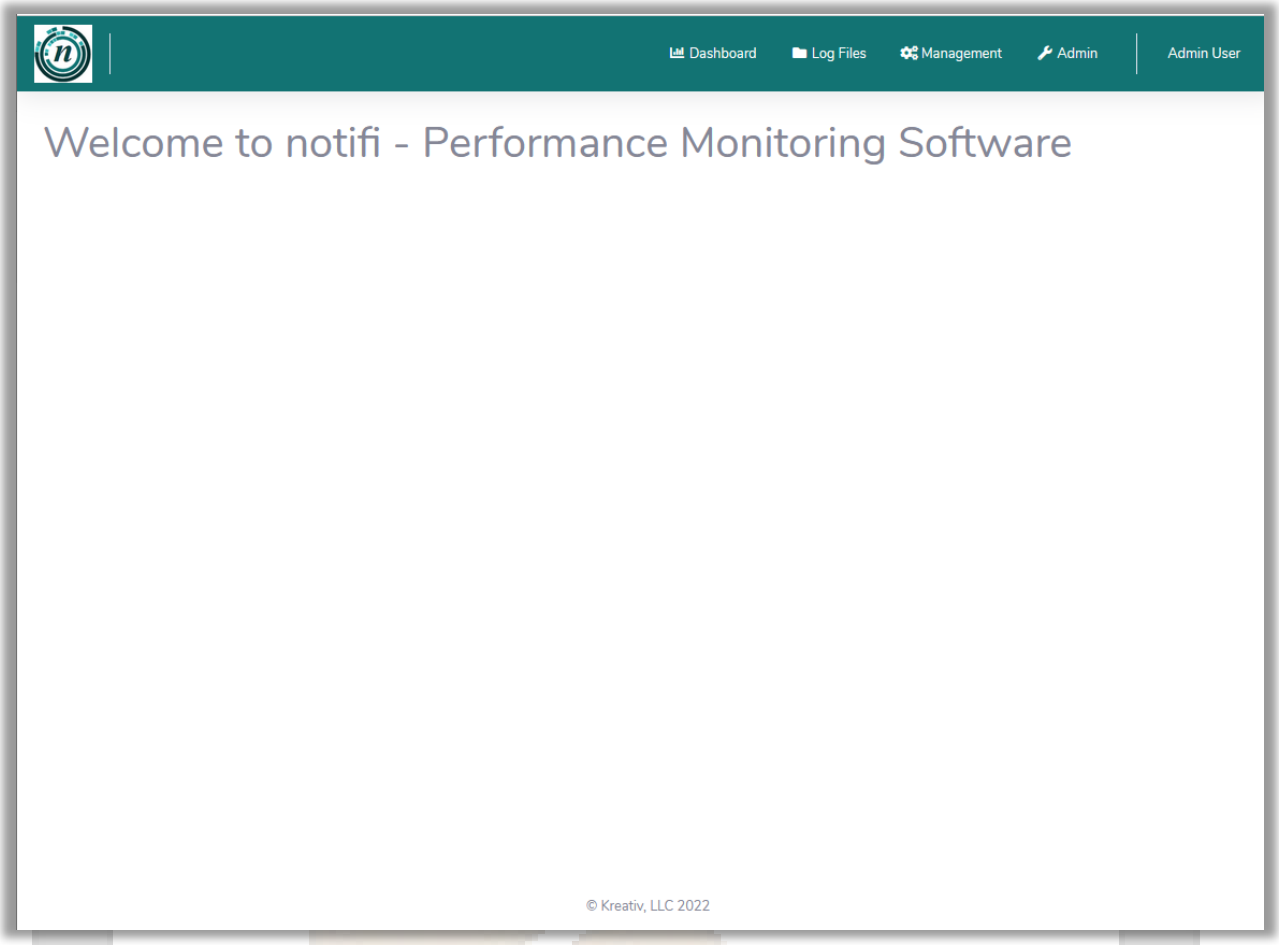
After successfully installing notifi access the web interface by using the URL Error! Hyperlink reference not valid., where <servername> is the name or IP address of the install server and <port> is the port defined for the site. If using Internet Information Services (IIS) to host the website, you can find the URL by selecting the notifi Site in the Internet Information Services (IIS) Manager and looking in the Browse Website section in the Actions bar.



Once you have successfully entered the URL, notifi opens to the Login Page. The default login after installation is Login: admin@admin.com and Password: password.

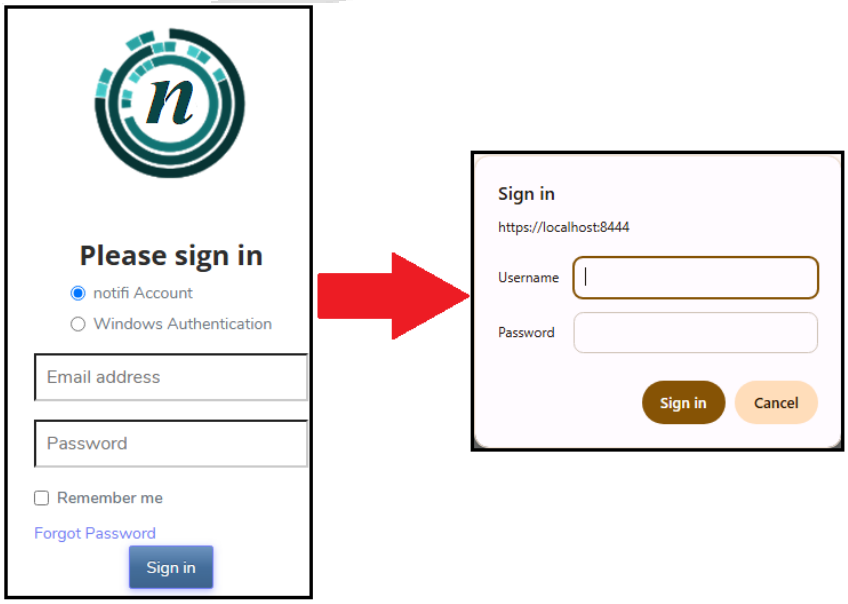


After logging in the home page is displayed.


Dashboard
Log Files
Management
Admin
Admin User
Welcome to notifi - Performance Monitoring Software
© Kreativ, LLC 2022

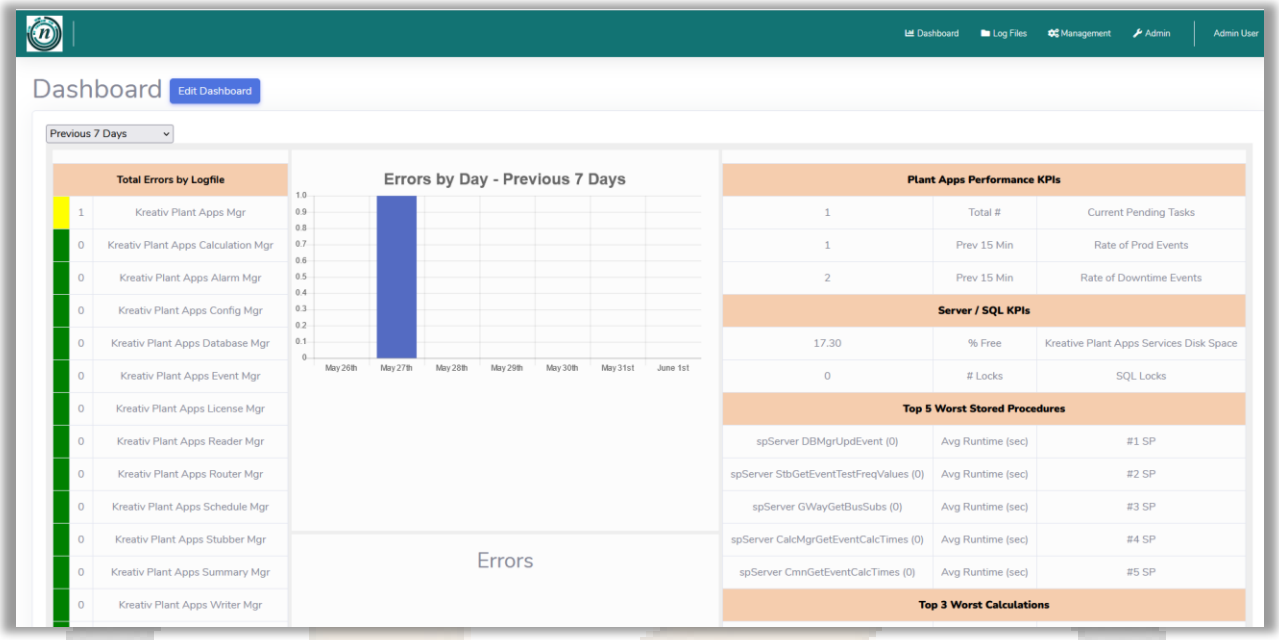
I. New in Version 1.2: Windows Authentication (if configured) now requires the user to actually enter their Windows credentials when signing in - previously it would silently sign the user in without prompting.

Update: Windows-authenticated Users can now optionally skip that credential prompt on their own computer - see Automatically log in with Windows credentials under Users below. This is off by default and must be turned on per User by an Administrator; it does not change the sign-in behavior for any User it isn't explicitly enabled for.

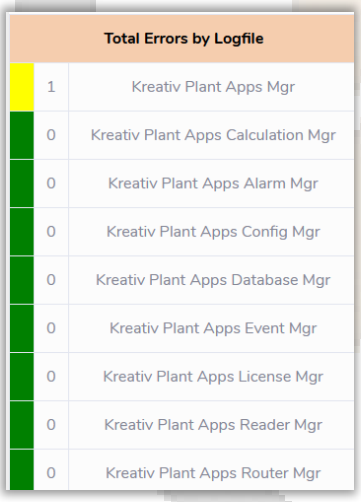


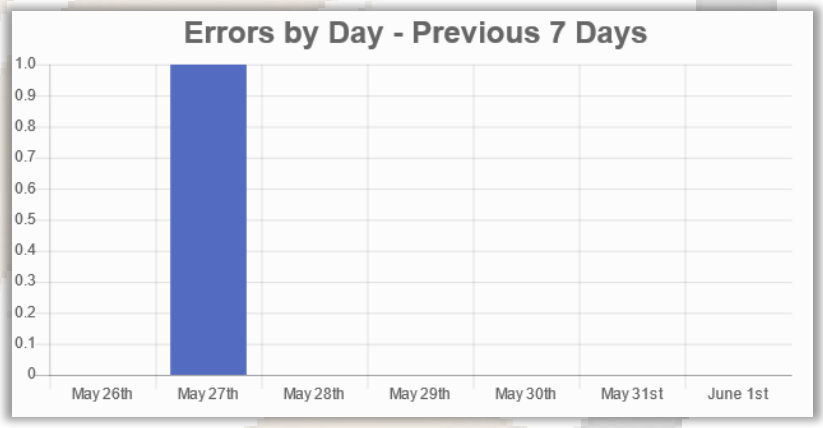
Dashboard

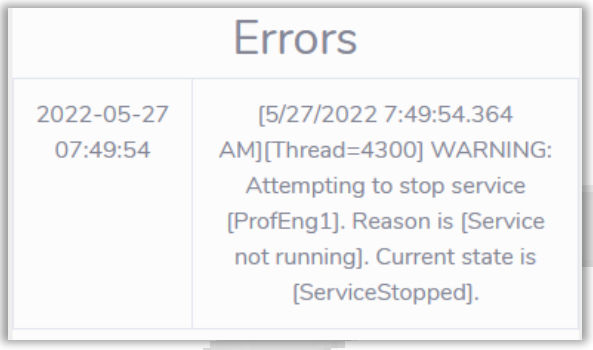
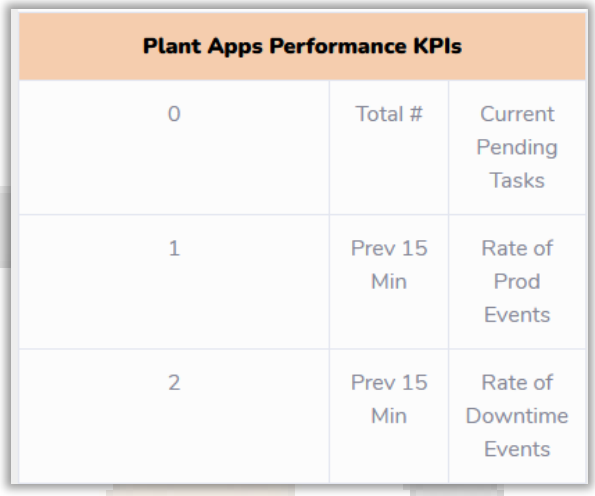
The notifi Dashboard provides a quick current status look into your applications. Color coding, green, yellow and red indicate status of log file errors.



Total Errors By Logfile	Errors by Day





Errors	SQL Scripts
	

Total Errors By Logfile – each configured logfile is displayed with the total number of errors logged for the selected timeframe. The logfiles are sorted by total errors descending and color coded.

0 errors = green; 1 – 10 errors = yellow; > 10 errors = red.

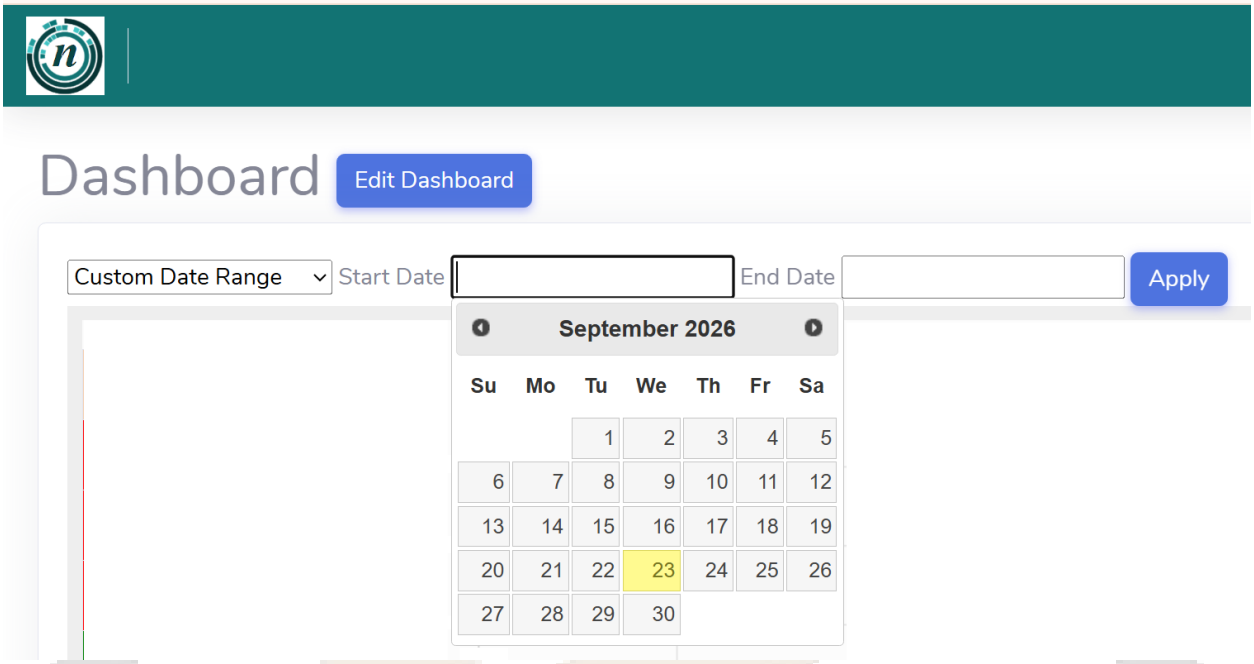
Previous 24 Hours – Shows the number of errors by hour for the Previous 24 Hours.

Previous 7 Days – Shows the number of errors by day for the Previous 7 Days.

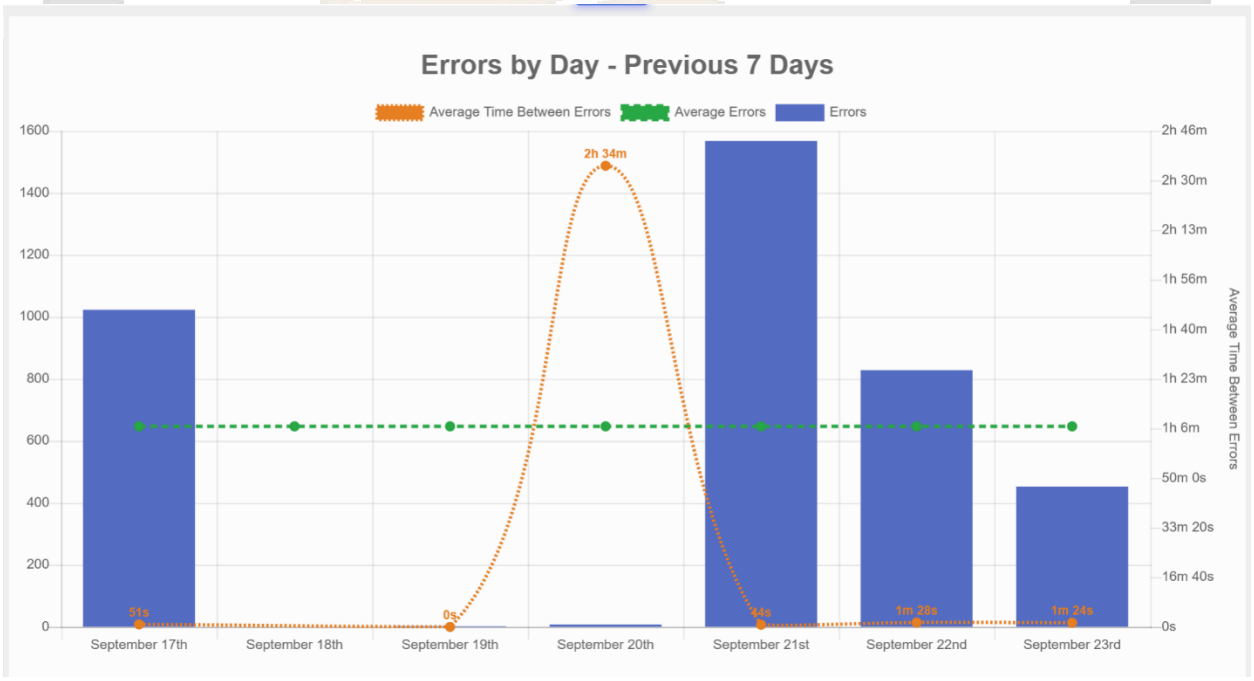
Previous Month (Days) – Shows the number of errors by day for the Previous Month.

Previous 12 Months – Shows the number of errors by month for the Previous 12 Months.

Custom Date Range - Lets you pick any start and end date instead of using one of the presets above.



New in Version 1.2: the chart also plots two reference lines - Average Errors (a flat green line showing the average number of errors per bar) and Average Time Between Errors (an orange line, on its own scale on the right, showing how far apart errors were within each bar).



New in Version 1.2: the Dashboard's automatic refresh interval (how often it checks for new errors) can be adjusted by an Admin on the Codes settings page. The current notifi version number is shown in the page header.

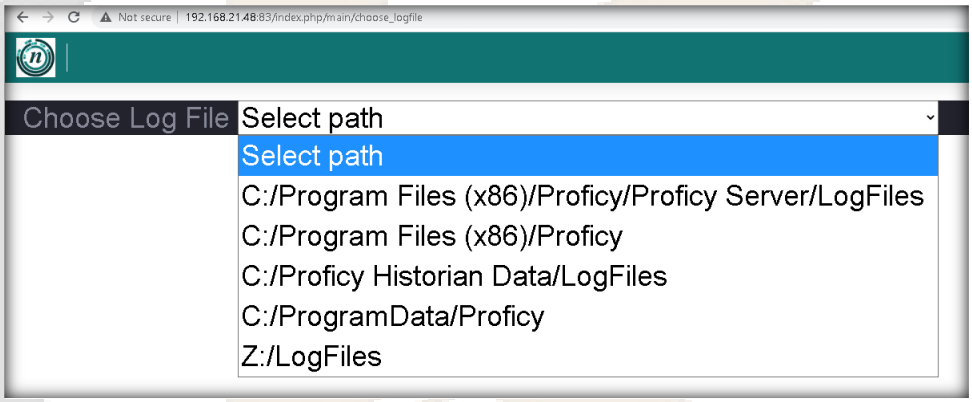
Administering notifi

Log Files

Text based files storing log messages from any source including but not limited to applications and hardware.

Add Log File

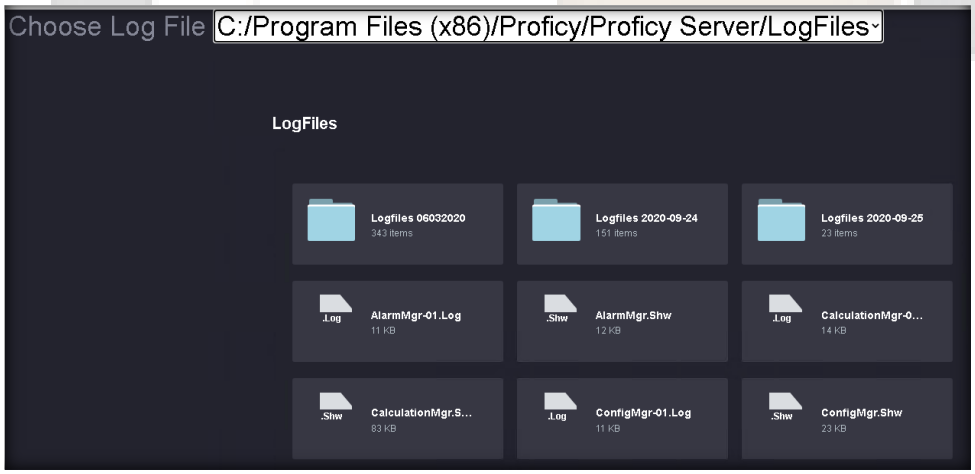
Select Log File Path



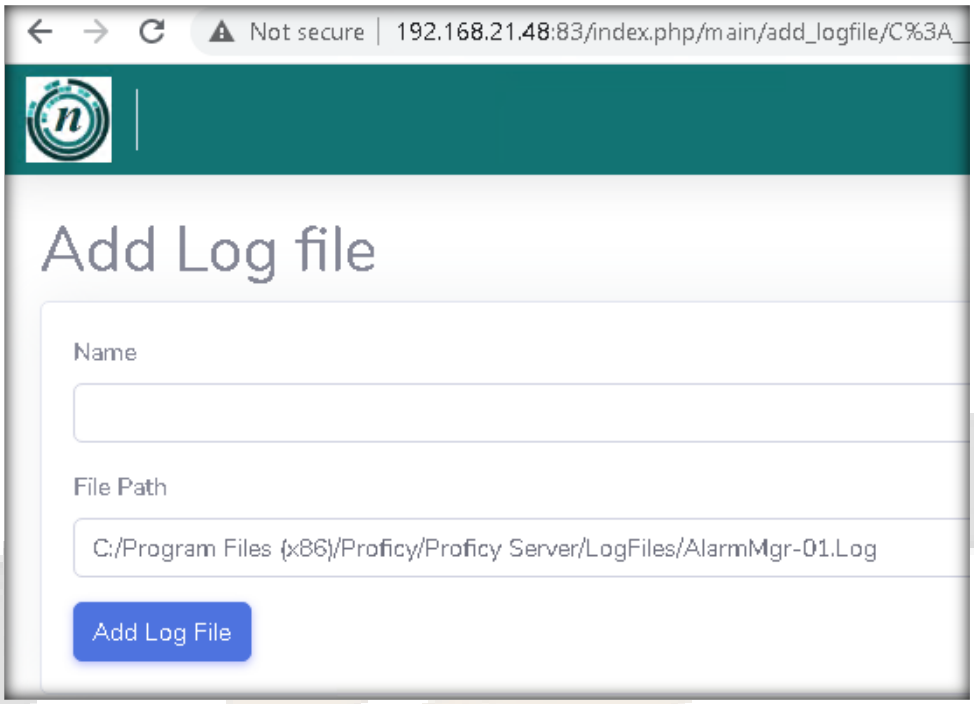
Name

Enter a name that describes the log file.

File Path

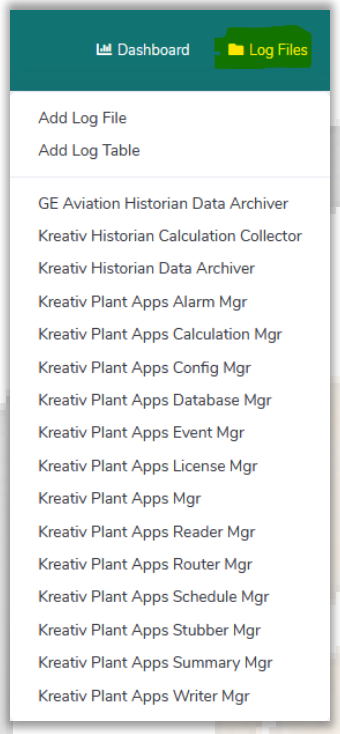


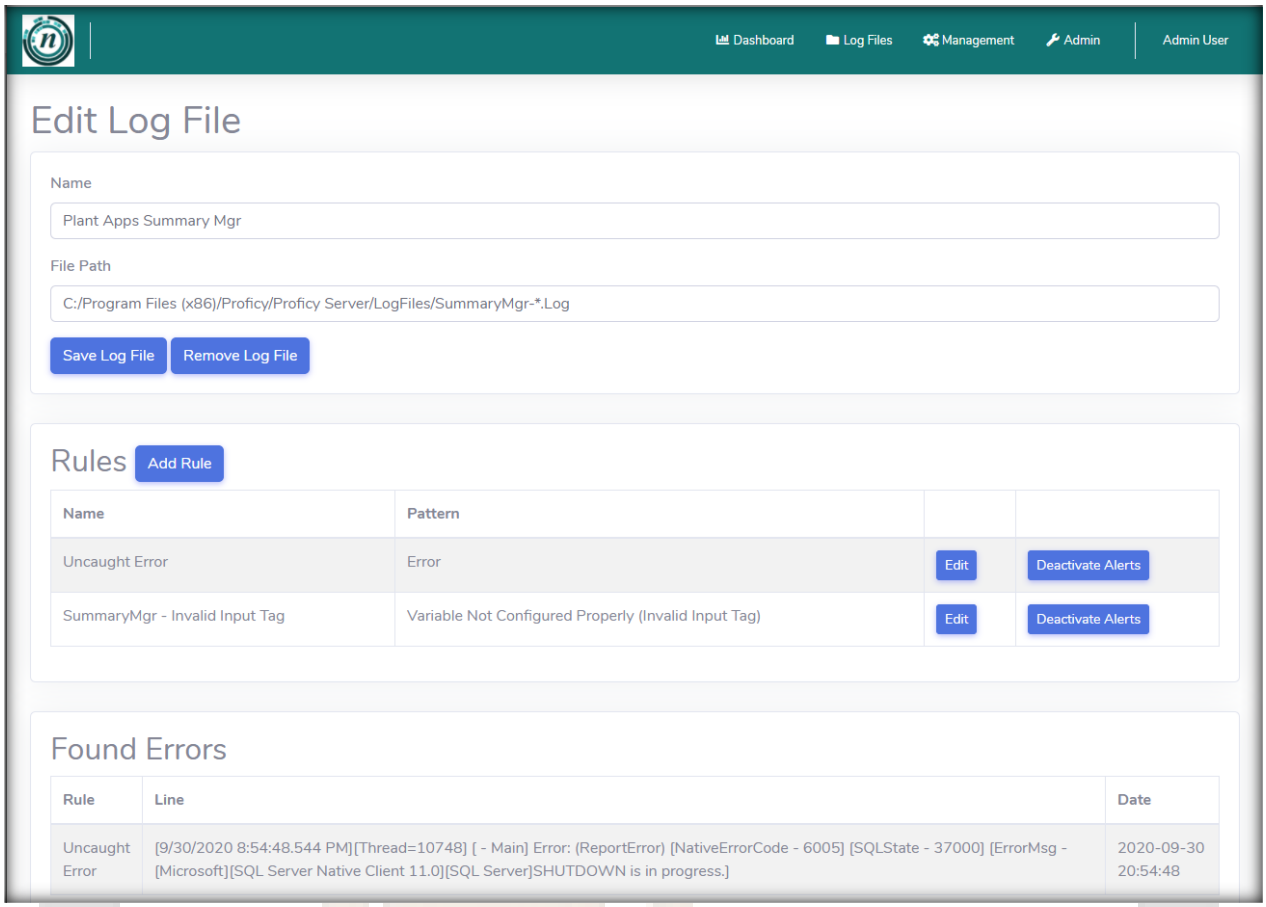
Automatically filled in based on log file selection.



Configured Log Files

Selecting Log Files from the notifi© menu displays the list of configured log files.





Edit Log File page

After selecting a log file, the Edit Log File page is displayed. The Name and File Path are displayed and you are given the option to Save Log File or Remove Log File. Rules can be created for the log file. Rules allow you define specific messages or phrases that notifi© will scan for in the log file.

When the log file is added, a default Rule called Uncaught Error is automatically created. The Uncaught Error rule will capture any message containing the phrase 'error'.

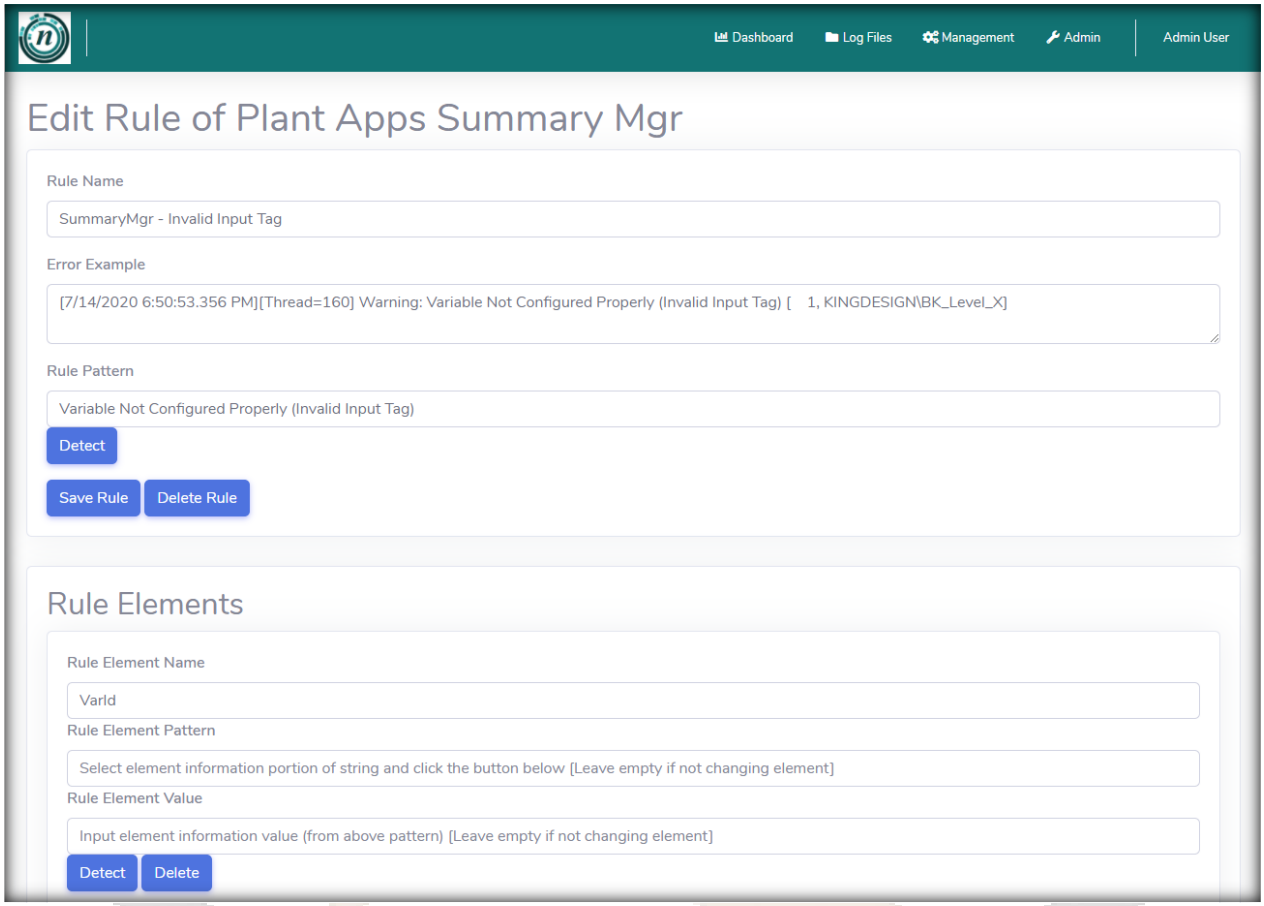
Rules

Rules allow users to configure specific 'patterns' identified in log messages to trigger an incident or issue that needs attention. The rule defines the pattern and rule elements. The pattern is used to search log messages by the notifi© engine to determine if a violation has occurred. If the pattern is matched to text in the log message then the rule is executed and any configured alerts are processed.

Rules can be marked active or inactive. This is useful if there an issue occuring that can not be resolved until a later time such as a down day. Alerts can be deactivated for the rule. This will

allow notifi© to continue to process, parse, the log file messages and capture any rule violations, but not alerts are sent.

Edit Rules



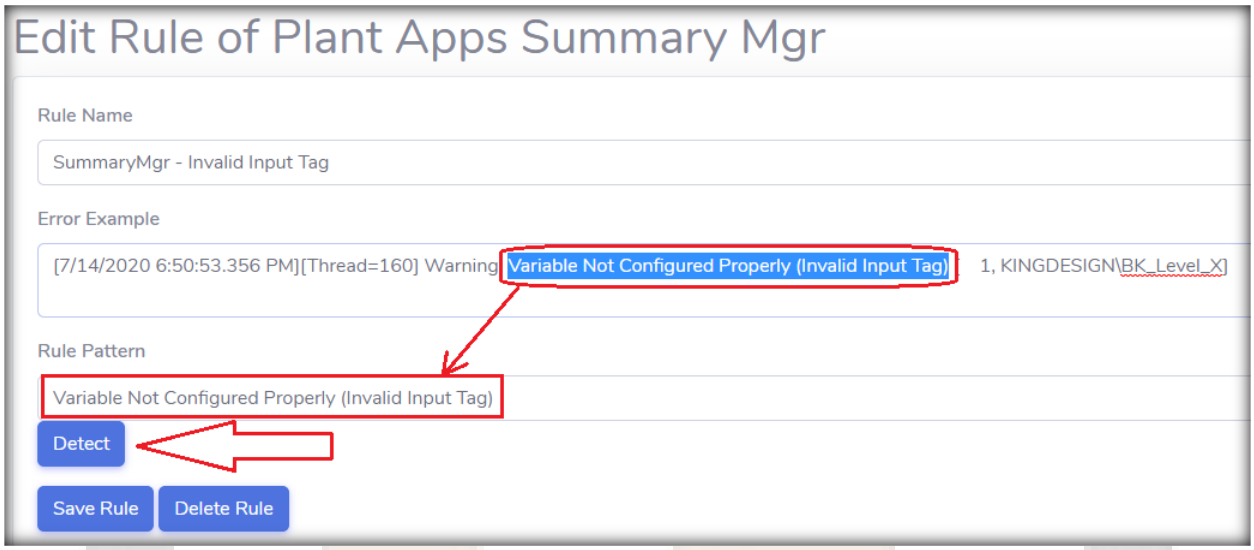
Rule Name

Unique description for Rule. Consider using your server name or some unique identifier as part of the description. This will allow you to quickly determine which server the alert is associated with. Also include a way to easily identify the log file and rule. For example, “Kreativ SummaryMgr – Invalid Input Tag”.

Error Example

Example of the error message that the rule is associated with. The error example can be copied from an actual log file and pasted into the Error Example text box. This can be

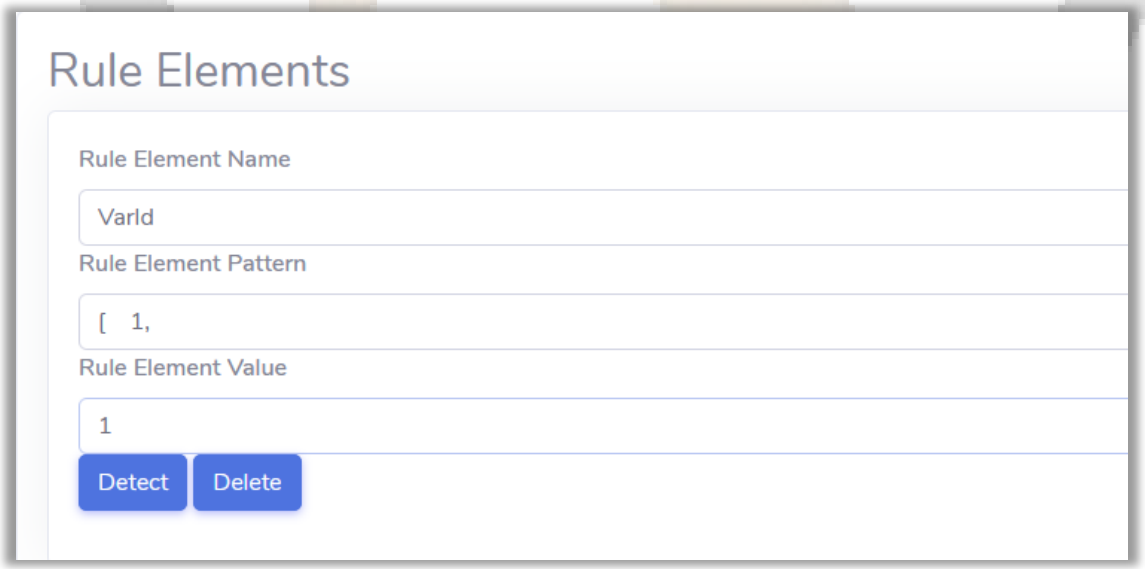
used to highlight the patten, click the Detect button to have notifi© copy the pattern to the Rule pattern text box. Beyond that the Error Example is not used by notifi©.



Rule Pattern

The Rule Pattern is used to compare against the log message to determine if a specific Rule has been violated. Each Rule defined for the log file is processed when a new message is identified in the log file. The messages are processed forward from the date/time and/or row location of the last engine execution to current time. The Rule Pattern should be a unique pattern that will specifically identify the error or issue that is required to be captured.

Rule Elements



Rule Elements allow users to 'scrape' information from the messages that are parsed from the log file. The information then can be used in the alert/notification to build messages and/or in SQL Scripts.

Rule Element Name

Description of element.

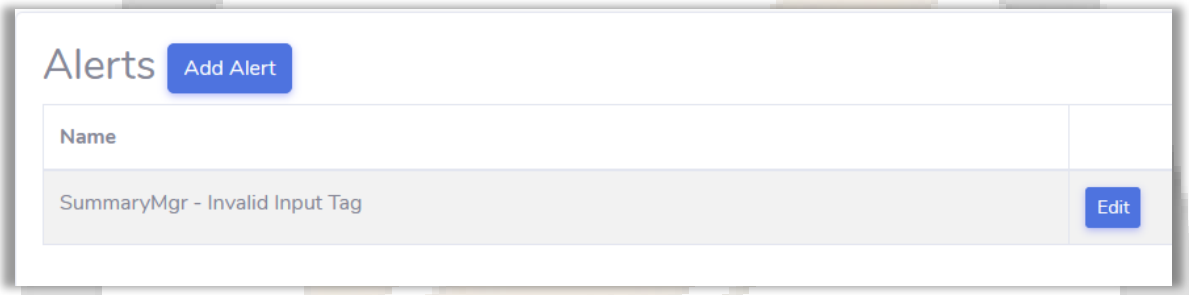
Rule Element Pattern

Pattern or phrase used to 'select' the element value from the log file msg.

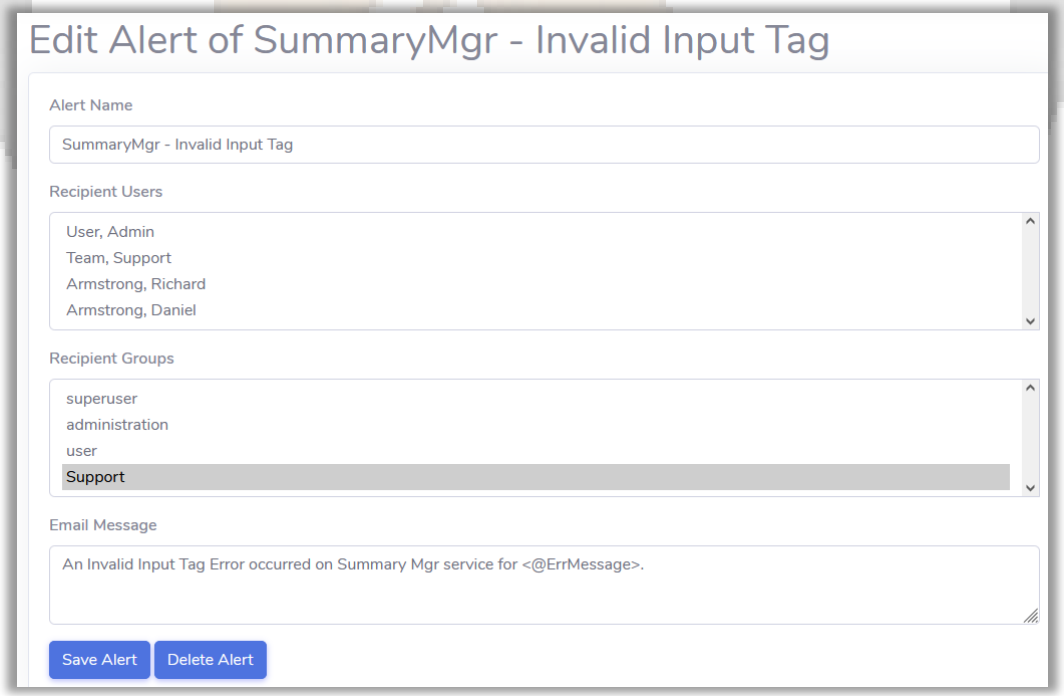
Rule Element Value

Value that is 'scraped' from the log file msg and stored in the element.

Alerts

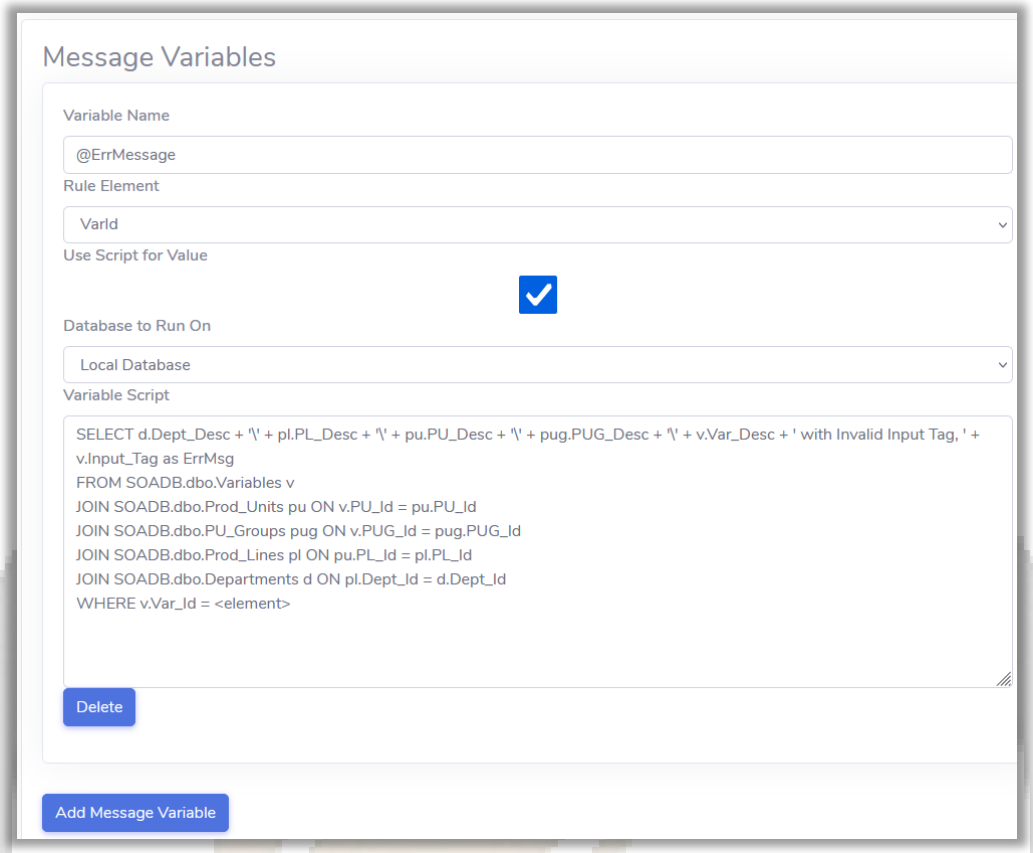


Edit / Create Alerts based on the notifi Rule. Alerts allow you to be notified by email and/or sms text when the rule is violated. The Alert configuration is used to define alert message and select users or groups that will receive the alerts.



Message Variables defined in the Rules configuration can be used in Alert emails.

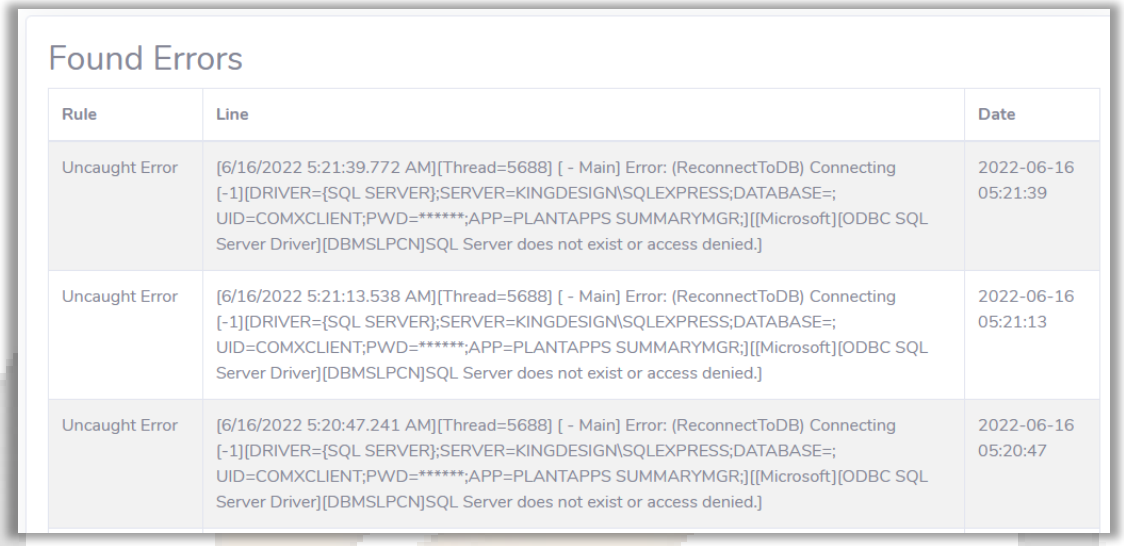
Variable Name	Provide a name for the variable that is descriptive of the value that will be assigned to it. At Kreativ, we typically prefix the description with @ to help indicate that it is a variable, but not required.
Rule Element	The Rule Element that was declared or defined earlier in the Rules configuration. A dropdown of rule elements is provided to chose from.
Use Script for Value	Select by checking the box and use the defined Database and Variable Script to run a SQL script to return a single value that will be stored in the Variable Name. You can access the Element Variable value by including <element> in your script. See below screenshot for an example.
Database to Run On	Select the SQL Database that the script will execute on. SQL Databases are defined and configured by selecting Admin / Databases from the notifi menu. For more information, refer to the Databases section in this document.
Variable Script	Define the SQL script to run against the "Database to Run On". As mentioned earlier you can use the Element Variable in the script by including <element>. The script MUST return a single value.



Additional Message Variables can be defined for use in the alert email message by clicking the Add Message Variable button. The Message Variable(s) is included in the email message by inserting the Message Variable name in the format '<messsage variable name>'.

Found Errors

At the bottom of the Edit Log File page is the Found Errors section which lists errors identified and flagged for this log file.

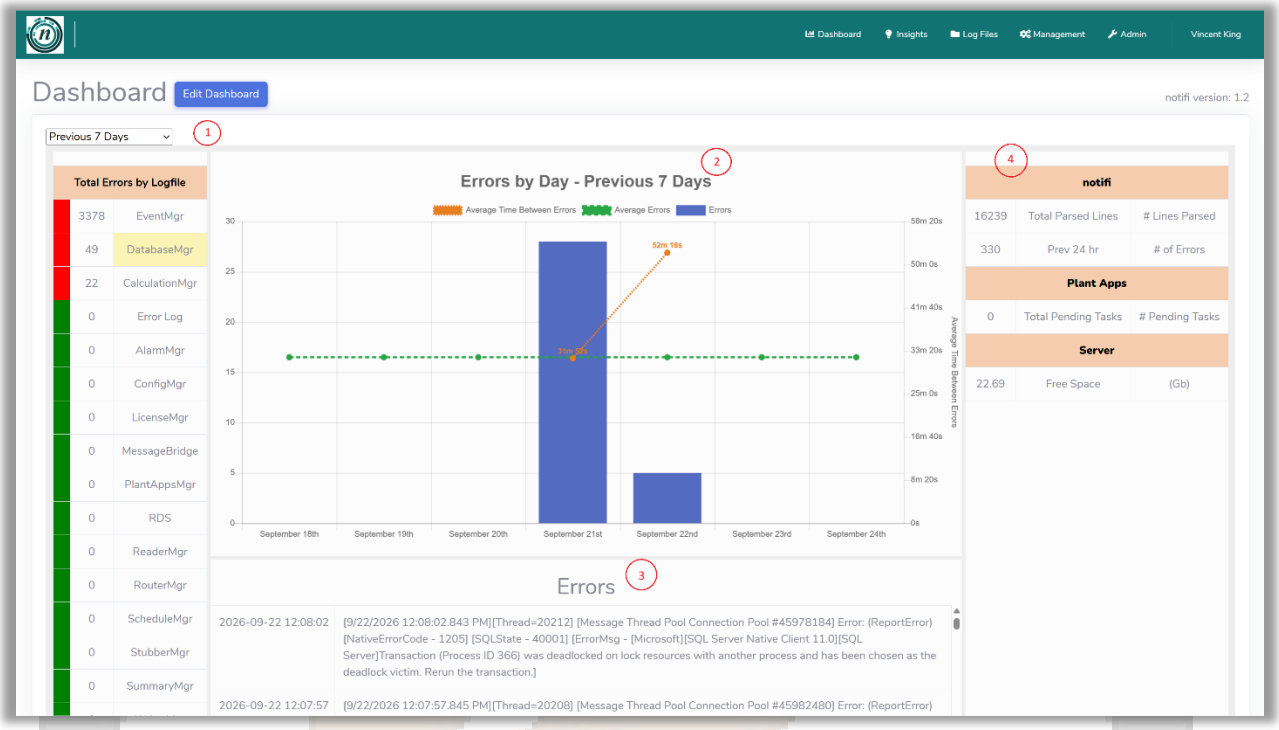


Found Errors

Rule	Line	Date
Uncaught Error	[6/16/2022 5:21:39.772 AM][Thread=5688] [- Main] Error: (ReconnectToDB) Connecting [-1][DRIVER={SQL SERVER};SERVER=KINGDESIGN\SQLEXPRESS;DATABASE=; UID=COMXCLIENT;PWD=******;APP=PLANTAPPS SUMMARYMGR;][[Microsoft][ODBC SQL Server Driver][DBMSLPCN]SQL Server does not exist or access denied.]	2022-06-16 05:21:39
Uncaught Error	[6/16/2022 5:21:13.538 AM][Thread=5688] [- Main] Error: (ReconnectToDB) Connecting [-1][DRIVER={SQL SERVER};SERVER=KINGDESIGN\SQLEXPRESS;DATABASE=; UID=COMXCLIENT;PWD=******;APP=PLANTAPPS SUMMARYMGR;][[Microsoft][ODBC SQL Server Driver][DBMSLPCN]SQL Server does not exist or access denied.]	2022-06-16 05:21:13
Uncaught Error	[6/16/2022 5:20:47.241 AM][Thread=5688] [- Main] Error: (ReconnectToDB) Connecting [-1][DRIVER={SQL SERVER};SERVER=KINGDESIGN\SQLEXPRESS;DATABASE=; UID=COMXCLIENT;PWD=******;APP=PLANTAPPS SUMMARYMGR;][[Microsoft][ODBC SQL Server Driver][DBMSLPCN]SQL Server does not exist or access denied.]	2022-06-16 05:20:47

Dashboard

The notifi dashboard provides a quick visual tool to quickly see the status of your applications by presenting logfile error totals, pareto chart, listed logged errors and notifi sql script analytics.



1) Total Errors by Logfile

Total Errors by Logfile is displayed on the left of the dashboard. The logfiles listed are ordered descending by total number of errors. Color codes are displayed. 0 Errors = Green, 1-10 Errors = Yellow and 11+ Errors = Red.

There is a relative time selection for Previous 24 Hrs, Previous 7 Days, Previous Month (Days) and Previous 12 Months.

2) Pareto Chart – Total Errors

The pareto chart reflects the relative time selection. The breakdown of pareto bars are as follows.

Previous 24 Hrs – Total errors grouped by hours for previous 24 hours.

Previous 7 Days – Total errors grouped by days for previous 7 days.

Previous Month (Days) – Total errors grouped by days for previous for last 30 days.

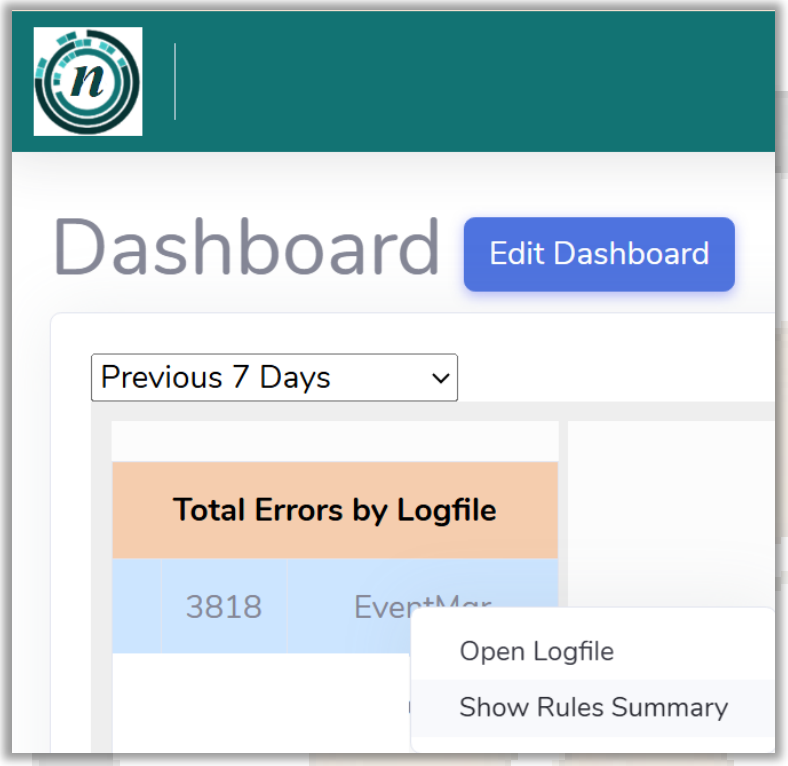
Previous 12 Months - Total errors grouped by month for previous 12 months.

New in Version 1.2: Custom Date Range - lets you pick any start and end date instead of one of the presets above.

3) Errors

The ***Errors*** section list errors for a selected logfile. Click on the logfile name in the Total Errors by Logfile list.

New in Version 1.2: right-click a logfile in the Total Errors by Logfile list for a menu to Open the Logfile directly, or Show Rules Summary - a breakdown of that logfile's errors grouped by which Rule matched.

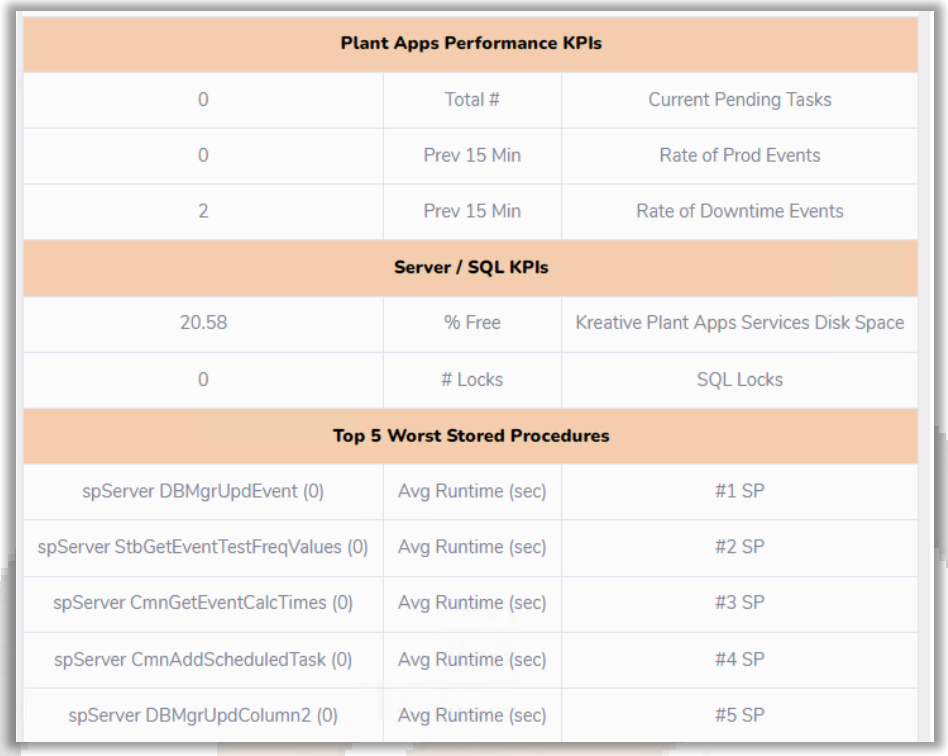


New in Version 1.2: once a logfile is selected, single-click a chart bar to narrow the Errors list to just that bar's time window; double-click a bar to open Rules Summary scoped to that same window.

New in Version 1.2: click the Total Errors by Logfile header to reset the Dashboard back to its initial view.

4) SQL Scripts

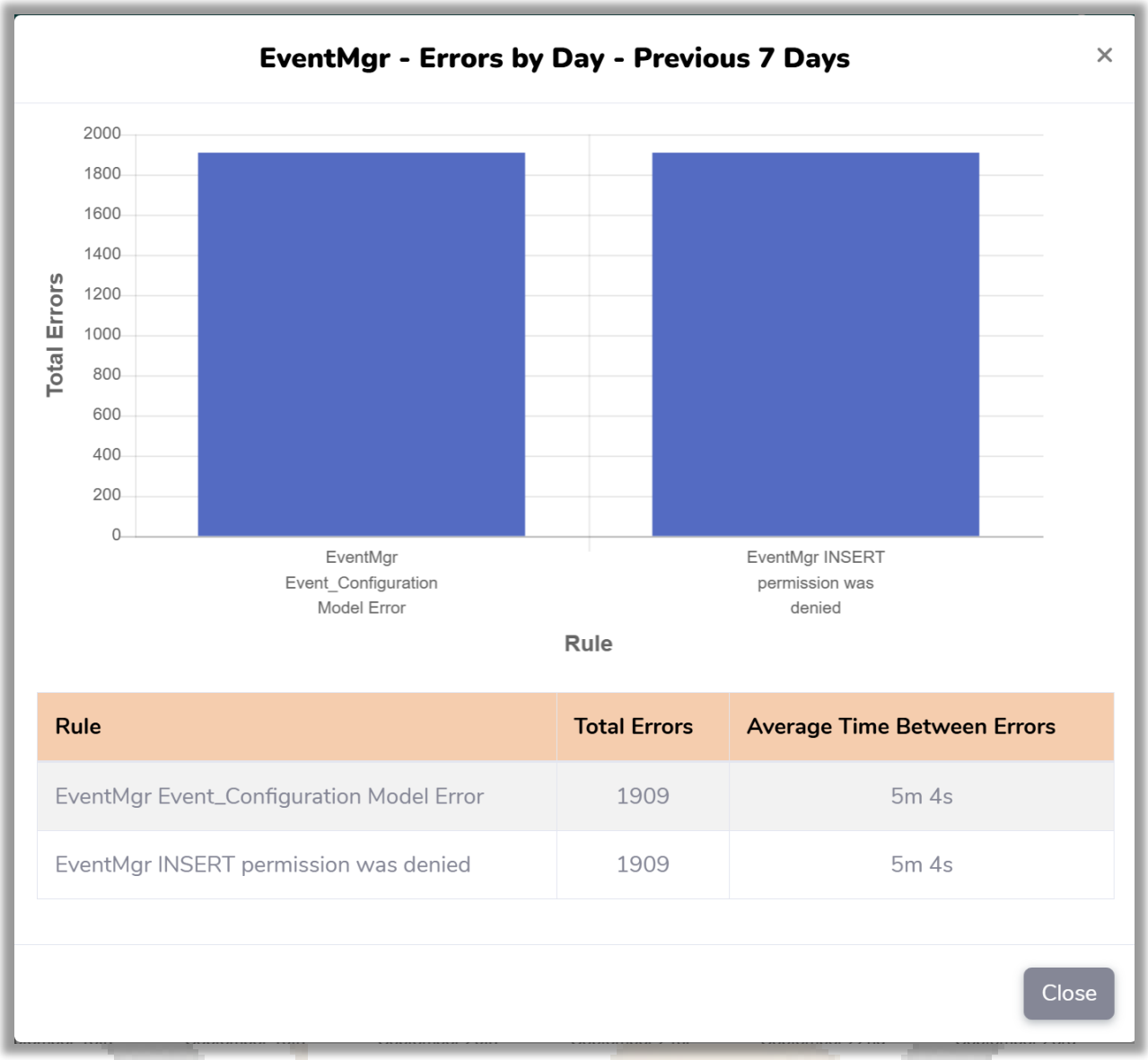
SQL Scripts show results from the scripts that you have configured. The Dashboard functionality allows you to manage your scripts, organize them in the order you require and group them using Titles.



Plant Apps Performance KPIs		
0	Total #	Current Pending Tasks
0	Prev 15 Min	Rate of Prod Events
2	Prev 15 Min	Rate of Downtime Events
Server / SQL KPIs		
20.58	% Free	Kreative Plant Apps Services Disk Space
0	# Locks	SQL Locks
Top 5 Worst Stored Procedures		
spServer DBMgrUpdEvent (0)	Avg Runtime (sec)	#1 SP
spServer StbGetEventTestFreqValues (0)	Avg Runtime (sec)	#2 SP
spServer CmnGetEventCalcTimes (0)	Avg Runtime (sec)	#3 SP
spServer CmnAddScheduledTask (0)	Avg Runtime (sec)	#4 SP
spServer DBMgrUpdColumn2 (0)	Avg Runtime (sec)	#5 SP

5) Rules Summary & Error Details

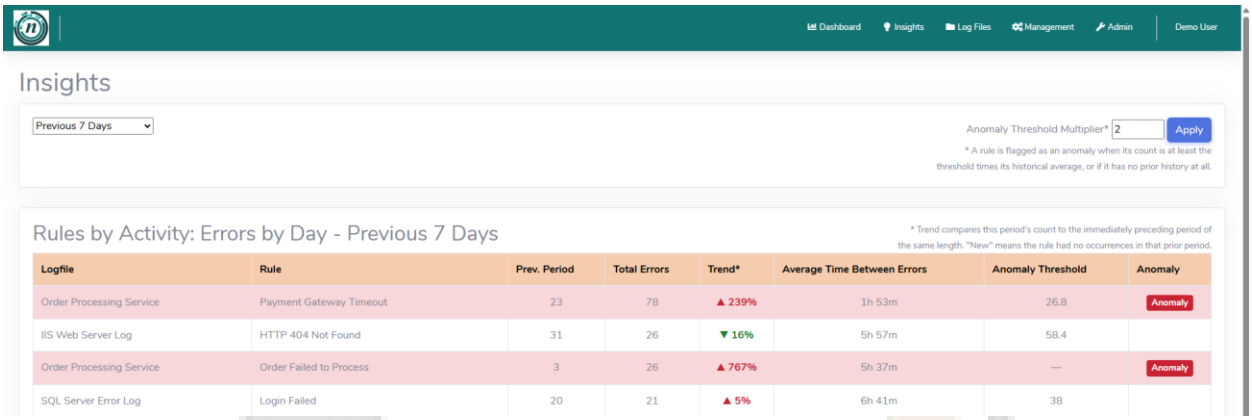
New in Version 1.2. Right-click a logfile in the Total Errors by Logfile list and choose Show Rules Summary (or double-click a chart bar once a logfile is selected) to see that logfile's errors broken down by which Rule matched, along with the average time between occurrences for each Rule.



Click any Rule in the table to open Error Details - a chart plotting the time between each individual occurrence of that Rule over actual dates, with a dashed reference line showing the overall average. Drag across the chart to zoom into a date range, and use Reset Zoom to return to the full view. The table below the chart lists each individual occurrence.

Insights

New in Version 1.2. The Insights page (available from the top navigation) shows every Rule across all Logfiles at once, so it's easy to see which ones need attention without checking each Logfile individually.



Prev. Period - the count of that Rule's errors in the immediately preceding period of the same length, shown alongside Total Errors for context when interpreting the Trend percentage.

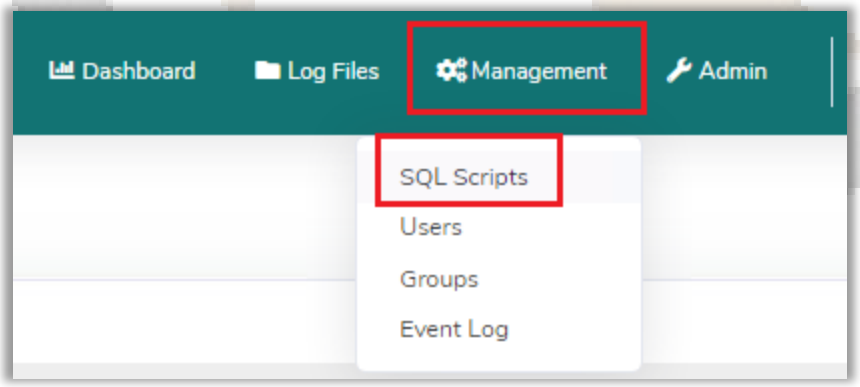
Total Errors - the count of that Rule's errors in the selected time period, same as elsewhere in the app.

Trend - the percent change compared to the immediately preceding period of the same length, or New if the Rule has never occurred before.

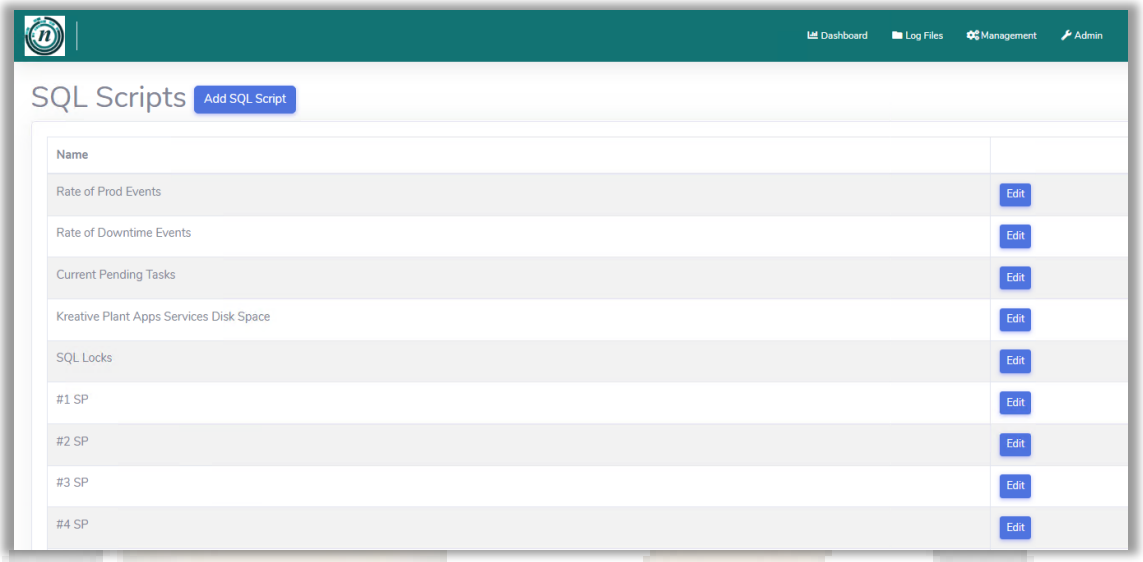
Anomaly Threshold - the actual cutoff Total Errors is compared against for that Rule (its historical average times the Anomaly Threshold Multiplier above). Shown as a dash for a brand-new pattern with no prior history at all, which is flagged as an anomaly for that reason rather than for crossing a number.

Anomaly - flagged when a Rule's count is at least the Anomaly Threshold Multiplier times its historical average, or when it has no prior history at all. The threshold can be adjusted directly on the page - change the value and click Apply to see the results update immediately.

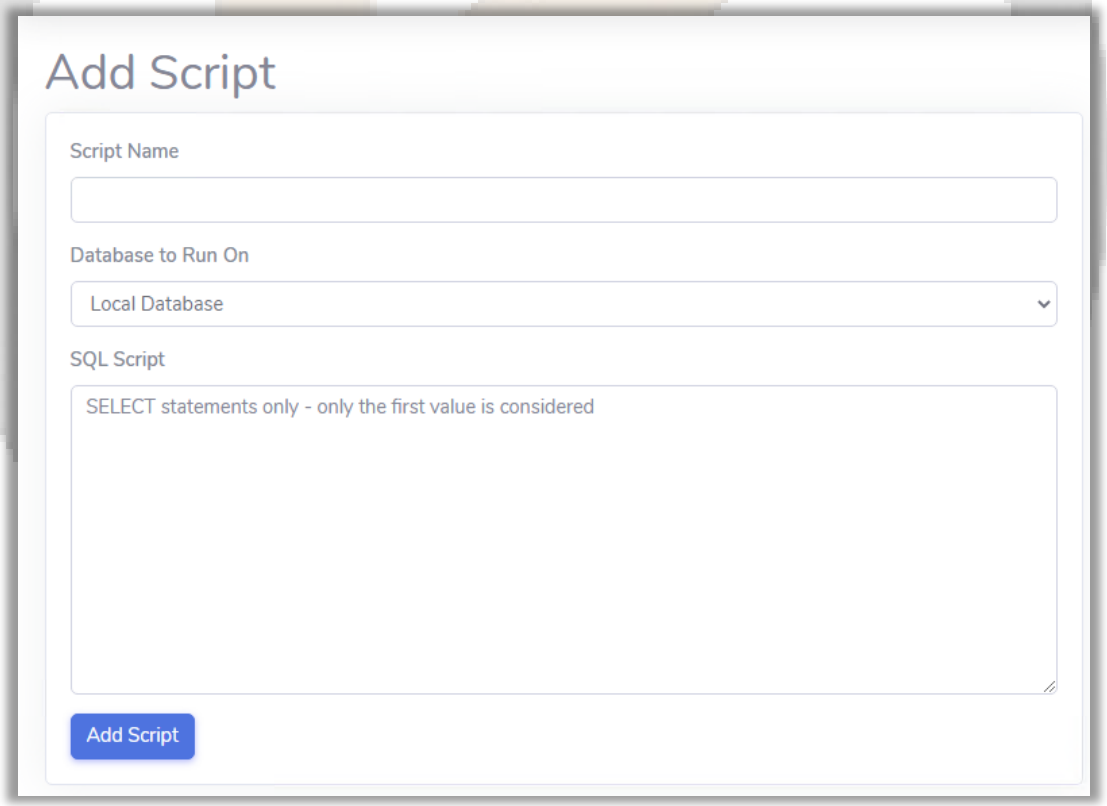
Manage SQL Scripts



SQL Scripts can be created and managed by clicking ***Management*** on the toolbar, then select ***SQL Scripts***. The ***SQL Scripts*** page is displayed.



Click ***Add SQL Script*** to create a metric using a sql script. The ***Add Script*** page is displayed.

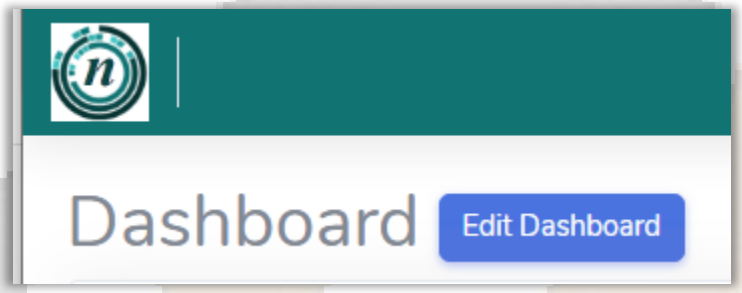


Script Name – Add a name that uniquely identifies the script metric that you are creating. This name will be displayed in the ***SQL Scripts*** section on the dashboard.

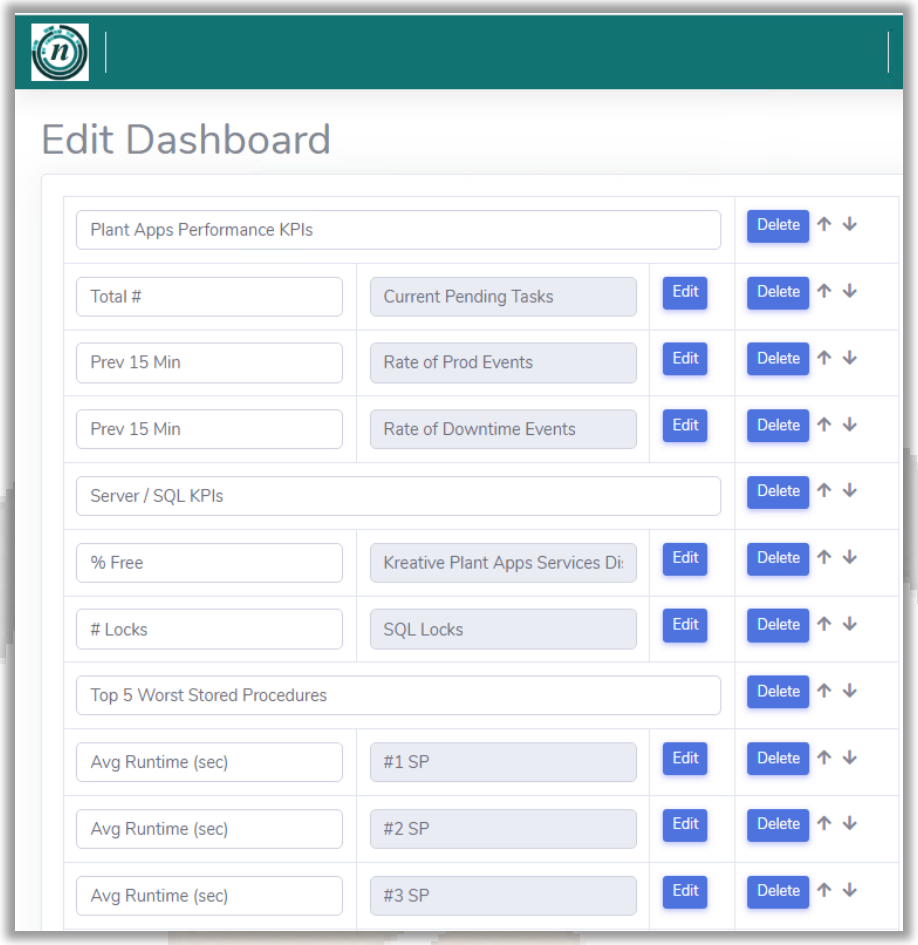
Database to Run On – Select the pre-configured database that you will be running script against. The ***Local Database*** refers to the same sql database that the notifi database was installed.

Notifications

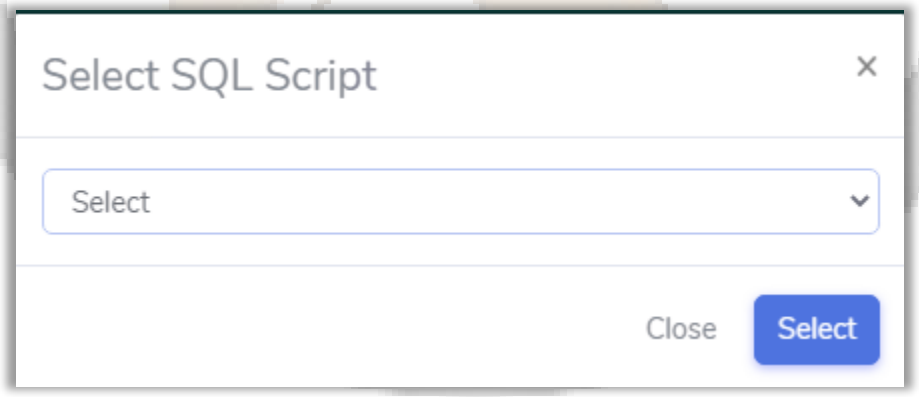
Edit Dashboard



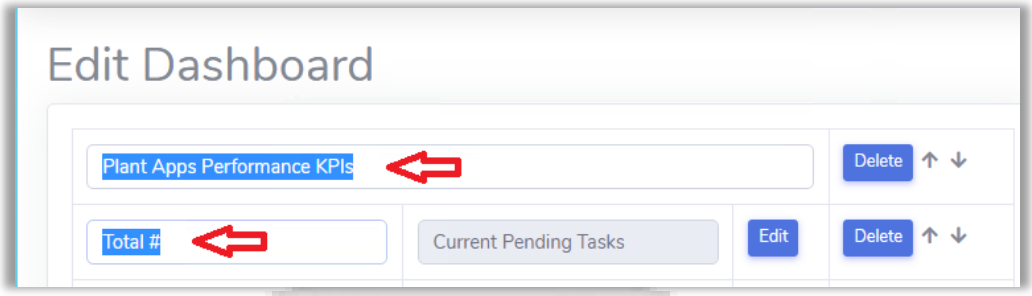
Click the ***Edit Dashboard*** button to manage the SQL Scripts formatting on the dashboard. The edit dashboard page is displayed that allows you to add, edit and delete SQL scripts and titles.



Edit button allows you to select an existing SQL Script.

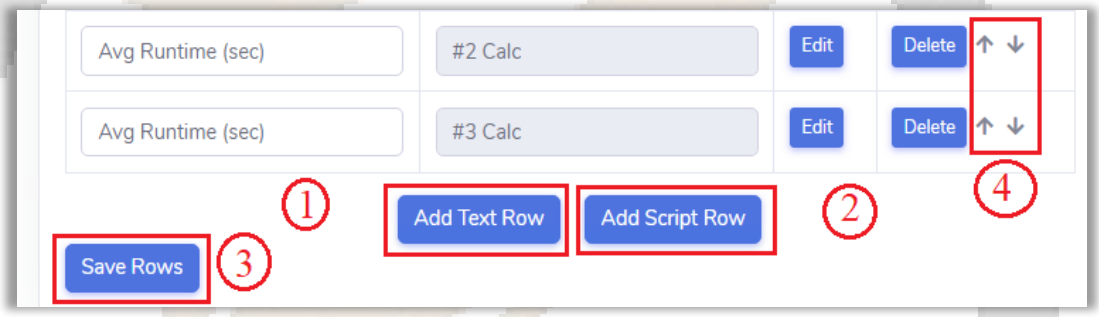


And update SQL Script descriptions and section Titles.



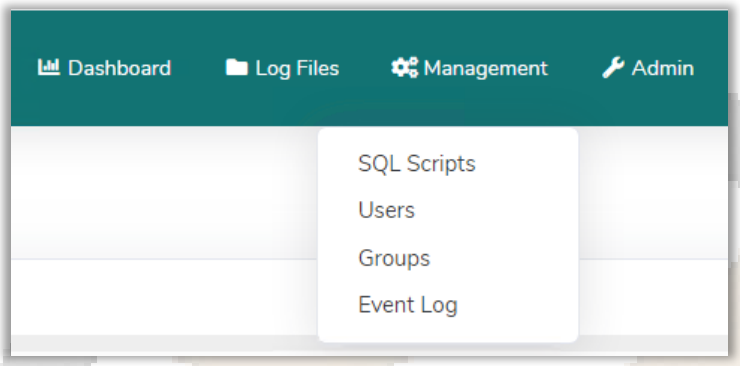
To add a new Text Row (Title or Header), click on the ***Add Text Row (1)*** button. Click the ***Add Script Row (2)*** to add a new SQL script metric and ***Save Rows (3)*** to save all changes.

The ***Up and Down arrows (4)*** on each script or title row can be used to manage the position of rows.



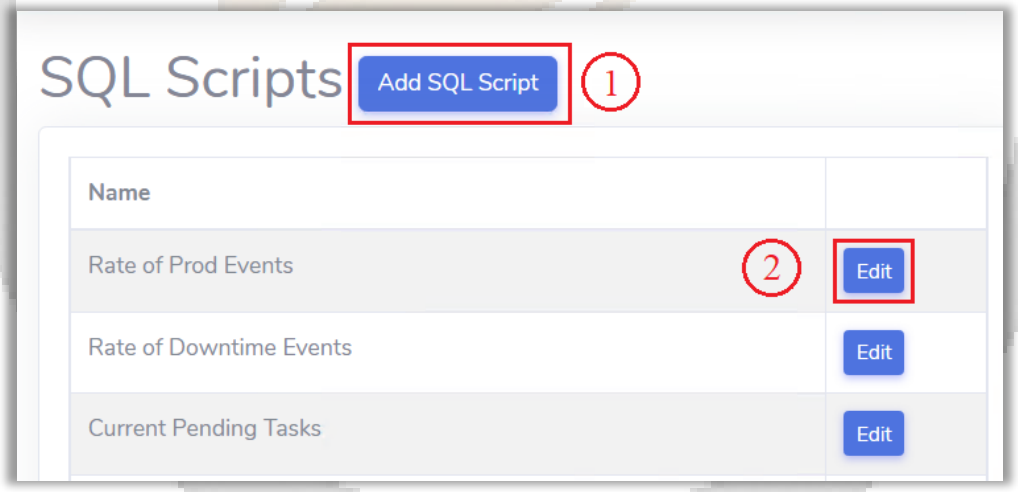
Management

Management allows the user to manage ***SQL Scripts***, ***Users***, ***Groups*** and to view the ***Event Log***. Available to all users that are members of the administration or superuser groups.

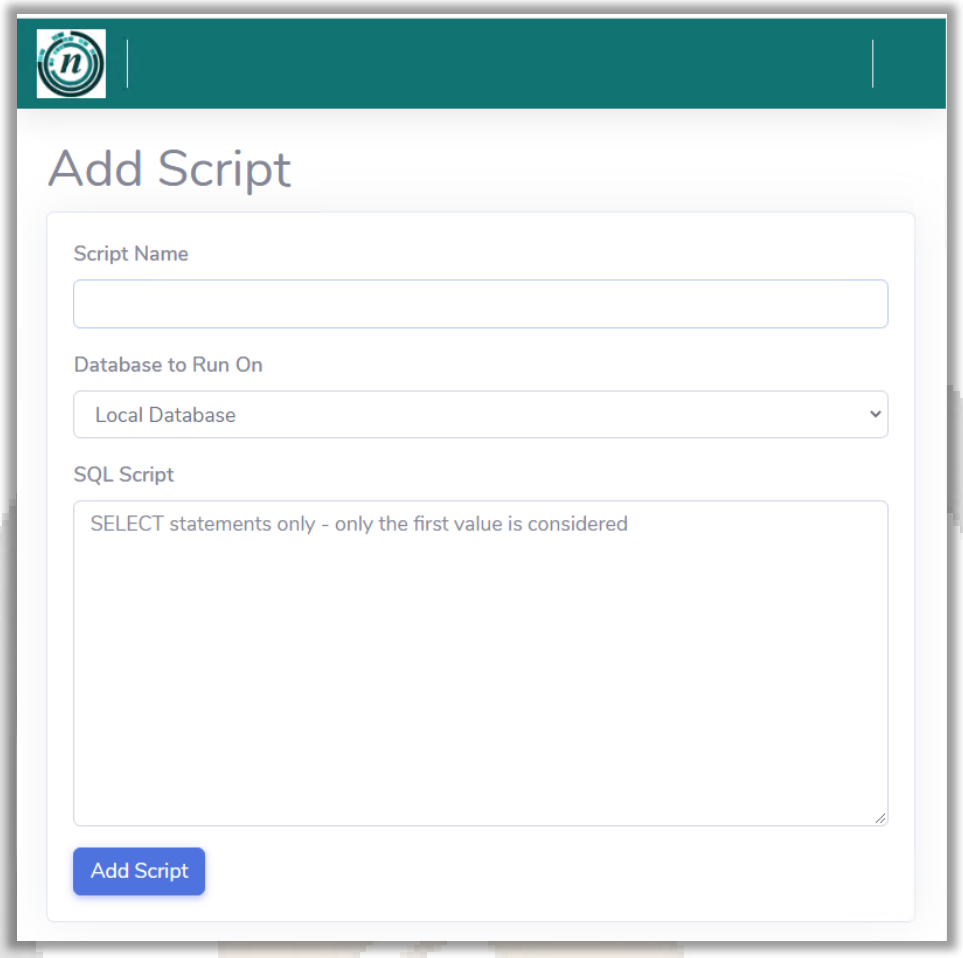


SQL Scripts

SQL Scripts allows administrators to create new sql scripts by clicking the button ***Add SQL Script (1)*** and manage existing scripts by selecting the ***Edit (2)*** button on a specific script row.



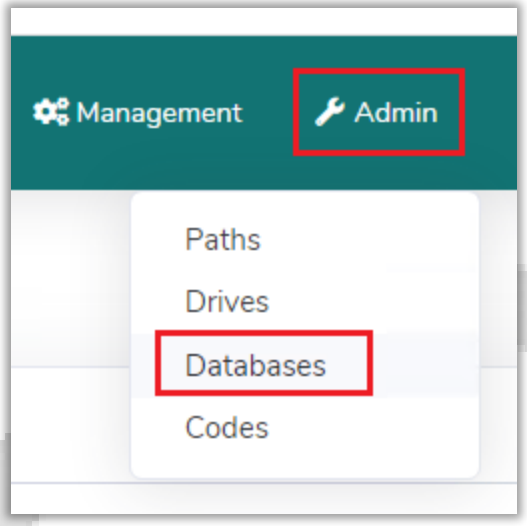
Add SQL Script



New SQL Script(s) can be added by clicking the ***Add SQL Script*** button after selecting Mangement / SQL Scripts from the menu.

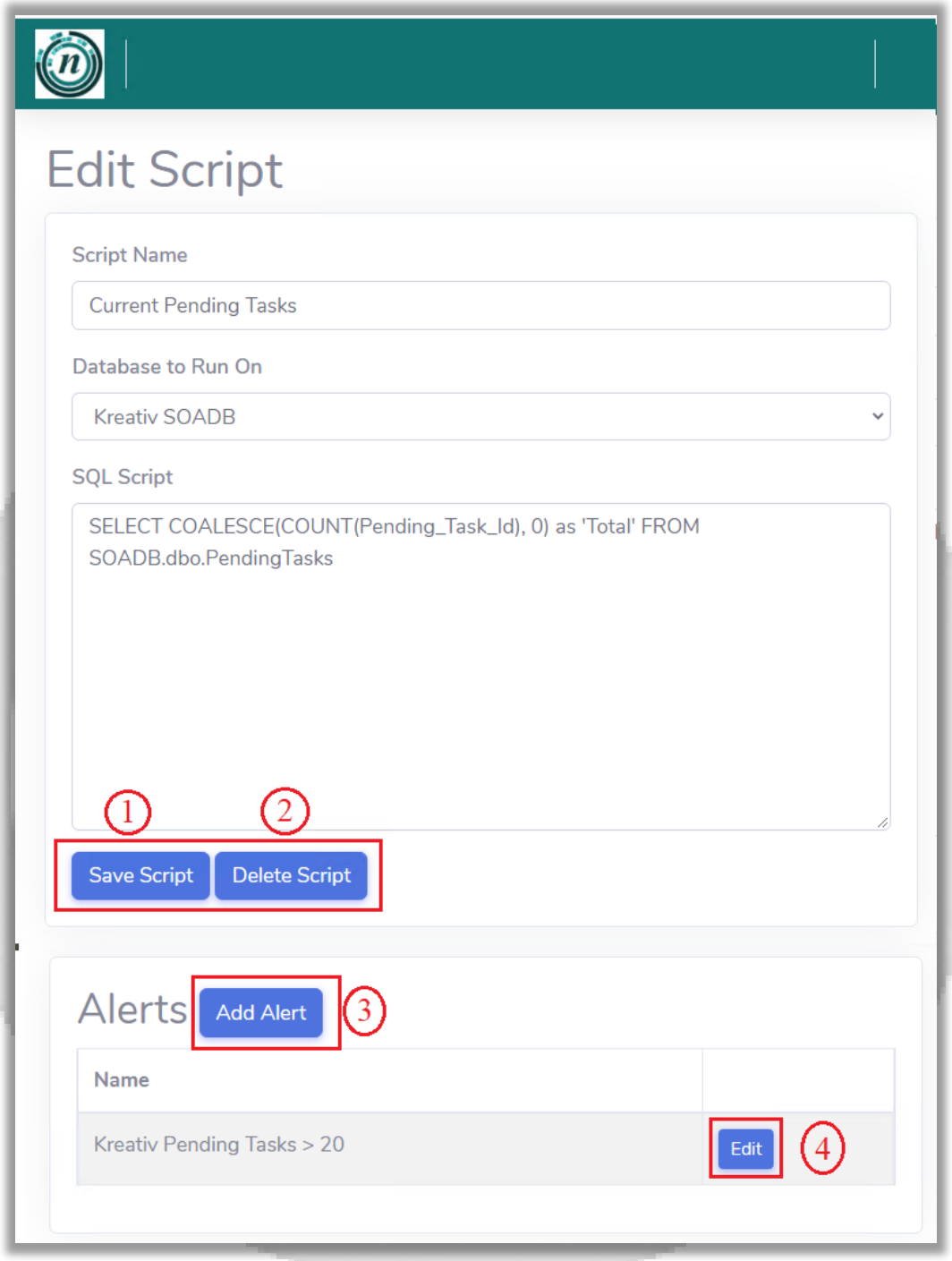
Script Name – enter a unique name that describes the script. This will be used for display on the Dashboard.

Database to Run On – select the sql database to execute the script against. (Select Admin / Databases to configure external databases. Local Database refers to the sql / mysql instance that the notifi database has been installed.



SQL Script – Enter the SQL Script to execute and return the desired results. As noted in the above screenshot, only the first column from the result set will be used. This result column can then be used for alerts based on an acceptable range.

Once a sql script has been added, select the ***Edit*** button to manage the configuration and add or manage alerts.



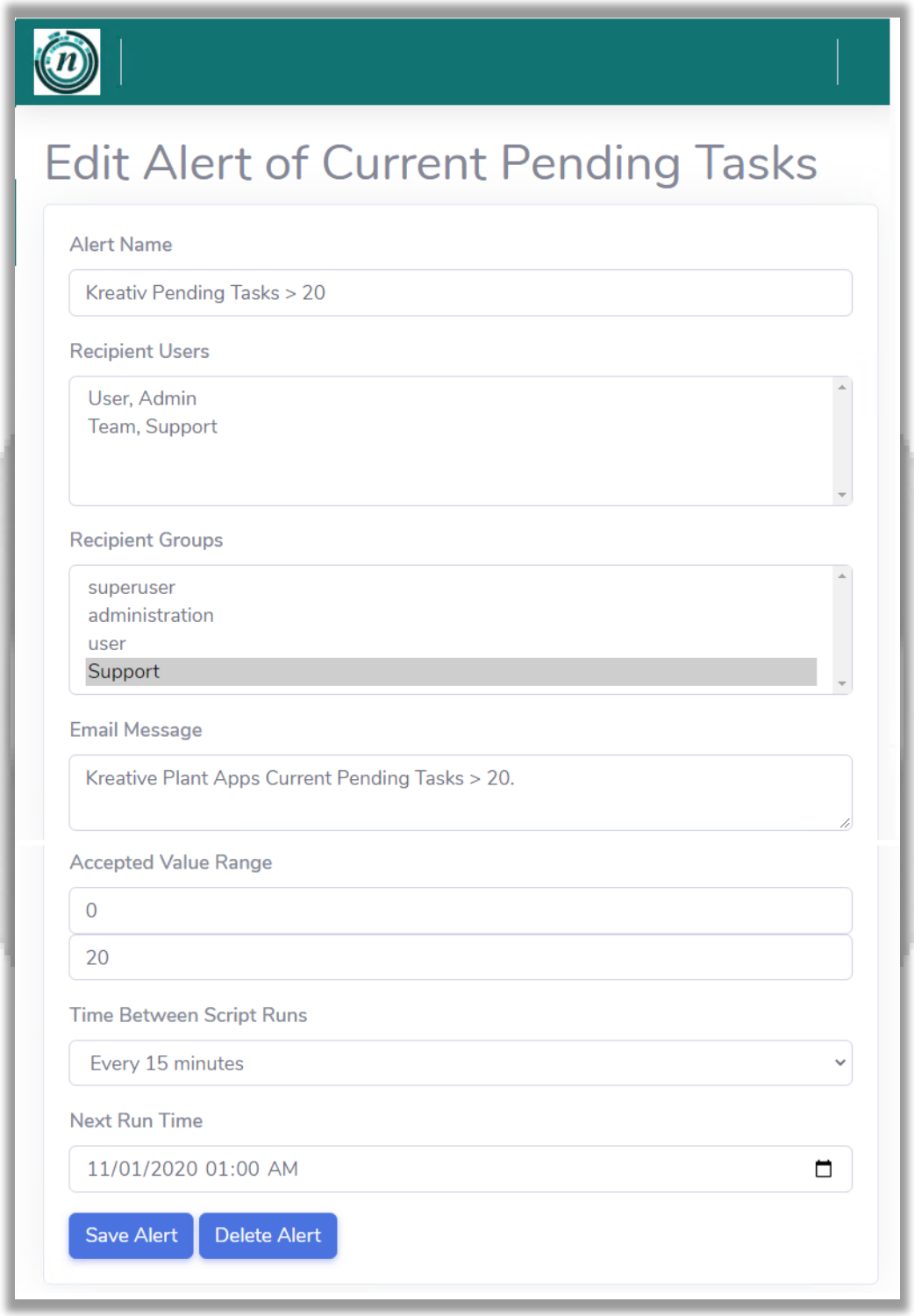
Save Script (1) – click the Save Script button to save any changes.

Delete Script (2) – click Delete Script to delete the currently selected SQL Script.

Add Alert (3) – Add Alert allows you to define Alerts for the selected SQL Script.

For existing Alerts on the selected SQL Script, click the ***Edit (4)*** button to modify the alert configuration.

Managing SQL Script Alerts



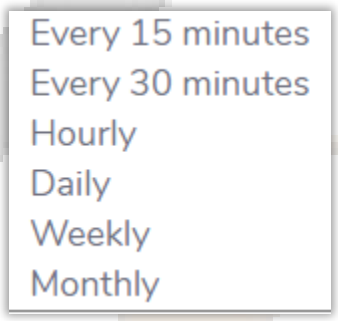
Alert Name – unique name for the Alert. It is recommended that you include a phrase that will allow you to quickly determine the server/database that this alert is associated with.

Recepient Users / Recepient Groups – user and groups that have been configured for receipt of notifications. Each user is a member of one or more groups and is configured for email and/or SMS alerts. Users and Groups are configured by selecting Management then Users or Groups from the notifi menu.

Email Message – enter a message to be included in the content of the email alert.

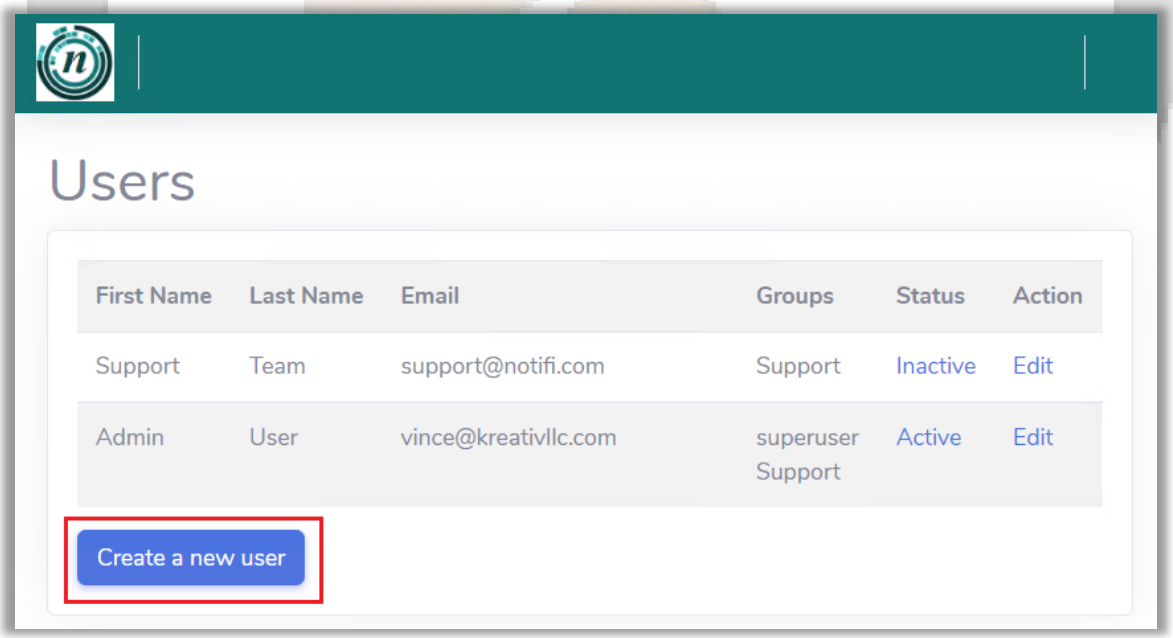
Accepted Value Range – enter a minimum and maximum value that is acceptable. The range will include the values entered, i.e. >= min AND <= max.

Time Between Script Runs – select an option for the frequency of executing the sql script. Options are shown below.



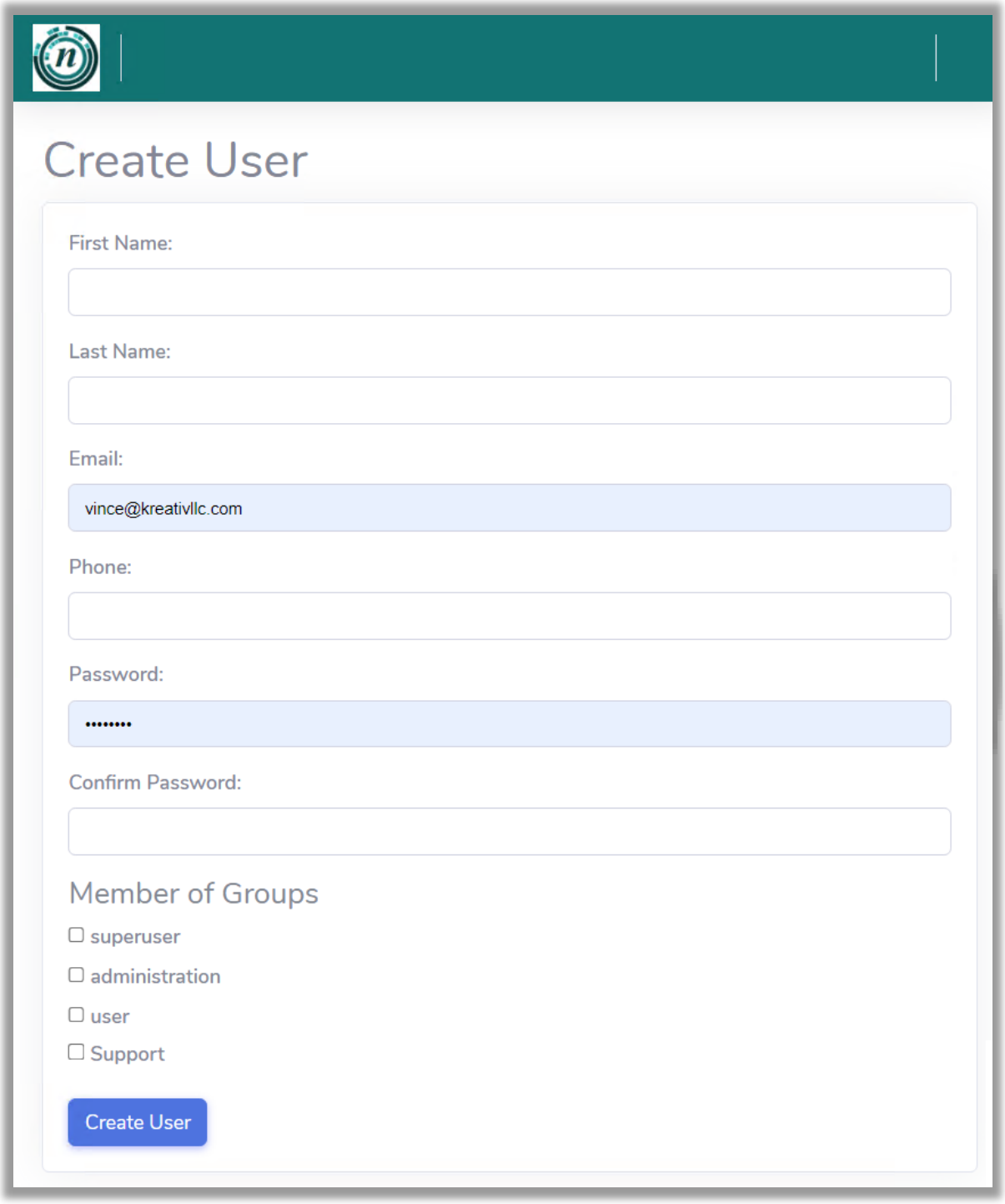
Next Run Time – allows user to set the intial start of the run.

Users



New Users can be added by clicking the ***Create a new user*** button. For existing users, click on the Status hyperlink to set the user as **Active** or **Inactive**. Click on the Action **Edit** hyperlink to edit the user configuration.

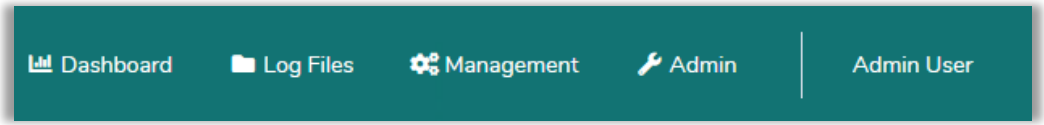
Create a new user



Enter a **First Name**, **Last Name**, **Email** (also used as login), **Phone** (if SMS will be used) and a **Password** followed by **Confirm Password**.

Members of Groups – shows all configured groups. Superuser, administration and user are pre-defined groups.

superuser – all menu items availabe including **Admin**.



administration – user has access to Dashboard, Log Files and Management.

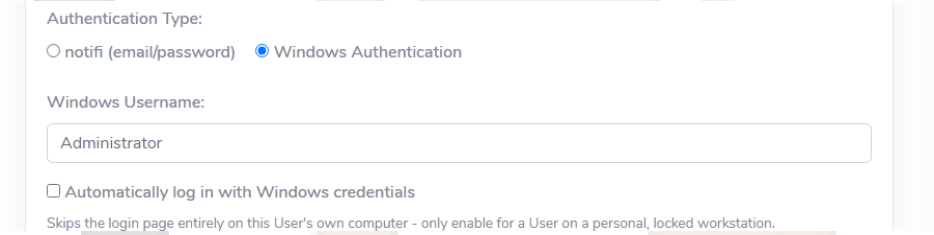
User – configured user only has access to Dashboard, read only, cannot edit Dashboard.

Any administrator defined groups are shown below the pre-defined notifi groups.

Authentication Type - choose notifi (email/password) or Windows Authentication for how this User signs in. Windows Authentication accounts also need a Windows Username (e.g. DOMAIN\username) instead of a password.

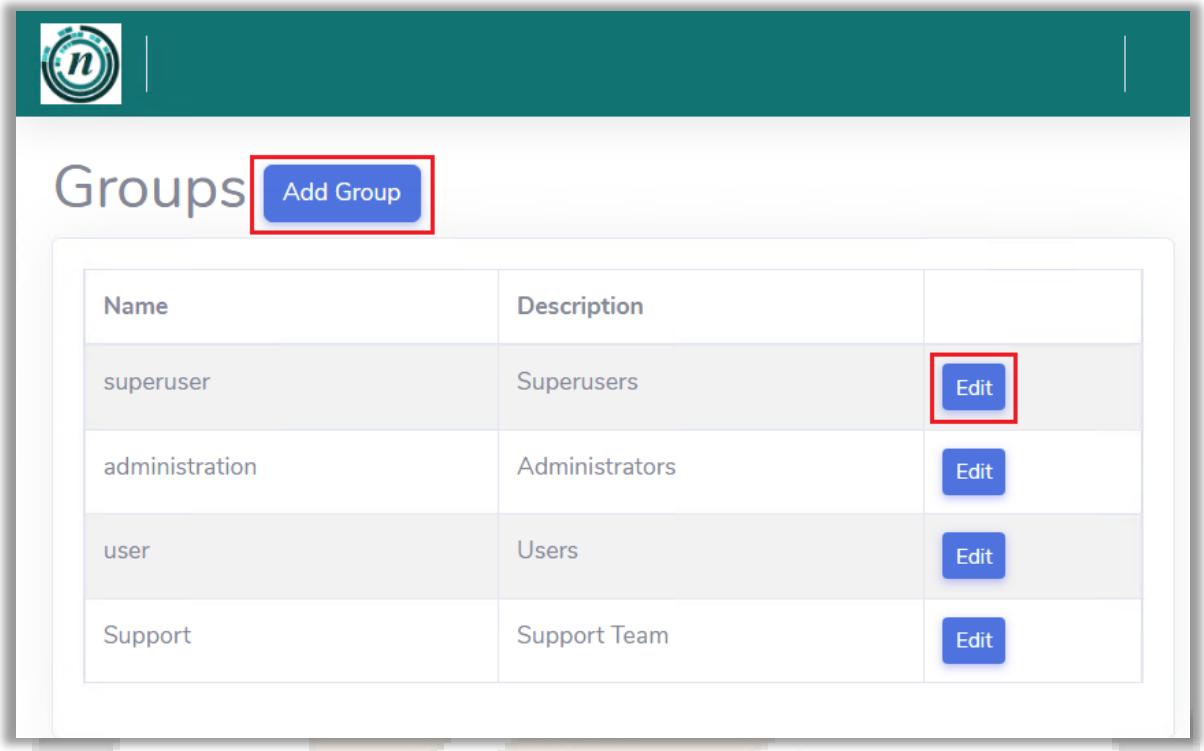
Automatically log in with Windows credentials - only shown for Windows Authentication accounts. When enabled, this User's browser skips the login page entirely after their first Windows sign-in on that computer. Only enable this for a User on a personal, locked workstation, since it removes the visible sign-in step.

Click **Create User** to save changes and create the new user.

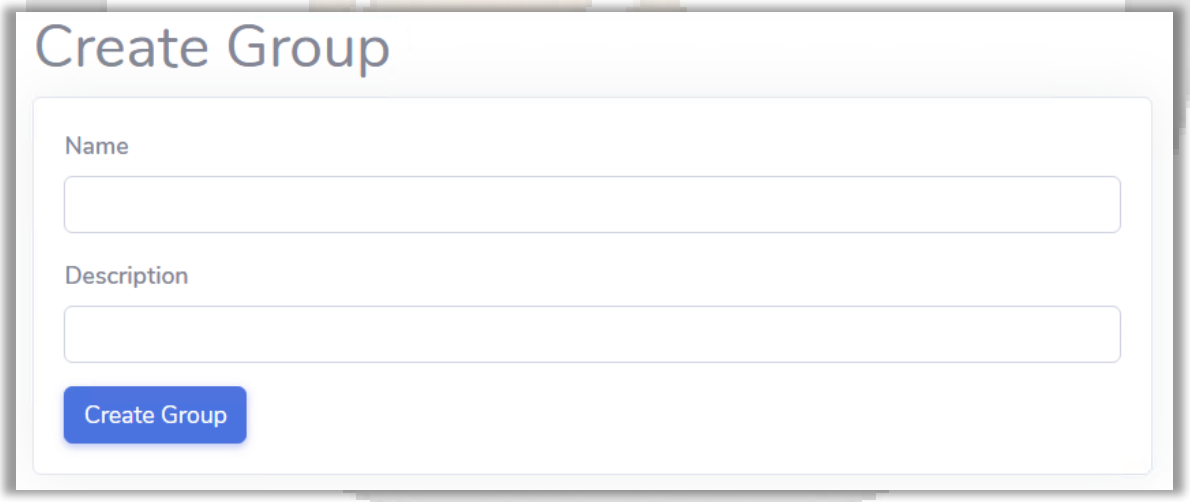


Groups

Add and manage existing user groups by selecting Management / Groups from the notifi menu.



Click the Add Group button to add a new group. For existing groups click the Edit button to manage.



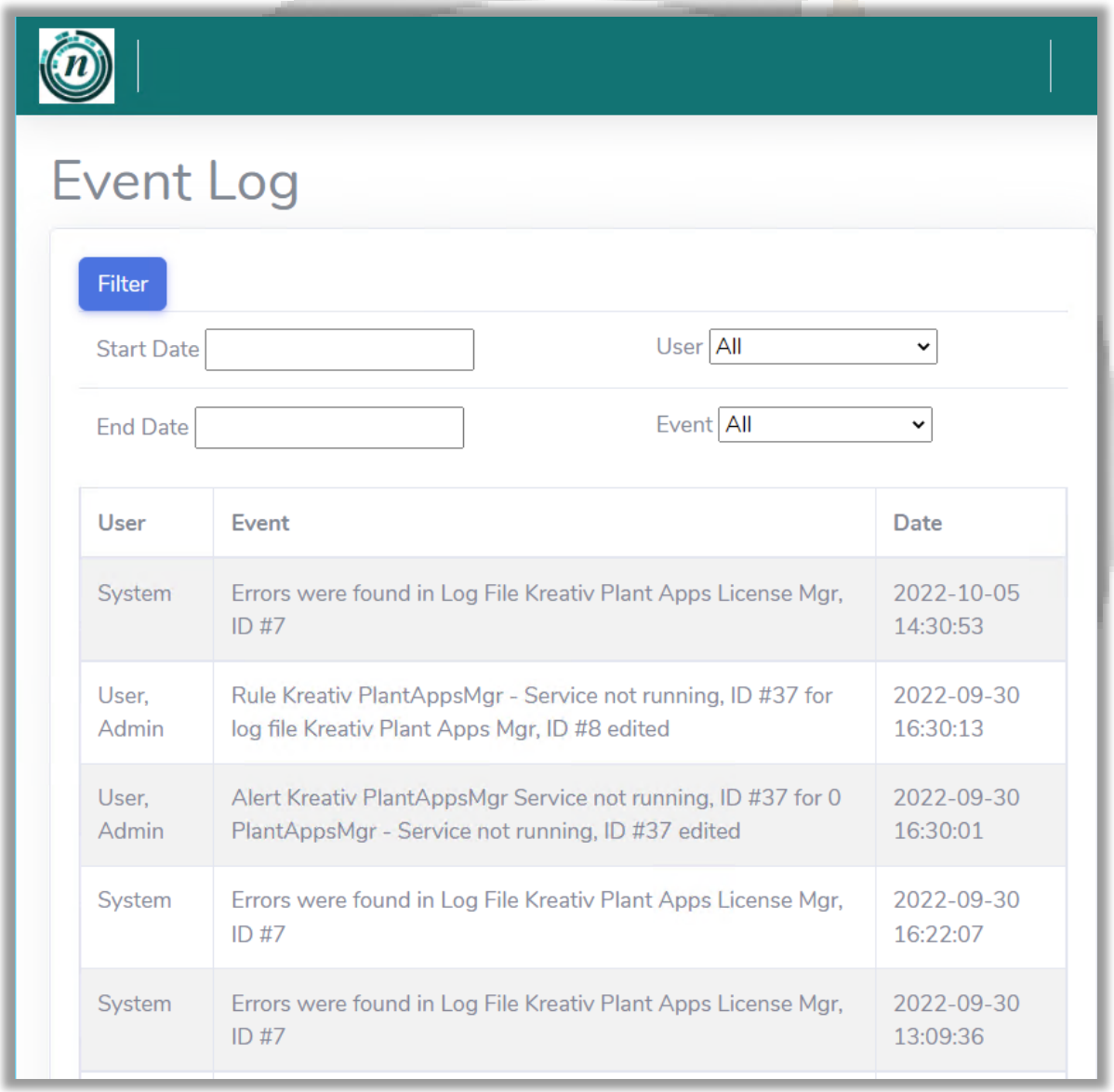
Enter a unique Name and detailed Description then click **Create Group**. You will be returned to the Groups page where you can add additional details for the newly created group.

Warning! Modifying the superuser and administrator groups may affect and/or prevent access to critical features in notifi. It is recommended to create new superuser or administration groups to change configuration. Always make sure to have at least one

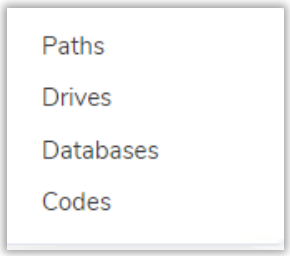
user configured with superuser access to ensure constant access. Passwords are encrypted and not available through the notifi UI or database.

Event Logs

Event Logs allows administrators to review system messages. Some basic search features are included.

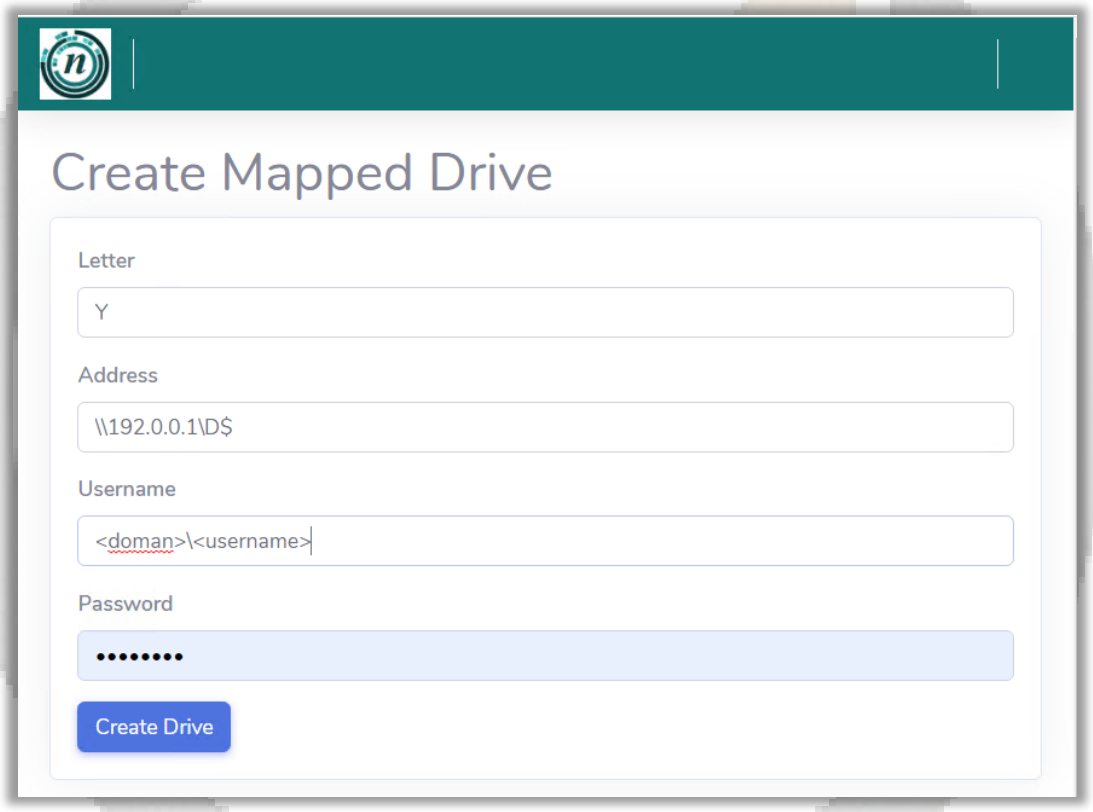


Admin



Drives

Configure server virtual drive where log files are located.



Enter a virtual Letter. Select a drive letter that is not being used on the notifi server.

Address – IP or server name and shared folder where log files reside.

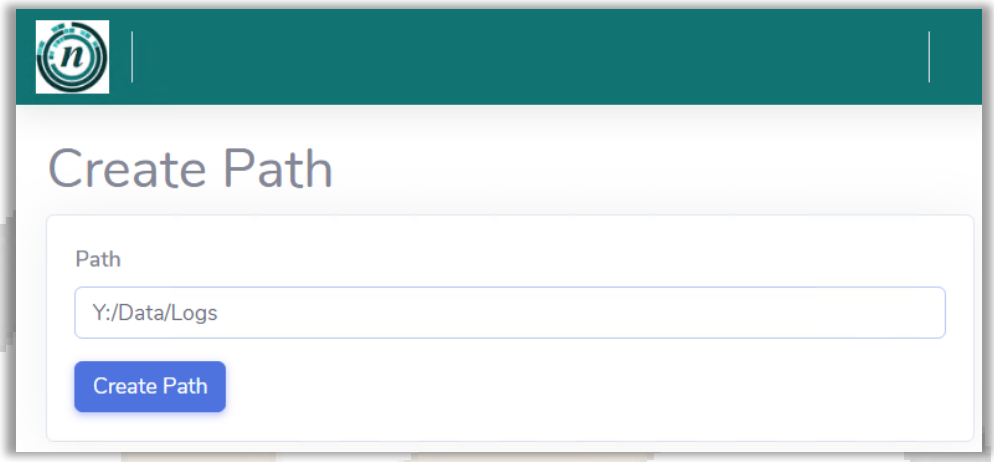
Username – full path of user with a minimum of READ only access to the path/folder.

Password – password for declared Username.

Click **Create Drive** button to save configuration. This Mapped Drive will be used to configure the full path of the folder where log files are stored.

Paths

Configure specific path to log file(s) folder.

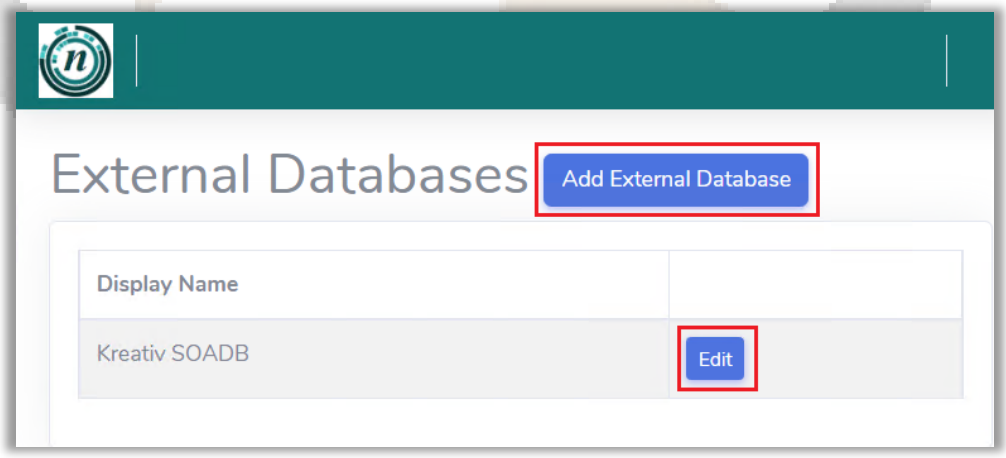


Enter the Path to the folder where the log files reside using the pre-defined Drive.

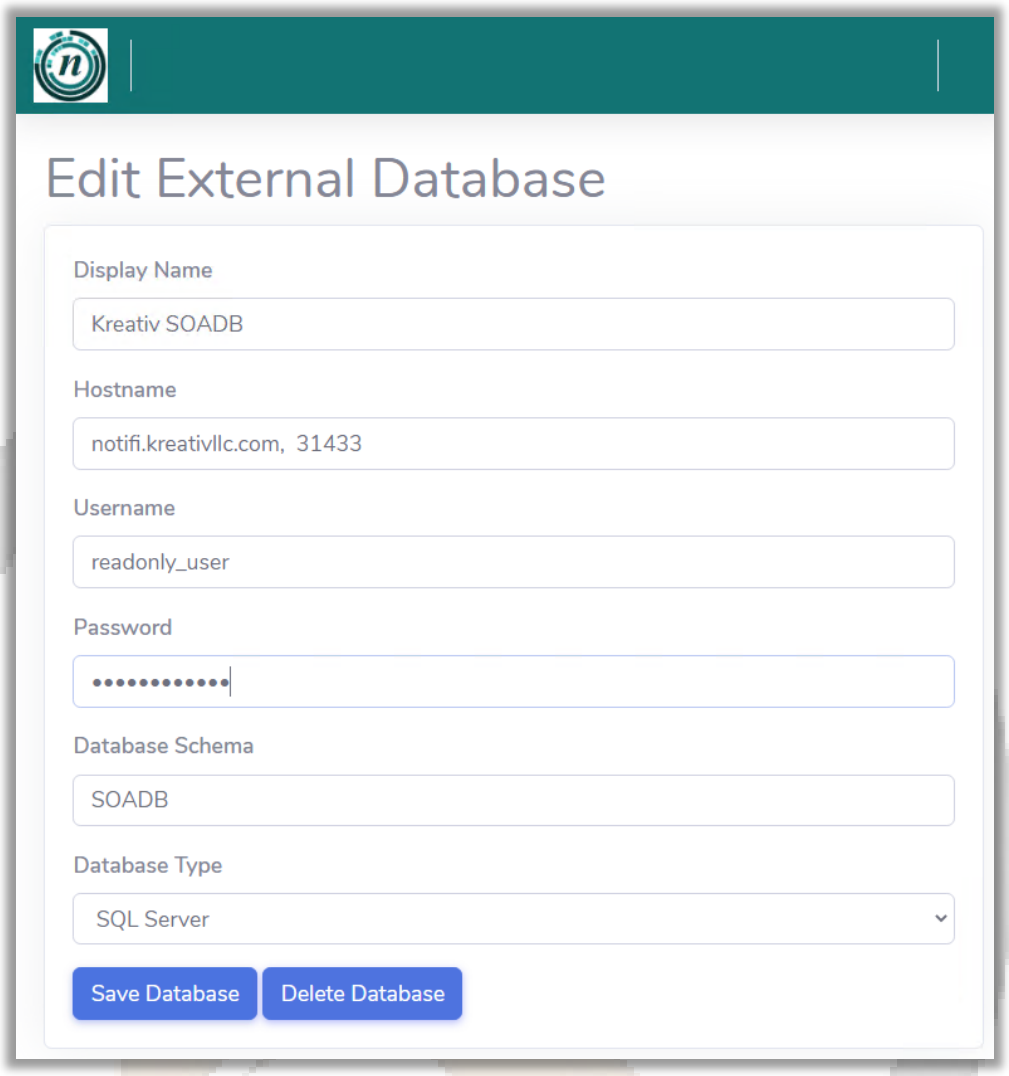
Note: notice the format of the path in the above screenshot. It is required to use forward slashes (/) in the folder Path.

Databases

Select **Admin** / **Databases** to configure sql database connections to be used in the configuration of **SQL Scripts**.



Select Add External Database to configure a new database connection.



Display Name – unique display name that will be used in the select database dropdown.

Hostname – hostname / instance for database including port, if different from default.

Username – user that has minimum of READ only access to the server / database.

Password – password for configured user.

Database Schema – enter database/schema name.

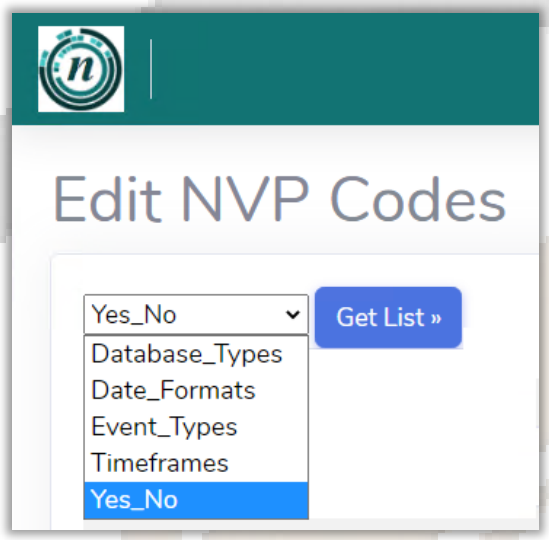
Database Type – select the type of database that is being configured. SQL Server or MySQL.

Click **Save Database**. If editing an existing database connection, the **Delete Database** button can be used to delete the configuration for the selected database.

Codes

Codes allow access to the SYSTEM codes used by notifi. This is NOT intended for user modification but instead available to superusers in the rare event that the notifi support staff needs to make modifications.

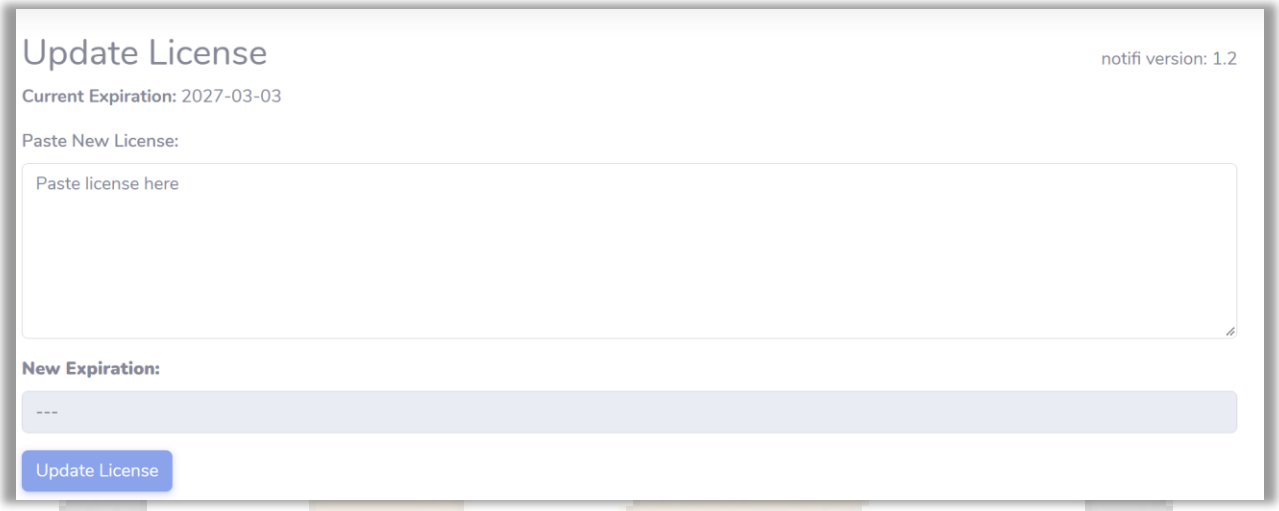
New in Version 1.2: selecting a different context/category above now refreshes the list immediately, without needing an extra button click.



Warning! Do not make changes to the NVP Codes. These are system codes used by the notifi. Any changes can affect the effectiveness and operability of the notif application.

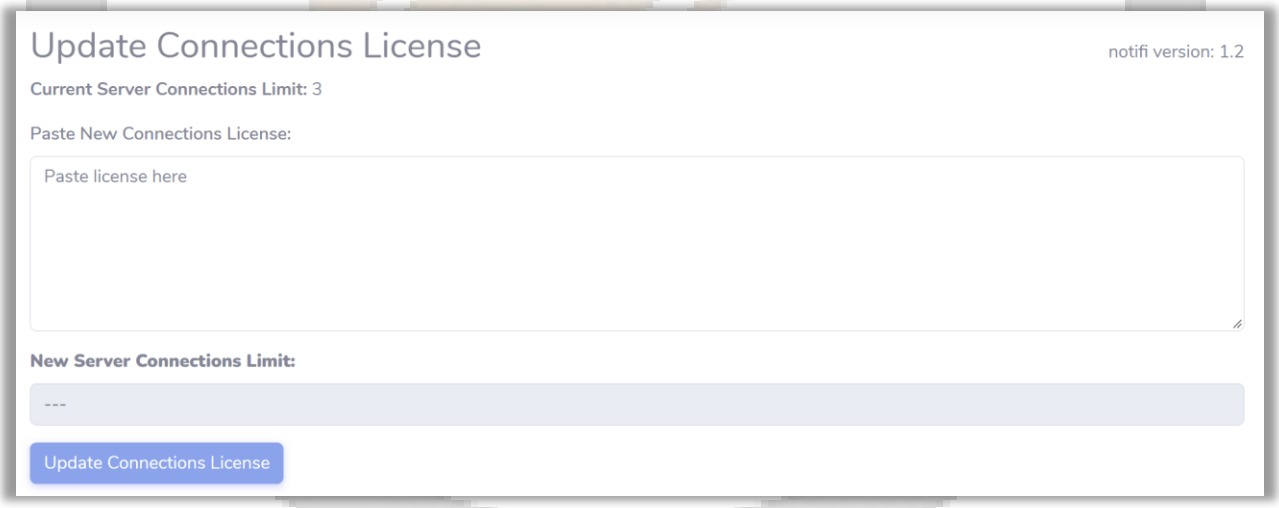
License

View the current license expiration date and paste in a new license (provided by application support) to update it.



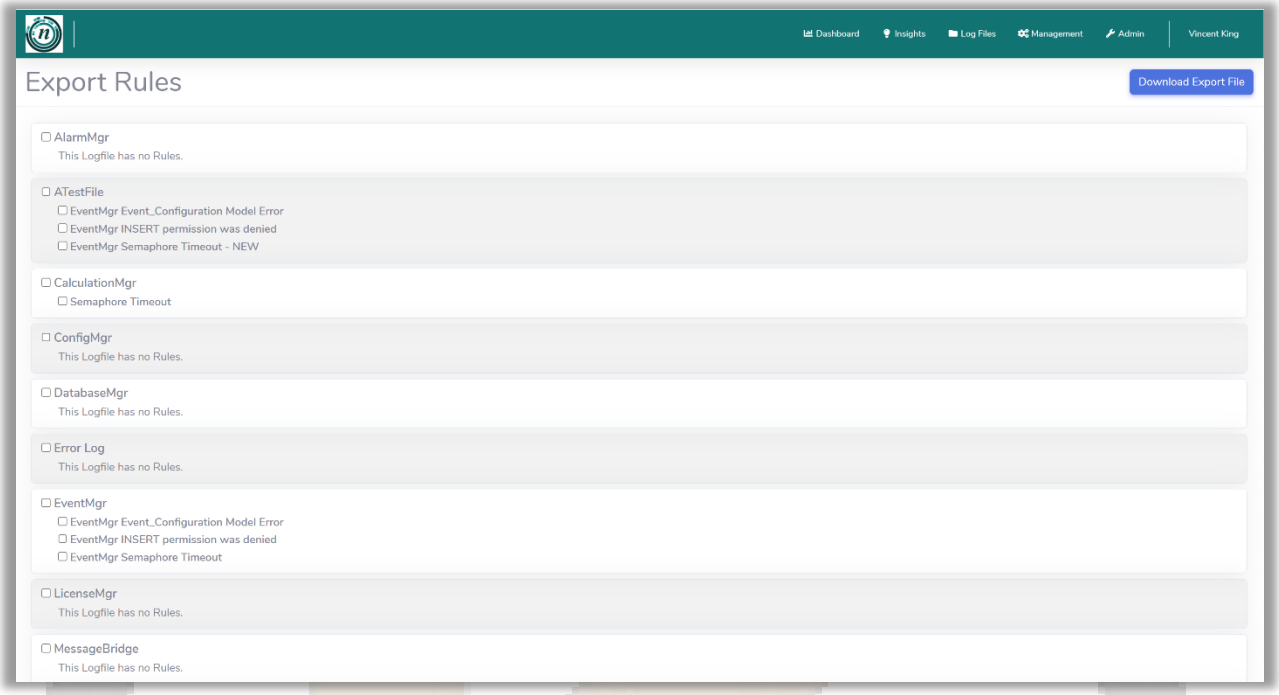
Connections License

View the current limit on how many Mapped Drive server connections this install is allowed, and paste in a new connections license (provided by application support) to change it.



Export Rules

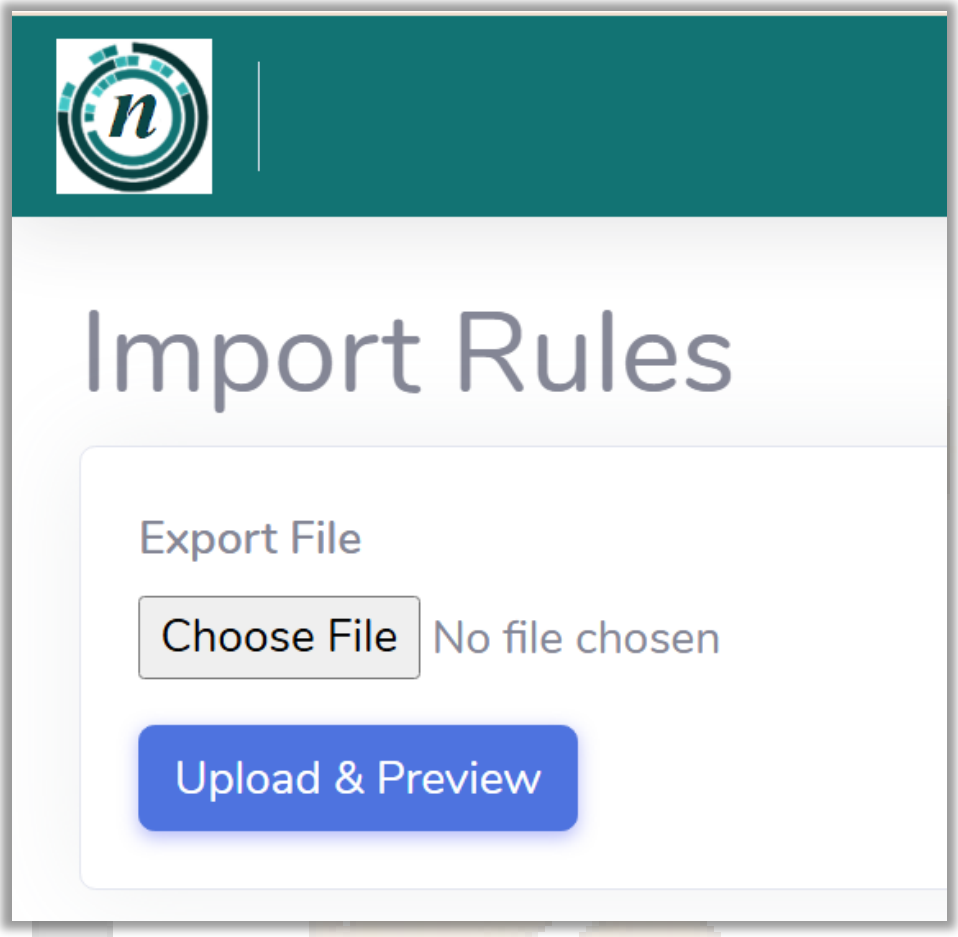
New in Version 1.2. Superusers can export selected Rules - including their Elements, Alerts, and Alert settings - from one or more Logfiles to a file, for reuse on another notifi install.



Check the Rules to include (or check a Logfile's own checkbox to select all of its Rules), then click Download Export File.

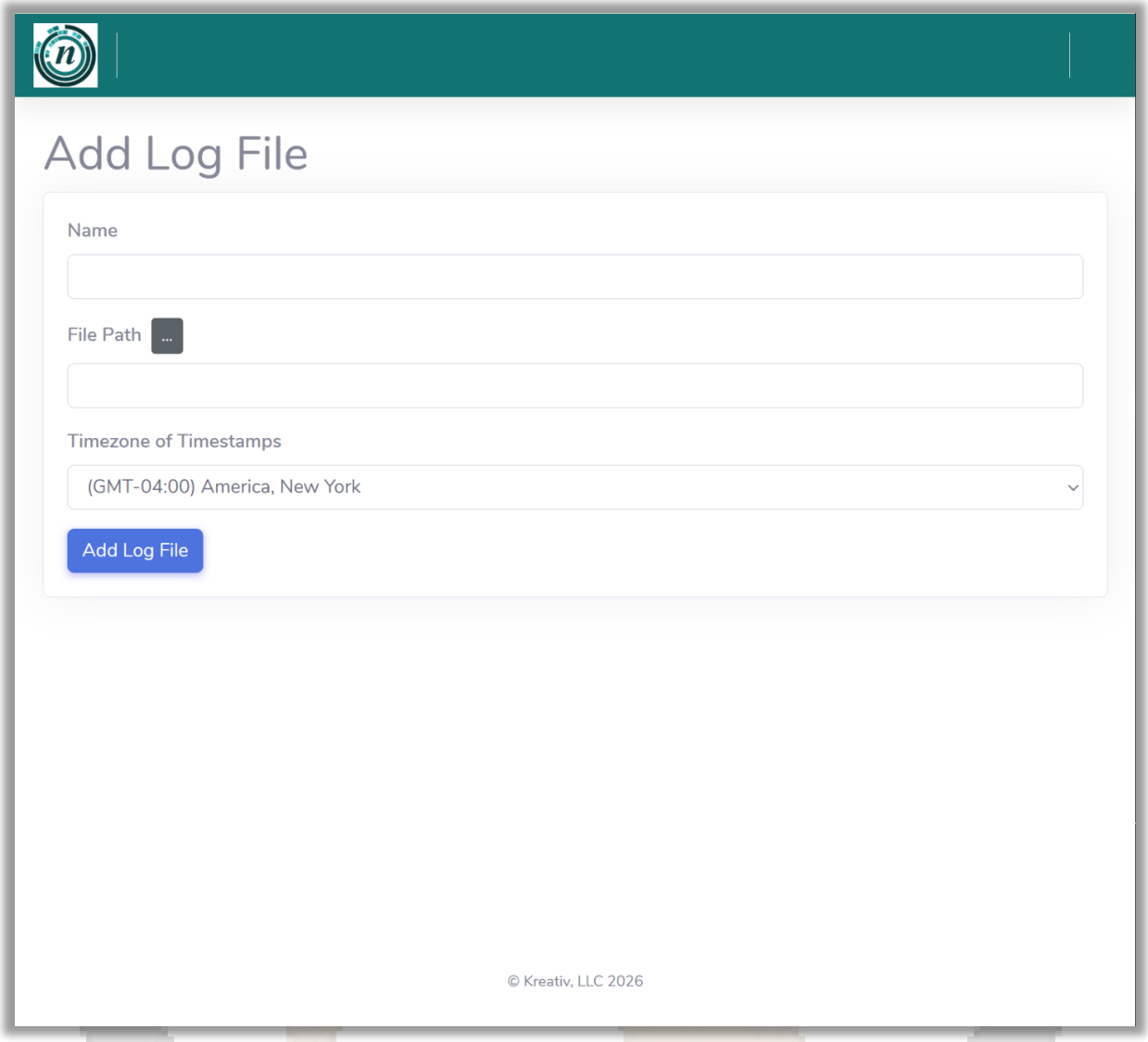
Import Rules

New in Version 1.2. Upload a Rules export file to bring those Rules into this install.

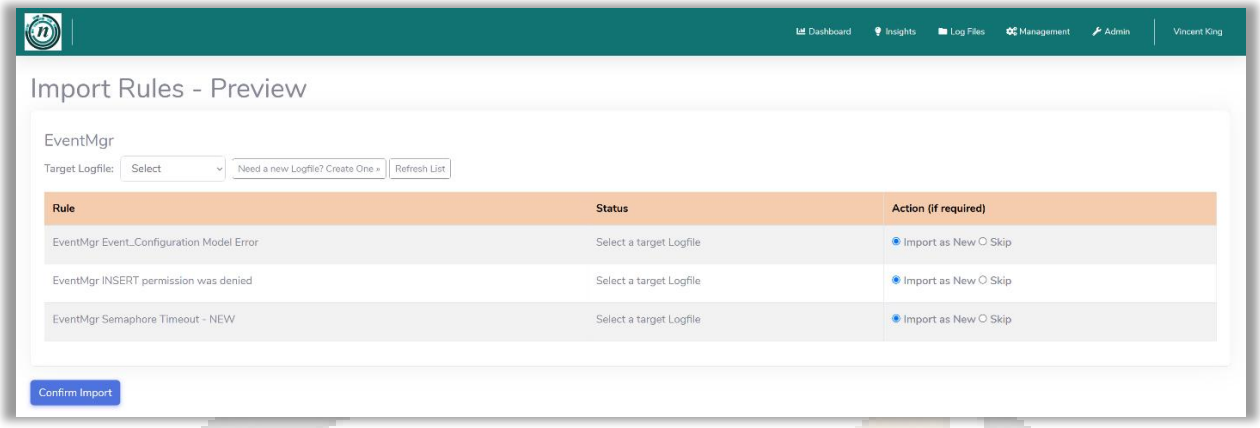


After uploading, the Preview screen groups the imported Rules by their source Logfile. Choose which Logfile on this install each group should attach to, since names or file paths often won't match exactly between installs. If the right Logfile doesn't exist yet, use Need a new Logfile? Create One to add it in a new tab, then Refresh List to pick it up here.

Since no path is pre-selected on that new tab, use the ... button next to File Path to browse for the file instead of typing it.



If a Rule's name already exists on the chosen Logfile, choose whether to Import as New (add it alongside the existing one), Skip it, or Replace Existing (update the existing Rule while keeping its historical error data). Click Confirm Import when ready.



Appendix A: Version 1.2 Development Summary

This appendix recaps everything added, changed, or fixed during the Version 1.2 development cycle, for reference alongside the feature-by-feature sections earlier in this manual.

Security & Authentication

- Windows Authentication now requires an actual password prompt, validated against the real Windows account - previously it silently signed users in without asking.
-
- Added an optional Automatically log in with Windows credentials setting per Windows-authenticated User (Users > Create/Edit User) - off by default, admin-controlled; when enabled, skips the login page on that User's own computer after their first Windows sign-in there.
- Added a license-enforced limit on how many "server connections" (Mapped Drives) an install is allowed to have.
- Rebuilt the admin Encryption/Decryption tool, which was broken (wrong key, missing page, broken forms) - now works correctly and supports encrypting/decrypting for other customer installs.
- Restricted the Encryption tool to a new, dedicated "Support" group, hidden from all normal user-management screens so it can't be granted by mistake.
- Added an "Update Connections License" admin page so that server-connection limit can be changed without a code deployment.

Dashboard Improvements

- Fixed a layout bug where selecting a Logfile would compress and distort the rest of the page.
- Added a Custom Date Range option, in addition to the original fixed presets (24 Hours, 7 Days, Month, 12 Months).
- Added drill-down: double-click a chart bar to see that exact time window's error breakdown by Rule; single- or double-click narrows the Recent Errors list to that same window.
- Added a trend chart (with zoom) showing the time between errors for a selected Rule over time.
- Added two new reference lines to the main chart: Average Errors and Average Time Between Errors, so above/below-normal periods are visible at a glance.
- The Dashboard's auto-refresh interval (previously fixed at 30 seconds) is now admin-adjustable.
- The app version number is now displayed on the Dashboard and License pages.

- Click Total Errors by Logfile to reset the chart and grid data back to initial load.

New: "Insights" Predictive Reporting Page

- A new page showing every Rule's error trend and anomaly status across all Logfiles at once, to surface what needs attention without checking each Logfile individually.
- The sensitivity of anomaly flagging is admin-adjustable in real time, right from the page.
- Automatically shows the same date range currently selected on the Dashboard for a consistent view between the two pages.

New: Export / Import Rules

- Admins can now export selected Rules - including their Elements, Alerts, and Alert settings - to a file, and import that file into another notifi install.
- On import, each Rule can be attached to any Logfile on the destination install, since names or file paths often won't match exactly between installs.
- Per-Rule control when a naming conflict is found: add it as a new Rule anyway, skip it, or replace the existing one while preserving its historical error data.
- A needed Logfile that doesn't exist yet can be created on the fly during import, without losing progress on the import screen.
- Considered a dedicated "Duplicate Rule" button as a separate ask, and determined Export/Import already covers that need without additional work.

Parse Script Performance

- Removed a redundant database check that ran on every single matched error line.
- Log Files now resume reading from where they left off, instead of re-reading the entire file from the start on every run - a meaningful speedup for large or fast-growing log files.
- Database inserts for extracted Rule data are now batched together instead of one at a time.
- Inactive Rules are now filtered out up front instead of being checked against every line.

MySQL Compatibility

- Confirmed and verified the application runs correctly on MySQL as well as SQL Server, with a full parallel MySQL environment set up for ongoing testing.
- Found and fixed two genuine, pre-existing bugs during that testing (an Event Log page error, and the privileged "support" group being visible where it shouldn't be) - neither was caused by MySQL.

Other Admin Tools & Usability

- The Admin Codes settings page now updates its list immediately when the category is changed, instead of requiring an extra click.
- The Add Logfile page, when used from the Import Rules page, can now browse for a file visually instead of requiring the path to be typed by hand.
- The top navigation bar no longer scrolls out of view on longer pages.
- Discussed the feasibility of a full guided install package and of supporting Linux in addition to Windows - both are technically achievable but were scoped as future work, not built yet.

Notable Bug Fixes Along the Way

- Fixed a server error when saving Dashboard edits.

- Tracked down and fixed a file-permission issue that was silently blocking the License and Connections License save features.
- Fixed two database structure mismatches that were causing Delete Rule and Remove Logfile to fail.
- Fixed a bug where a brand-new Rule was silently skipped during import due to a hidden, unintended form value.
-