Monitor Qlik Sense sites

Qlik Sense®
2.1.2

Contents

1 About this document

This guide documents the *Operations Monitor* and *License Monitor*, the apps used to monitor a Qlik Sense site. This document is derived from the online help for Qlik Sense. It is intended for those who want to read parts of the help offline or print pages easily, and does not include any additional information compared with the online help. Please use the online help or the other documents to learn more.

The monitoring apps are accessed from the QMC start page. The **Monitoring apps** link under **GOVERNANCE** in the navigation panel takes you to the **Monitoring apps** stream where you can start the individual apps.

The *Operations Monitor* app provides information about hardware utilization, such as server memory and CPU usage, active users, and reload task activity. It also provides summary and detailed information about errors, warnings, and log activities in the Qlik Sense server environment that can be used for troubleshooting.

The *License Monitor* app tracks license usage, and it facilitates monitoring changes to license allocation.

The monitoring apps provide historical status and trending data. Real-time status is provided by QMC management resources. Actions taken in response to issues revealed by the monitoring apps are also performed in the QMC

You find these documents and much more at help.qlik.com/sense.

2 Monitoring a Qlik Sense site

2.1 Monitoring apps

The Qlik Management Console (QMC) provides apps for monitoring system performance and usage on Qlik Sense server nodes and for monitoring license usage.

The monitoring apps are accessed from the QMC start page. The **Monitoring apps** link under **GOVERNANCE** in the navigation panel takes you to the **Monitoring apps** stream where you can start the individual apps.

The *Operations Monitor* app provides information about hardware utilization, such as server memory and CPU usage, active users, and reload task activity. It also provides summary and detailed information about errors, warnings, and log activities in the Qlik Sense server environment that can be used for troubleshooting.

The *License Monitor* app tracks license usage, and it facilitates monitoring changes to license allocation.

The monitoring apps provide historical status and trending data. Real-time status is provided by QMC management resources. Actions taken in response to issues revealed by the monitoring apps are also performed in the QMC.

2.2 No configuration required

The monitoring apps do not require configuration. They are configured to scan existing server logs on all the nodes in a Qlik Sense server environment and present data in various lists and charts. Data in the operations and license monitors is not live; it is updated when the app is reloaded. Reload frequency can be changed by editing the triggers for the task.

2.3 Customizing the apps

While no configuration is required, it is nevertheless possible to extend the monitoring apps with visualizations users find useful in their particular environments. Both the *Operations Monitor* and the *License Monitor* provide libraries with the dimensions and measures they use. Those dimensions and measures can be used to create customized visualizations on separate sheets that the user can add to the apps.

The libraries also include extra visualizations that are not used on any of the apps' sheets but which the user may find useful in a particular environment.

See: *Operations Monitor library (page 18)*

See: *License Monitor library (page 29)*

2.4 Multi-node environments

In multi-node environments, the apps can be reloaded on any node.

Do the following:

1. Share the Qlik Sense folder on the central node.
   The default location is *C:\ProgramData\Qlik\Sense*.
2. Update the data connections *ServerLogFolder* and *ArchivedLogFolder* by replacing *C:\ProgramData\Qlik\Sense* with the path to the shared folder.
3. Reload the apps on the rim nodes.

Because of the way multi-node environments are synchronized and the way logs are archived, the results of reloads may not be completely current. Reloads include all logs from the Archived Logs folder on the central node and the active .txt log files stored in the *Sense\Log* folder on the central node.

2.5 Starting the monitoring apps from the QMC

The apps for operations and license monitoring are started by going to the QMC**start** page. The monitoring apps are accessed from the **Monitoring apps** link under GOVERNANCE in the navigation panel

Do the following:

1. Start the Qlik Management Console.
2. Allocate user access to users who will use QMC apps or allocate login access to groups whose users can use apps with login passes.
3. Click the **Monitoring apps** link under GOVERNANCE in the navigation panel.
   This takes you to the **Monitoring apps** stream where you can start the individual apps.

*The first time the monitoring apps are started, they may not contain data to display because they have not yet been reloaded. In the case of the License Monitor, it has no data until at least one license token has been allocated or an access denial has taken place, so it might display no data even if it has been reloaded. To get fresh data for the apps before their next scheduled reload, return to the Apps overview in the QMC and click **More actions > Reload now**.*

3 Operations Monitor

The *Operations Monitor* loads service logs to populate charts covering performance history of hardware utilization, active users, app sessions, results of reload tasks, and errors and warnings. It also tracks changes made in the QMC that affect the *Operations Monitor*.

With the *Operations Monitor*, you can track system performance and investigate activity that might adversely affect it. For example, by analyzing reload tasks and sessions, you can find bottlenecks that might be alleviated by rescheduling reloads or redistributing sessions. Or you can use the **QMC Change Log** sheet to review changes that might explain changes in system performance.

3.1 Operations Monitor sheets

The *Operations Monitor* consists of eight sheets that display Qlik Sense performance on the current node.

24-hour Summary	Displays hardware utilization, active users, active apps, and reload tasks over the last twenty-four hours.
Performance	Allows the user to select a time period over which to display hardware utilization, concurrent users, and concurrent apps.
Task Overview	Provides a statistical overview of the success, duration, and failure of reload tasks.
Task Details	Provides details about the success and failure of individual app reloads, including execution details about duration and start and end times.
Session Overview	Provides summary information about apps, app sessions, and app users over selected periods to show which users use which apps when.
Session Details	Provides details about individual user and app sessions, including number, average duration, days since last session, start and end times, reasons for ending sessions, and the type of client on which the app was run.
QMC Change Log	Displays changes made in the QMC that affect a range of factors from system performance to user access, including changes by QMC resource type, by specific QMC resources, by users who made changes, or by a type of action performed in the QMC.
Log Details	Provides details about reloads of the *Operations Monitor*, including the time of reloads, results, error messages and warnings, and log entries.

The *Operations Monitor* provides charts for:

- Server CPU
- Server RAM usage
- number of active users

- reload tasks statistics and execution details
- errors and warnings

It also reports:

- average and maximum RAM usage in the period
- average and maximum CPU usage in the period
- average and maximum number of active users in the period
- average and maximum number of active sessions in the period
- number of errors and warnings
- warnings and error entries
- number of reloads and their average and maximum duration
- number of reload failures
- reload task execution details

Data in the Operations Monitor is updated when the app is reloaded. Data is not live.

3.2 24-Hour Summary

The *24-hour Summary* provides an overview of system performance during the 24 hours prior to the latest reload. It displays hardware utilization, active users, active documents, task reloads, failures and average duration, user sessions, and errors and warnings over the last twenty-four hours on the current node.

Data comes from all nodes in a multi-node environment. The average and maximum usage is for all nodes combined.

Six KPI visualizations highlight important performance indicators, and each of the KPI visualizations link to sheets in the *Operations Monitor* that provide details about the indicator. The following list shows the KPI visualizations included, and the linked sheets for each KPI is shown in parentheses:

- Max CPU (Performance)
- Max RAM (Performance)
- Reloads and Failures (Task Overview)
- Avg Reload Duration and Max duration (Task Overview)
- Max Concurrent Users and Max Concurrent Apps (Session Overview)
- Errors and Warnings (Log Details)

Overview table

In addition, the *Overview* table provides columns with data for the previous 7-day and 28-day periods to compare to the column with the 24-hour values.

During the first 7 days, the 28-day average will probably show a higher daily average than the 7-day because it calculates how many days have had activity whereas the 7-day average always divides by seven, regardless the number of days that actually had activity during that 7-day period.

The Overview table rows show:

Max CPU	Maximum CPU load on the QES process given as a percentage.
Max RAM	Maximum virtual memory committed by the QES process, given in Gigabytes.
Max Concurrent Users	Maximum number of concurrently active users during the periods.
Max Concurrent Apps	Maximum number of apps running concurrently during the periods.
User Sessions	The total number of user sessions started during the periods.
Reloads	Count of reload tasks started during the periods.
Reload Failures	Count of reload tasks that failed to complete during the periods, either because they failed or were aborted.
Avg Reload Duration	The average length of time reload tasks took to complete during the periods.
Errors & Warnings	The total number of errors and warnings during the periods.

Last 24 Hours of Activity table

The Last 24 Hours table shows metrics by the hour for the last 24 hours:

- Maximum CPU
- Maximum RAM (in GB)
- Percent of RAM committed
- Concurrent apps
- Concurrent users
- Reloads
- Errors and warnings

3.3 Performance

The *Performance* sheet displays the history of hardware utilization, active users, and active documents on the current node over a period selected by the user. In a multi-node environment, data comes from all nodes, unless specific nodes have been selected. The average and maximum usage is for all nodes combined or all selected nodes. The user can select on months, weeks, dates, and days of the week. Selections can also be made by hour and by ten-minute time period.

The performance charts and summary table can highlight periods of peak CPU and RAM usage and help identify concurrent events that might be contributing to the high usage. They can also help diagnose trends for concurrent users and apps that could contribute to periods of high activity that cause problems reflected in RAM or CPU usage.

Performance measures

The sheet provides line charts for:

Chart name	Measure	Measure definition
Qlik Sense Server **CPU**	Average CPU	Averages the CPU load on the Qlik Sense Engine Service (QES) process by hour and is given as a percentage.
	Maximum CPU	Maximum value in each hour of CPU load on the QES process and is given as a percentage. Threshold line at 90% provides visual cue to times when CPU usage approaches maximum usage.
Qlik SenseServer **RAM**	Average RAM	Average virtual memory committed by the Qlik Sense Engine Service process, given in Gigabytes.
	Maximum RAM	Maximum virtual memory committed by the QES process, given in Gigabytes. The Max Free line near the top of the chart shows the maximum amount of RAM that can be used by Qlik Sense.
Concurrent Users & Apps	Totals	The number of active users and active apps in the QES at the given point in time

The *Performance Summary* pivot table at the bottom provides additional average and maximum values for the granular time period selected. The summary can be used to illuminate issues observed in the line charts. For example, are there hours during each day that exhibit high activity or load?

Date	Dates selected are super headings for the table's columnar data headings.
Measures	Measures are the subheadings (with calculated values), such as Max CPU, Max RAM, and Concurrent Users.
Hour, Minute	The table rows are hourly data for the dates selected. Hourly rows can be expanded to display data by the minute.
Max CPU	The maximum CPU load for the selected period given as a percentage.
Max RAM (GB)	The average RAM load for the selected period in Gigabytes.

% RAM Committed	The percentage of available RAM that is committed to Qlik Sense and other processes.
Concurrent Apps	The number of active app sessions in the Qlik Sense Engine Service at the given point in time.
Concurrent Users	The number of active users at the given point in time.
Reloads	The number of reload tasks at the given point in time.
Errors & Warnings	The number of errors and warnings at the given point in time.

3.4 Task Overview

The *Task Overview* sheet provides a summary view of reload task activity. Three KPI visualizations highlight reload totals, with failures, reloads per day and per hour, and average duration of the reloads, with the maximum duration. Double-clicking on any of the KPI visualizations opens the *Task Details* sheet.

The *Reload Count* horizontal stacked bar chart displays the number of successful and failed reload tasks, during the selected period, for the *License Monitor*, *Operations Monitor*, and all other apps. The stacked bars make it easy to identify reload tasks that experience a high failure rate.

Reloads by Hour also charts the number of reload tasks (successful, failed, and aborted) by hour of the days during the selected time period. The chart can be used to identify peak reload times as well as periods when the number of reloads is low and when perhaps more reloads could be executed.

A third chart, *Reload Count and Duration Trend*, displays reload totals and the average amount of time taken by reload tasks during the selected period. It can be used to identify reloads that are taking longer than expected or are increasing over time. Or are there some reloads that take longer than the average time to complete.

When a user reloads an unpublished app in the client (hub), this reload is not listed under the general "task reloads" statistics and information. It is logged as a Reload App entry. These client app reloads can be found in the Log Details sheet of the Operations Monitor by searching for "App Reload".

In a multi-node environment, the data in the charts represents all nodes combined, unless specific nodes have been selected.

3.5 Task Details

The *Task Details* sheet contains two tables that enable users to drill into details about apps and their reload tasks. The filter pane allows users to specify periods by month, week, date, day of the week, by the hour, and by reload duration.

In addition to time periods, reload tasks can be selected based on:

- Hostname of the system on which the reload tasks are run.
- Task name to isolate individual tasks for analysis.
- Reload status to analyze tasks according to results of their reloads: FinishedFail, FinishedSuccess, and Aborted.
- App name to analyze the reload results of individual apps.

When a task is executed in the QMC, the reload is logged and displayed in the *Operations Monitor* statistics. When an unpublished app in the client (Hub) is reloaded, however, the reload task is not included in the reload statistics. Client app reload s can be found in the Log Details sheet by searching for “App Reload.”

In a multi-node environment, the data in the charts represents all nodes combined, unless specific nodes have been selected.

Reload Summary Statistics

The *Reload Summary Statistics* table can help identify tasks that have a high failure rate or take a long time to complete. You can also use it to identify tasks that have not been executed for a long time.

Task Name	The name of the reload task
App	The name of the app for which the task reloads data
Reloads	Count of reload start times
Reload Failures	The number of reloads that terminated with FinishedFail or Aborted
Failure Rate	The percentage of reload attempts ending in failure or abort
Avg Reload Duration	The average length of time reloads took to complete, either successfully or failing
Max Duration	The longest duration of a reload task
Last Reload	The time the last reload task started

Reload Details

The *Reload Details* table lists reload task status and details such as task name and duration. When tasks fail, you can examine details to see how long it took to fail and which other tasks were executing when it failed.

Task Name	The name of the reload task
App	The name of the app for which the task reloads data
Hostname	The name of the node to which the task execution details apply.

Reload Status	The result of the execution of the task. The status reported is “Success,” “Failed,.” and “Aborted.” All other status, such as skipped, is shown as “error code 65=finished failed.” *When Reload Status for an app is FinishedFail or Aborted, the Level of the message for the reload task on the Log Details sheet may be INFO instead of ERROR. The number of reload failures reported is, however, the same on both sheets.*
Start Time	The time when the execution of the task started.
End Time	The time when the execution of the task stopped.
Duration	The time (in seconds) for the execution of the task to be completed. Blank when the task terminates due to error or due to timing of the system monitor reload.
Message	The reason for the reload task failure. When the reload finishes successfully, the message can indicate the nature of the reload (for example, “Changing task state from Started to FinishedSuccess”).

3.6 Session Overview

The *Session Overview* sheet provides summary and detailed information (apps, app sessions, and their users over selected periods) to show which users use which apps when.

Four KPI visualizations highlight key data about users, apps, and sessions.

- Max Concurrent Users and Max Concurrent Apps
- Avg Session Duration and Avg Selections
- Users per Day and Users per Hour
- Apps Accessed per Day and Apps per Hour

Double-clicking any of the KPI visualizations opens the *Session Details* sheet.

In a multi-node environment, the data in the charts represents all nodes combined, unless specific nodes have been selected.

Bar Charts

Top 10 Apps	Displays the number of sessions each of the ten most frequently used apps has run during a selected time period.
Top 10 Users	Displays the number of sessions each of the ten most active users has run during a selected time period. When users have run multiple apps, each app’s usage total is indicated in the stacked bars.

Sessions by Hour	Displays the session activity by hour. The purpose of this chart is to show session activity across time. For example, when a month is selected, Sessions by Hour displays the total session activity by hour during that month. It is not the average session activity by hour.
User and App Count Trend	Displays the total number of users and apps used over the selected period.

3.7 Session Details

The *Session Details* sheet provides detailed information (apps, app sessions, and their users over selected periods) to show which users use which apps when. The user can select on months, weeks, dates, days of the week, hours of the day, and length of sessions.

In a multi-node environment, the data in the charts represents all nodes combined, unless specific nodes have been selected.

Tables

App Session Summary

Displays session activity by apps. The *App Session Summary* can be used to identify apps that have high session counts but low user counts and apps that have not been used recently.

App	Name of an app that has been used in at least one session.
Users	Number of users who have started sessions with the app.
Sessions	Number of sessions started with the app.
Days Since Last Session	Number of days since the last session with the app
Average Session Duration	Average length of time for sessions with the app

User Session Summary

Displays session activity by users. The *User Session Summary* can be used to identify users who are accessing a large number of apps. The table can also identify users who open apps for only very short sessions.

User	Directory from which the user started sessions.
Apps	Number of apps started by the user.
Sessions	Number of sessions started by the user.
Days Since Last Session	Number of days since the user last started a session.
Average Session Duration	Average duration for sessions run by the user.

Session Details

Displays details contained in *App Session Summary* and *User Session Summary* tables on a per session basis. This can help isolate apps or users that consistently show long duration or a high number of selections. Such session statistics can be used to evaluate app content and design.

Session Start	Date and time at which a session started.
Session End	Date and time at which the session ended.
User ID	ID of the user who started the session.
App	Name of the app run in the session.
Hostname	The name of the node to which the session details apply.
Duration	Length of time the session lasted.

3.8 QMCChange Log

The QMC*Change Log* sheet displays changes made in the QMC. It enables administrators to analyze operations that might have a range of effects, from system performance to user access. You can explore changes by QMC resource type, by specific QMC resources, by users who made changes, or by a type of action performed in the QMC.

QMC change summary

The table at the top of the QMC*Change Log* sheet is titled *Change Summary*. It summarizes changes by resource type, shows the latest change, and who it was made by.

QMCResource Type	Nine resource types are listed: 1. App 2. Content 3. Extension 4. File 5. Roles 6. Stream 7. System 8. Upgrading 9. User
Changes	The number of changes made to the resource type.
Latest Change	The most recent change to the resource type.
Changed by	The user who made the most recent change.

Users making changes

The *Change Users* table on the right side of the sheet lists the QMC users who have made changes. It includes the total number of changes made and the date of the latest change. It can be used to track users making a large number of changes.

UserID	The ID of the QMC user who made changes.
Changes	The number of changes made by the user.
Latest Change	The date of the latest change made by the user.

Change details

Details of changes made in the QMC are contained in a table named QMC*Change Log*. The *Change Log* can be particularly useful for tracking changes to Security Rules. It can also help identify apps that have been added, published or exported inappropriately.

Log Timestamp	The date and time the log file containing the change action was created.
QMCResource Type	The type of resource that made the change.
QMCResource	The specific resource that made the change.
QMCAction	The type of action the resource made, such as Add, Delete, or Update.
UserId	The ID of the user who made changes.
Change Detail	The details of the change. For example, if a system rule has been added, the detail includes the category of the rule, such as security, the name of the rule, the rule, actions permitted by the rule, the context of the rule and version.

3.9 Log Details

The *Log Details* sheet displays the current version of the Operations Monitor and the copyright notice. It also provides status of the most recent reload of the *Operations Monitor*, including errors and messages. The sheet contains three tables that list servers monitored and display the errors, warnings, and log details during the selected period :

Qlik SenseServers	Lists the servers from which log details have been collected. It can highlight servers that are generating high numbers of log entries.
Errors & Warnings	Provides a consolidated list of errors and warnings by Qlik services. When a specific Service Message is selected, the *Log Details* table displays log entries associated with that service message. This table can highlight services (for example, Proxy or Engine) that are producing numerous errors.

Log Details	Lists log entries by host name and log level. The Timestamp field shows the exact date and time the message was logged. The *Log Details* table provides details about specific events and time periods. *When Task Status for an app is reported as FinishedFail or Aborted on the Task Details sheet, the Level of the message for the reload task on the Log Details sheet may be INFO instead of ERROR. The number of task failures reported is, however, the same on both sheets.*

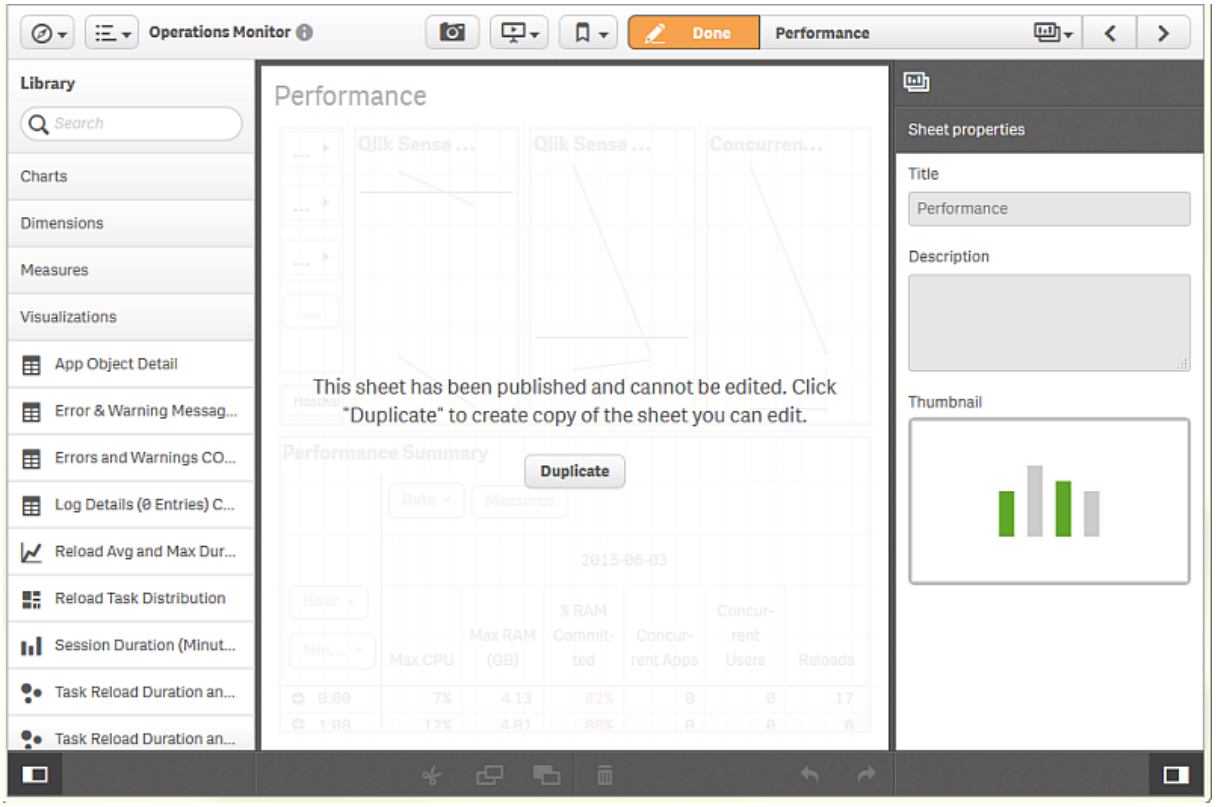
The *Operations Monitor* creates a log for that contains the status of each of its reloads. The log file, named "Operations_Monitor_Reload_Stats.txt," is located in the Log folder: *%ProgramData%\Qlik\Sense\Log*.

3.10 Operations Monitor library

The *Operations Monitor* includes a library that provides access to the dimensions and measures used for its visualizations. You can use these dimensions and measures to create additional visualizations for your particular environment.

The library also contains extra visualizations that are not used on the *Operations Monitor* sheets. These visualizations can be used on customized sheets that you create for your particular environment. You can use the library visualizations as is or customize them for your environment. The visualizations in the library are distinct from the standard visualizations used on the *Operations Monitor* sheets, which cannot be altered.

To access the library, open one of the *Operations Monitor* sheets and click in the toolbar. In the illustration below, the *Performance History* sheet is open in edit mode. You cannot edit the *Performance History* sheet, but you can make a copy of it and then customize it by adding new visualizations or altering or removing the existing visualizations.



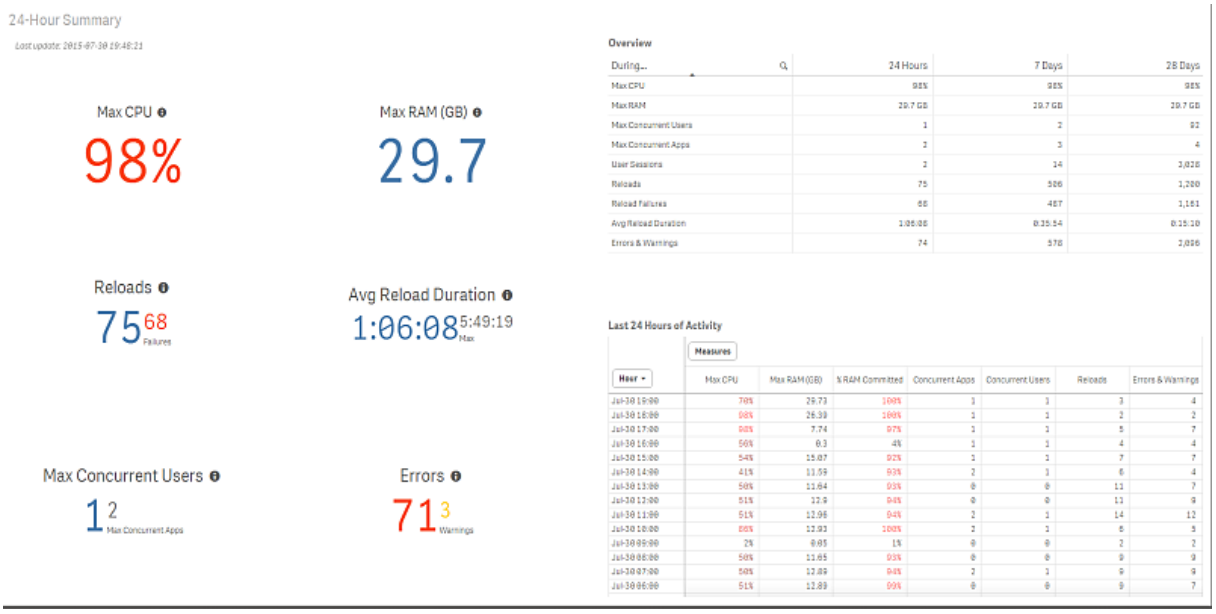
The individual dimensions, measures and visualizations have tool tips that describe their dimension type, such as single or drill-down, measure expressions, type of visualization chart, fields, and tags.

3.11 Analyzing operations data

The *Operations Monitor* gathers a large amount of data about Qlik Sense systems and operations and organizes the data in charts and tables that enable the natural analytics typical of Qlik Sense apps.The scenarios outlined in this section of the documentation offer approaches to analyzing operations data to diagnose problems and better understand how a Qlik Sense environment is performing.

Diagnosing reload task failures

The following scenario explores approaches to analyzing operations data that shows a high number of reload task failures in the last 24 hours. This condition would be identified by checking the *Reloads* KPI on the *24-Hour Summary* sheet. The *Reloads* KPI indicates how many reload tasks have been started and how many have failed.



If the KPI shows 75 reload task and 68 failures, that is high failure rate, and in most cases, you would want to find out why it is so high. The steps below offer one analytical path that might lead to a diagnosis.

Do the following:

1. Double-click on the the *Reloads* KPI to open the *Task Overview* sheet in the *Operations Monitor* app.
2. Review the *Reloads by Hour* chart to see if the failure rate is high over a particular time period during the last 24 hours.
   If you find that a large percentage of the failures occurred during a limited period of the day, you might be able to identify an isolated event. If the failures are spread out over the 24-hour period, you should compare the recent period to other periods.
3. Open the *Task Details* sheet and select a time period to examine.
4. If the current month shows a significant number of failures, select the month to see its specific data.
5. Select specific dates in the month to isolate the time periods in which a significant number of failures occurs.
6. Switch to the *Log Details* sheet and examine the types of errors in the *Errors & Warnings* table to find out if there is problem that affects multiple tasks.
   It is possible that there is an underlying problem with one of the services, such as the Engine or Scheduler, that affects a number of the reload tasks.
7. Switch back to the *Task Details* sheet and select individual tasks in the *Reload Summary Statistics* table, particularly tasks that have a high failure rate.
   When a task is selected, the *Reload Details* table displays the individual reload attempts for that task.
8. Examine reload attempts with **`FinishedFail`** status and their reasons for failure.

The *Operations Monitor* might not indicate directly what the problem is, but by understanding the types of errors or the reload tasks that are failing, you can investigate causes. For example, a load script may have been changed and introduced an error that causes it to fail.

Diagnosing slow system response

The following scenario explores approaches to analyzing slow system response for apps and reload tasks. This condition might be identified on the *24-Hour Summary* or *Performance* sheets if there is a very high average server CPU usage or on the *Task Details* sheet if average load duration time goes up significantly. Neither of these indicators are necessarily definitive. The changes shown might be normal variations, such as a series of reload tasks that normally run longer. Another indication might be that users complain that their system response time is unusually slow. The *Operations Monitor* can then be used to diagnose the problem.

When slow system response appears to be a problem, the steps below offer one analytical path that might lead to a diagnosis.

Do the following:

1. Switch to the *24-Hour Summary* sheet in the *Operations Monitor* app.
2. Review the *Last 24 Hours of Activity* pivot table to see if there is high average usage for an extended time during the 24-hour period. High CPU usage could indicate a hardware problem, or it could be a symptom of problems or conditions elsewhere on the server, such as reload failures, system errors, or increased usage.
3. Review the *Last 24 Hours of Activity* pivot table to see if memory usage is unusually high. Memory usage of 90% or above should be considered high. Average RAM and maximum RAM usage are usually quite similar over a 24-hour period.
4. If memory usage is high during some part of the 24-hour period, check the *Overview* table to see if average RAM is higher for the 24-hour period compared to the 7-day and 28-day periods. Higher current RAM usage could indicate that something unusual is occurring and could be causing the slow system problems.
5. Check *Concurrent Users & Apps* chart on the *Performance* sheet to see the number of users is high during the period when response has been slow.
6. If the number of users is high, switch to the *Session Overview* sheet to see if there is a correlation between the number of user sessions and the period of slow response.
7. Select the time period in which the slowdown occurs and review the *Sessions by Hour* chart and *Avg Session Duration* KPI to see if there is a large number of sessions or sessions that last a long time. Sessions with long duration times could be running apps that are very active (many selections), perhaps a meeting presentation or deep analysis. It is also possible that a session was left open without ongoing activity in the app, or an app got stuck or did not close properly. Usually a "frozen" session does not consume a lot of resources. Long session duration could be caused by users accessing apps during long meetings or doing extended analysis.
8. Switch to the *Session Details* sheet and review the *App Session Summary* table to see if there are specific apps running in a number of sessions. It is possible that one user has an app open in multiple browsers but is only actively using it in one place.
9. Switch to the *Task Details* sheet and select the date or dates for which slow system response is occurring to see if there is an extraordinarily large number of reloads being performed during the period or if there is a large number of reload failures occurring.
10. Switch to the *Task Overview* sheet and check the *Avg Reload Duration* KPI to see if the average duration is high during the slow response period.

11. Switch back to the *Task Details* and check the *Reload Summary Statistics* table to see how many reload tasks have high average durations and how many reload attempts those tasks have made. If there are one or two apps reloading data frequently and whose reloads take a long time, you might have to move those app reloads to another server or reduce the number of reload tasks to free up CPU time for other apps that are negatively affected.
12. Check the Reload Failures column in the *Reload Summary Statistics* table to see if the apps that have long average reload durations are failing frequently. Reload tasks that are failing frequently could be experiencing connection problems with their data source and are left in a wait state for long periods, or they are being rerun immediately after failures. Problems with the reload tasks might have to be fixed to reduce load that is slowing system performance. The most recent data load execution logs are available in *Qlik\Sense\Log\Script* and are listed in the app GUID.
13. Check the *Reload Details* table to see if tasks that fail have long durations or if they take a long time to run successfully. If the reload tasks run a long time and then fail, the problems with the task will have to be fixed to improve system performance. If the tasks take a long time to run successfully, they may have to be moved to a system with more resources to prevent them from blocking other apps.
14. Switch to the *Log Details* sheet to see the types of errors and warnings generated during the slow response time. If the errors are concentrated in one or two services, or perhaps one or two types of errors recur many times, then you can see whether one of the services has to be fixed or perhaps a particular type of error will point to a problem with a reload task that can addressed.

There are multiple issues that could cause poor system response time, and the preceding review of the *Operations Monitor* objects could reveal one or more problems that are affecting your systems.

4 License Monitor

The *License Monitor* loads service logs to populate charts and tables covering token allocation, usage of login and user passes, and errors and warnings. For the location and naming convention of the log files,

4.1 License Monitor sheets

The License Monitor consists of seven sheets that display Qlik Sense performance on the current node.

7-Day Summary	Displays summary data about login and user access sessions over the last 7 and 28 days, changes in the allocation of license tokens over the last 7 days, and a license usage time line.
Login Access History	Allows the user to select a time period over which to display login pass utilization, login access users, and denials of login access.
User Access History	Allows the user to select a time period over which to display user access pass sessions, the number of users starting sessions, and the individual users starting sessions.
Allocation History	Displays the latest changes and changes over selected times to the allocation of license tokens to login and user access passes.
Usage by App	Allows the user to select a time period over which to display the apps for which access passes are being used and the number of tokens consumed by each app.
API Calls	Provides a summary view of the Engine activity based on key API calls.
Log Details	Lists servers in the cluster and provides details about license usage entered in server's logs.

Data in the License Monitor is updated when the app is reloaded. Data is not live.

4.2 7-Day Summary

The *7-Day Summary* sheet provides an overview of license changes and user access in the last 7 days and the last 28 days. Charts and tables contain information about the login and user access passes and user-specific access history.

Data comes from all nodes in a multi-node environment.

KPIs

There are four KPIs contain data for the most recent 7-day period. Double-clicking on the KPIs opens the related *License Monitor* sheet. The KPIs are:

Users Accessing Apps	The total number of login access users who have used apps over the last 7 days. Double-click to see the *Login Access History* sheet.
Login Access Passes	The total number of login passes used and the daily average number of login passes used over the last 7 days. Double-click to see the *Login Access History* sheet.
Allocation Changes	The number of changes made to login and user access passes over the last 7 days. Double-click to see the *Allocation History* sheet.
User Access Sessions	The total number of user access passes used and the daily average number of user access passes used over the last 7 days. Double-click to see the *User Access History* sheet.

Tables

Overview

During the first 7 days, the 28-day average will probably show a higher daily average than the 7-day because it calculates how many days have had activity whereas the 7-day average always divides by seven, regardless the number of days that actually had activity during that 7-day period.

Total Users	The total number of users who have used either a login or an access pass over the last 7 days and the last 28 days.
Avg Daily Login Access Passes	The average number of login passes used on a daily basis over the last 7 days and the last 28 days.
Max Daily Login Access Passes	The highest number of login passes used on a daily basis over the last 7 days and the last 28 days.
Total Login Passes	The total number of login passes used over the last 7 days and the last 28 days.
User Access Sessions	The number of sessions started by users with a user access pass over the last 7 days and the last 28 days.
Access Denials	The number of times access was denied over the last 7 days and the last 28 days. Denials can be for login or user access. A user is denied login access when all the login passes for the group to which she belongs have been used. User access is denied when a user pass has not been allocated to the user.
Allocation Changes	The number of changes over the last 7 days and the last 28 days in the way tokens are allocated.

Allocation Changes in Last 7 Days

This table lists the date changes were made, the type of change, such as adding more passes, the user and group affected by the change, and the user who made the change. When login access passes are allocated, they are allocated in groups of ten. That is because ten login access passes are granted for one token. Login passes are allocated to groups, and then users in that group can access those passes.

A single user access pass requires one token. User access passes are allocated to specific users.

The *Allocation Changes in Last 7 Days* table can be used to detect unexpected changes made to token allocation.

Charts

License Usage Timeline

This stacked bar chart shows the number of login and user access passes used on a monthly, weekly, or daily basis. For example, selecting one month will change the chart to display passes used by week.

4.3 Login Access History

The *Login Access History* sheet shows the totals of login pass usage and the usage by individual users. The usage values are the passes that have been used, not the number of passes allocated. The period of history shown can be selected by month, week, by a specific date, by days of the week, or a specific date and time. Selections can also be made based on users, login access rules, and number of login passes used.

Login access pass usage

The *Used Login Access Passes* stacked bar chart displays, by default, a month-by-month breakdown of login access passes used by groups. When different log dates and times are selected, the chart displays login access usage by group for those selected times. Because the bar chart is stacked, it is easy to see how usage across different groups is changing.

Login access pass users

The *Login Access Passes per User* table is a sortable list of users, who have used login access passes in total and over the last 28 days. It displays the number of login passes each user has used and the last time the user accessed the system.

Users who use more than ten login passes in a 28-day period might be candidates for getting user access passes. User access passes allow the assigned user to login as many times as necessary during a 28-day period, but they require the allocation of a whole license token. Login access passes, on the other hand, are allocated to groups on a basis of ten passes per license token.

The table also enables you to find inactive users who have not used Qlik Sense recently.

Access denied

The *Users Denied Access* pivot table shows users who were denied login access, when they were denied, and how many times they were denied on a particular date. Examining access denials can help administrators understand whether recent token allocation changes have caused or resolved denials.

4.4 User Access History

The *User Access History* sheet shows the number of non-concurrent sessions started by users with user access passes and the number of users who started non-concurrent sessions. The period of history shown can be selected by month, by week, by a specific date, or by days of the week. Individual users can also be selected, and selections can be made by number of sessions. The *User Access Sessions per User* list consists of the number of sessions started by each user, so you can select a number to see which user or users started that number of sessions. For example, if you want to see who the most active users are, select the highest number of user sessions.

The *User Access Sessions* chart shows the number of sessions started and the number of users who started them during the selected period of time. It is useful to track the ratio of unique users to user passes over time.

The *User Access Sessions per User* table lists individual users who have started sessions during the selected period and the total number of sessions they started.

The table also lists the number of sessions each user started in the last 28 days and the date of the last session. Knowing how often a user has started sessions in the last 28 days allows you to determine whether or not a user is making full use of his or her user pass. Users who have not started at least ten sessions in the last 28 days might be able to use login access passes instead of user access passes because login passes are allocated to groups on a basis of ten passes per license token. User access passes are allocated to individual users on a basis of one pass per token.

The session numbers here are not exactly the same as the session numbers by user in the *Operations Monitor*. The user access sessions shown in the *Session Details* do not count concurrent sessions. If a user has more than one app open concurrently, only one user pass session is counted.

4.5 Usage by App

The *Usage by App* sheet shows the apps for which access passes are being used. The usage values are the passes that have been used, not the number of passes allocated. The period of history shown can be selected by month, by week, by a specific date, by days of the week, or a specific date. Selections can also be filtered by specific hosts, users, and apps.

Login passes used for apps

The *Login Access Pass by App* table displays the number of login access passes used for each app during the last 28 days, and the total number of tokens used for login access passes used during the selected period. The *Totals* row shows the number of login passes used. Multiple apps can be accessed using a single login access pass, so the total of login passes used can be lower than the sum of passes shown for the apps listed.

For example, if User A and User B login with login access passes and both use the Sales Data app and the Scheduler app, the total login passes used is 2. That is the value shown for *Totals* at the bottom of the table. Because the two users accessed both apps, each app also shows two passes used, and if those values were totaled, the sum would be 4. But that is not the value shown for *Totals*.

The table makes it easy to see if apps are being opened with login passes from multiple login access groups.

User passes used for apps

The *User Access Pass by App* table displays the number of user access passes used for each app and the total number of user access passes used during the selected period. For each app in the table, the number displayed represents the number of user access passes used for the app. Multiple apps can be accessed by a single user, so the total count of *User Access Users* can be lower than the sum of users shown for the apps listed.

For example, if User A and User B login with user access passes and both use the Sales Data app and the Scheduler app, the total user passes used is 2. That is the value shown for *Totals* at the bottom of the table. Each app also shows two passes used, and if those values were totaled, the sum would be 4. But that is not the value shown for *Totals*.

This table is valuable for showing which apps are most heavily accessed with user access passes.

Token consumption per app

The *Token Consumption over Last 28 Days* table shows:

- the number of each type of token (login access and user access) used by each app
- the total tokens used by each app
- the percentage of tokens used by the individual apps

The *Totals* values at the bottom of the table are the total number of passes used. Because multiple apps can be used by individual access passes, the values for *Totals* can be lower than the sum of passes show for the apps listed.

The 28-day values in the tables are for the last 28 days of the period selected. When no *Log Date-Time* selections are made, the 28-days period is prior to today. When *Log Date-Time* selections are made, the 28-day periods are the days prior to the latest day in the period. If, however, some days are excluded from that period, they are also excluded from the values for the 28-day period. In other words, such periods are actually less than 28 days.

For example, if the month of July is selected and July 15-17 are deselected, the 28-day period is July 31 back to July 4. The first three days of July are not included. But the value for that 28-day period does not include data for July 15-17, so in effect, the period is 25 days (28 minus the 3 days for July 15-17).

Analyzing how token usage from login access passes compares to token usage for user access passes can help in allocating operating costs across an organization.

4.6 Allocation History

The *Allocation History* sheet provides status of the access allocated and the history of license allocation changes over the selected time period. Status and history can also be displayed according to the operation performed, a login access rule, and the user who performed an operation.

The *Allocation Changes* KPI shows how many changes have been during the selected period.

The *Allocation Users* pivot table allows you examine user allocation changes by the type of action and the administrator who took the action.

The *Affected Objects* table lists the user group affected by the changes. Each change is listed with the date the change was made.

License Allocation Change History

This table shows how licenses have been allocated to login and user access and the details of the allocations. Here it is easy to see which users have recently been allocated User Access Passes and how often tokens are being reallocated among Login Access Groups.

Timestamp	The date and time of the allocation change.
Modified By	The administrator who performed the allocation operation.
Affected Object	The group to which login access was granted or the user to whom user access was granted.
Change	The specific operation that took place with this change. • Add indicates the group was created and allocated login access passes or a . • Update indicates the group was allocated additional login access passes or the number of access passes allocated was reduced. • Delete indicates the group was deleted and its login access passes removed.
Change Detail	The specific operation that took place with this change. • Add indicates the group was created and allocated login access passes. • Update indicates the group was allocated additional login access passes or the number of access passes allocated was reduced. • Delete indicates the group was deleted and its login access passes removed.

4.7 Log Details

The *Log Details* sheet in the *License Monitor* app displays the current version of the monitor and the copyright notice. It also provides status of the most recent reload of the *License Monitor*, including errors and messages.

The Qlik Sense*Servers* table lists the nodes in a multi-node environment on which licensing activity has taken place in the last 24 hours.

The *License Log Details* table shows events recorded in the license log file.

Timestamp	The date and time of the activity related to licensing.
Hostname	The name of the server on which the activity took place.
User Id	The user who initiated the activity.
Object	The user who is the object of the activity.
Description	A description of the activity, such as license maintenance or user access request.
Command	The type of action that caused the log to be generated.
Message	A detailed description of the activity, including the type of operation (for example, Timeout).

The *License Monitor* creates a log for that contains the status of each of its reloads. The log file, named "License_Monitor_Reload_Stats.txt," is located in the Log folder: *%ProgramData%\Qlik\Sense\Log*.

4.8 API Calls

The *API Calls* sheet in the *License Monitor* app provides a summary view of the Qlik engine activity based on key API calls. It is primarily useful for understanding usage of the Qlik Analytics Platform. KPIs display *Total Calls* and *Calls per Day*. These are high-level aggregations of select API calls. The *Calls per Day* KPI includes a value for calls per hour.

The *Calls by Type* bar chart shows the types of calls made and the number of each type of calls.

The *Timeline* bar chart shows the total number of calls by time period.

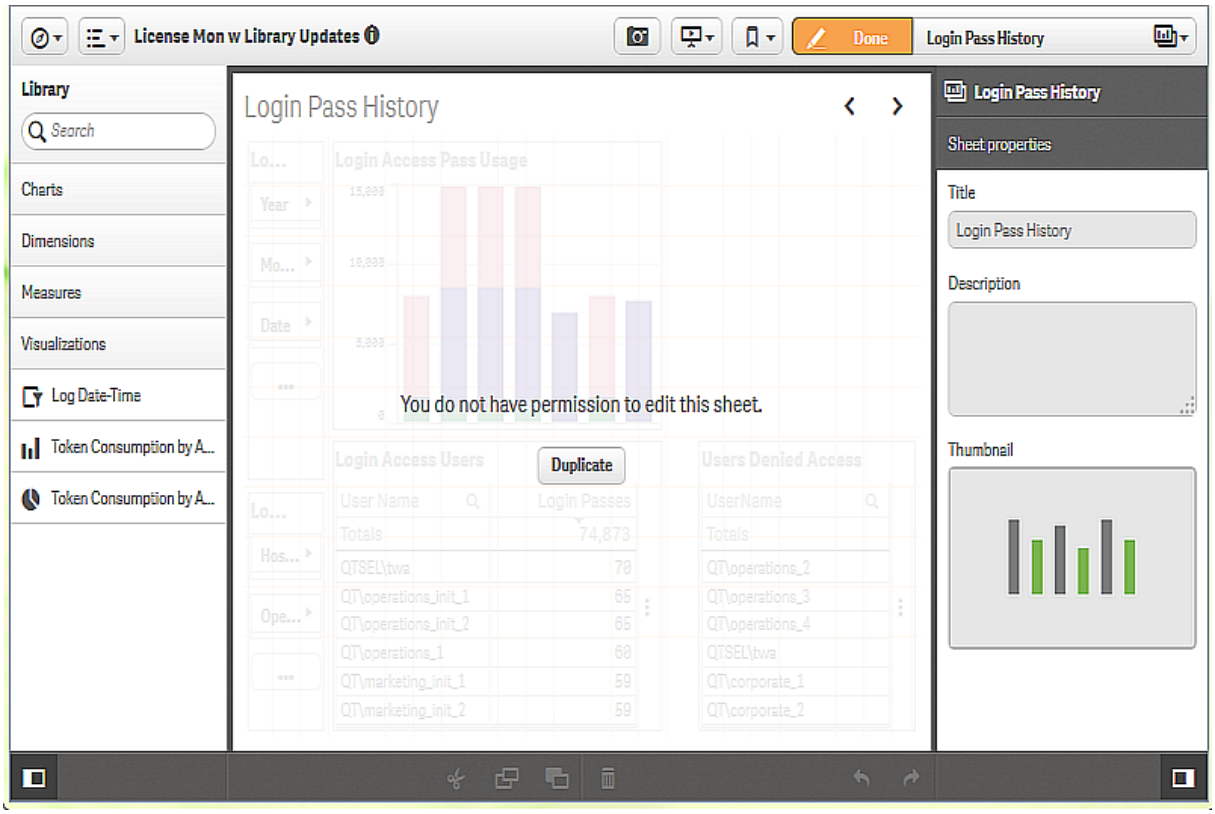
The pivot table breaks down calls by type across month and date.

4.9 License Monitor library

The *License Monitor* includes a library that provides access to the dimensions and measures used for its visualizations. You can use these dimensions and measures to create additional visualizations for your particular environment.

The library also contains extra visualizations that are not used on the *License Monitor* sheets. These visualizations can be used on customized sheets that you create for your particular environment. You can use the library visualizations as is or customize them for your environment. The visualizations in the library are distinct from the standard visualizations used on the *License Monitor* sheets, which cannot be altered.

To access the library, open one of the *License Monitor* sheets and click in the toolbar. In the illustration below, the *Login Pass History* sheet is open in edit mode. You cannot edit the *Login Pass History* sheet, but you can make a copy of it and then customize it by adding new visualizations or altering or removing the existing visualizations.



The individual dimensions, measures and visualizations have tool tips that describe their dimension type, such as single or drill-down, measure expressions, type of visualization chart, fields, and tags.

4.10 Analyzing license data

The *License Monitor* gathers a large amount of data about how Qlik Sense license tokens are allocated and used and organizes the data in charts and tables that enable the natural analytics typical of Qlik Sense apps.The scenarios outlined in this section of the documentation offer approaches to analyzing license data to better understand how access passes are being used. That knowledge can then be used to allocate access passes most efficiently.

Diagnosing login access overutilization

When managing login access passes, it is important to monitor the number of login passes used in the 28-day period to find users who exceed the threshold (10 passes).

Open the *Login Access History* sheet and sort the *Login Access Passes per User* table in descending order to see the high-frequency users at the top of the list. The high-frequency users who use more than 10 login access passes in 28 days can be managed more efficiently by giving them user access passes.

Scenario 1: Appropriate utilization

In this case, the *Login Access Passes per User* table shows that all the login access users have used fewer than 10 sessions in the last 28 days. It requires fewer license tokens to service these users than it would be to allocate user access passes to any of them.

Login Access Passes per User

805 Users

User Id	Last 28 Days	Total	Last Access
finance_409	6	11	2015-07-21
finance_2	5	15	2015-07-20
finance_200	5	11	2015-07-20
finance_202	5	11	2015-07-20
marketing_95	4	11	2015-07-28
marketing_96	4	11	2015-07-28
Total	**5,579**	**11,740**	**2015-07-30**

Scenario 2: Overutilization

In this case, the *Login Access Passes per User* table shows that several users have accessed well over 10 times in the last 28 days. These users are candidates for dedicated user access passes. The number of login passes freed up by reassigning the high-frequency users would be the sum of the passes the users used in the last 28 days.

Login Access Passes per User

805 Users

User Id	Last 28 Days	Total	Last Access
marketing_4	21	48	2015-07-15
marketing_5	21	48	2015-07-15
marketing_6	21	48	2015-07-15
marketing_7	21	48	2015-07-15
marketing_8	21	48	2015-07-15
marketing_9	21	48	2015-07-15
Total	**3,951**	**8,678**	**2015-07-15**

User access underutilization

When managing user access passes, it is important to monitor the number of passes used in the 28-day period to find users who are not making sufficient use of passes allocated to them.

Open the *User Access History* sheet and sort the *User Access Sessions per User* table in ascending order to see the low-frequency users at the top of the list. The low-frequency users can be managed more efficiently by giving them login access passes.

Scenario 1: Appropriate allocation

In this case, the *User Access Sessions per User* table shows that even the lowest frequency user access pass users are accessing Qlik Sense more than 10 times in the last 28 days. None of these users should be converted to login access passes.

User Access Sessions per User

516 Users

User Id	Last 28 Days	Total	Last Session
finance_176	23	45	2015-07-30
marketing_51	23	51	2015-07-29
operations_1	24	56	2015-07-29
marketing_41	27	61	2015-07-30
marketing_31	28	63	2015-07-30
marketing_14	29	65	2015-07-30
Totals	**4,146**	**9,106**	**2015-07-30**

Scenario 2: Undererutilization of user access

In this case, the *User Access Sessions per User* table shows that a number of users listed at the top of the table have accessed Qlik Sense far fewer times than the threshold for a user access pass. These users could be added to login pass groups, and their user access passes could be reallocated to high-frequency users who do not currently have user access passes. Or the license tokens used for the user access passes could be converted to login access passes.

User Access Sessions per User

516 Users

User Id	Last 28 Days	Total	Last Session
marketing_130	1	6	2015-07-28
marketing_131	1	6	2015-07-28
marketing_132	1	6	2015-07-28
marketing_133	1	6	2015-07-28
marketing_134	1	6	2015-07-28
marketing_135	1	6	2015-07-28
Totals	**4,146**	**9,106**	**2015-07-30**

Diagnosing problems with login pass denials

From the *Overview* table on the *7-Day Summary* sheet it is evident that there have been a number of access denials in the past seven days and many more in the past 28 days. Has this affected a number of different users, or are there specific users who are being denied access frequently?

Overview

2015-07-23 to 2015-07-30

Measure	Last 7 Days	Last 28 Days
Total Users	613	881
Avg Daily Login Access Passes	160	202
Max Daily Login Access Passes	329	507
Total Login Passes	1,119	5,638
User Access Sessions	1,080	4,151
Access Denials	150	692
Allocation Changes	0	6

To investigate this issue, review the *Users Denied Access* table on the *Login Access History* sheet. The table lists users who were denied access, when they were last denied, and how many times each user was denied access.

Users Denied Access

40 Users

Date ▾ User Id ▾	Access Denials
2015-07-30	**26**
finance_init_2	4
finance_2	2
finance_20	2
finance_22	2
marketing_2	2
marketing_20	2
marketing_22	2

A solution

Check the *Login Access Passes per User* table on the *Login Access History* sheet to see if any users are exceeding the 28-day access threshold. Those users would be candidates for a dedicated user access pass.

Login Access Passes per User

805 Users

User Id	Last 28 Days	Total	Last Access
finance_409	6	11	2015-07-21
finance_2	5	15	2015-07-20
finance_200	5	11	2015-07-20
finance_202	5	11	2015-07-20
marketing_95	4	11	2015-07-28
marketing_96	4	11	2015-07-28
Total	**5,579**	**11,740**	**2015-07-30**

In this case, however, no login pass users have exceeded the threshold in last 28 days.

Because there are no login pass users who should be given user pass access, resolving the problem of login access denials can probably be handled by allocating more tokens to the specific groups whose users are being denied access. License tokens are allocated in the Qlik Management Console.