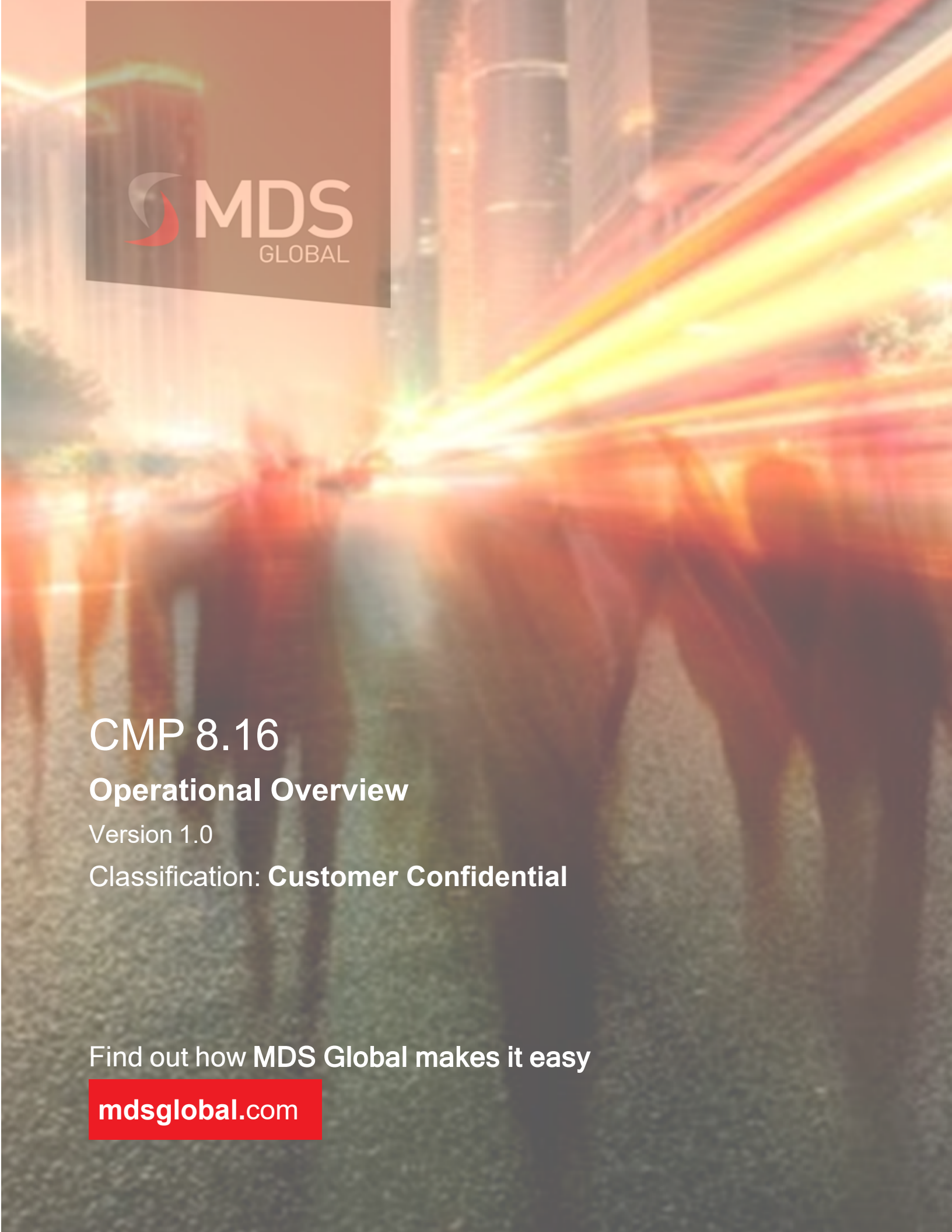


CMP 8.16

Operational Overview

Version 1.0

Classification: **Customer Confidential**

Find out how **MDS Global makes it easy**

mdsglobal.com

Copyright

Confidentiality

Disclaimer

Trademarks

Contact Details

Please visit www.mdsglobal.com for further information on MDS Global products, solutions and services.

ISO 22301 standard is applicable to MDS Global Business Operations.

Table of Contents

Version Control

Version	Issue Date	Author	Comments
Version 1.0	25 July 2024	MDS	CMP 8.16 Release - No changes since the last release.

Terms Used in this Document

For definitions and explanations of the terms, abbreviations and acronyms used in this document, please see the *CMP Glossary* document.

1.0 CMP Operational Architecture

Operationally, processes running in CMP need to be submitted, monitored, and assured. Wherever possible, these operational tasks should be automated.

The CMP operational architecture is responsible for submitting, monitoring, and assuring operational processes.

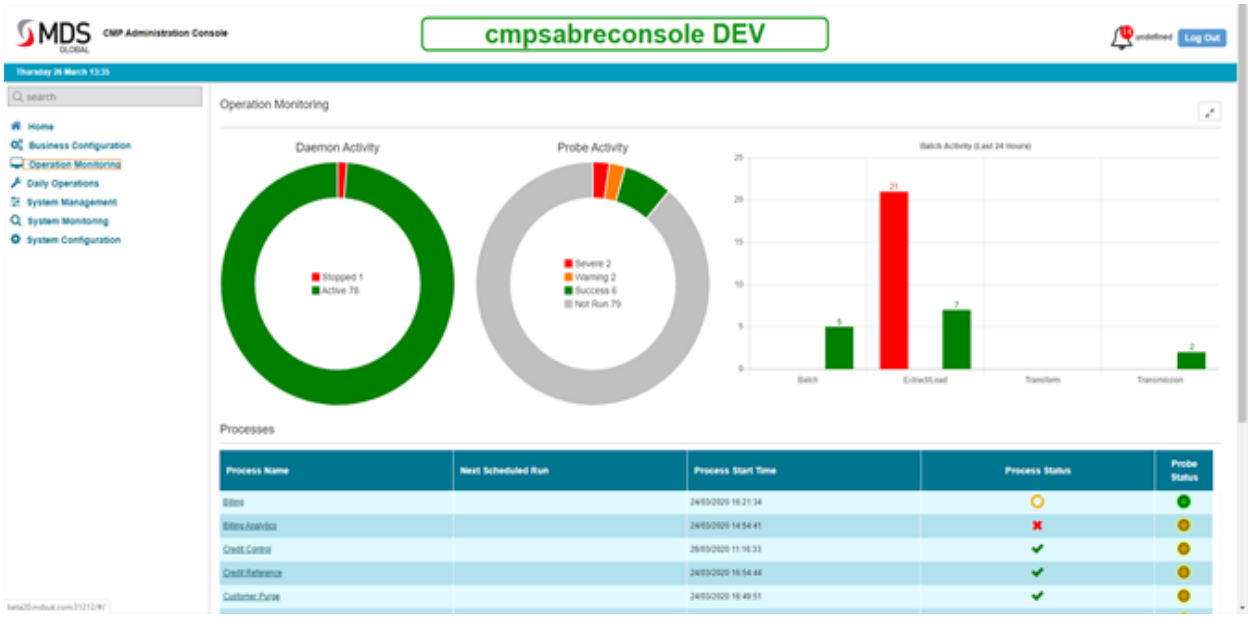
The architecture covers three main areas:

- Operational Architecture
- Probes
- Application Processes

1. 1 Operational Architecture

In the CMP operational architecture, batch jobs are run and monitored in the Administration Console. Alert and auditing facilities are also available.

The Administration Console provides the operational teams with an interactive environment, making it simpler for the operations teams to run, manage, and monitor batch server jobs. The Administration Console can be accessed via the operator's web browser:



1. 1. 1 Probes

The probes feature is a mechanism allowing the execution of predefined queries and the comparison of the query results against pre-configured targets. Probes can be reviewed

and managed via the Administration Console.

1. 1. 2 Audit Logs

The Administration Console Logs facility allows operators to interrogate the persisted log records. These logs are for the entire batch server and also the Administration Console. The filter functionality allows a subset of the logs to be retrieved in order to investigate a specific issue or job.

This document provides a detailed overview of the Administration Console, and lists and describes the CMP batch jobs (process), daemons and probes.

1. 2 Service Management Responsibilities

CMP requires a service management function to operate. This function is typically responsible for the following key tasks:

- Process monitoring
  - Responding to alerts from the monitoring system
  - Periodic manual checks for any unmonitored processes
- Maintaining the batch schedule
  - Managing processes through planned outages, where applicable
- Data purge and archive in line with agreed schedules
- Usage error monitoring
- Payment allocation monitoring
- System backups

This list reflects the tasks required to manage the CMP application and excludes non-application driven processes such as service level agreement (SLA) reporting and monitoring and billing process reviews.

2.0 About Administration Console

The Administration Console provides the following functionality:

- Business Configuration

  Business Configuration allows users to configure market propositions, price plans and tariffs, communications with customers, and business process workflows. Users can access Business Configuration from the Administration Console navigation pane or the tile on the **Home** page.

  For more information on Business Configuration, see the *Online Help* for that module.

- Operation Monitoring

  A dashboard that enables users to monitor the overall status of day-to-day operations including executions status and any abnormal system activity with click-through troubleshooting.

- Daily Operations

  Daily Operations enables users to configure probes and manually execute jobs. It provides comprehensive status information about jobs, daemons, probes and job *interfaces* - all inbound, outbound and internal batch activity.

- System Management

  System Management enables users to fully manage processes and jobs, including scheduling and planned outages.

- System Monitoring

  System Monitoring provides detailed log records of all system and operational processes; enabling rapid troubleshooting.

- System Configuration

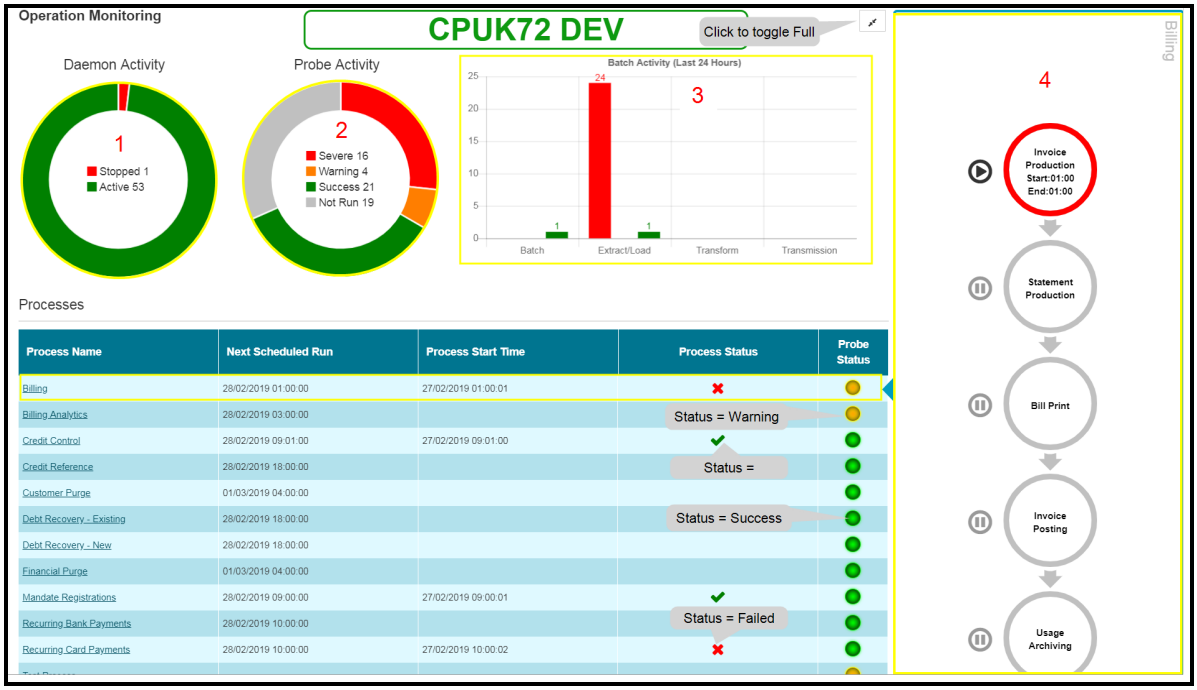
  Users can configure system-wide parameters, application parameters and parameters for all modules installed on the system.

- System Administration

  Enables console users to create users and assign them access to applications and functionality.

3.0 Operation Monitoring

The Operation Monitoring Dashboard monitors the overall situation of day-to-day operations including process execution status and any abnormal system activity with click through troubleshooting. The execution and status of jobs, daemons[1] and probes[2] are monitored and updated in real time. This takes place in the highlighted and numbered areas of the dashboard below as follows:



Operation Monitoring Dashboard

1. Daemon Activity

The current overall execution status of daemons can be:

- Green = active
- Red = stopped.

2. Probe Activity

Probe Activity shows the current overall status for probes:

---

[1]A daemon is a lightweight background process that runs without user intervention and typically performs tasks such as the extract, load, transform, transmission and acknowledgement of data/files.

[2]A quality measure that involves the execution of predefined queries and the comparison of the query results against preconfigured targets. A probe can be configured to send alerts to selected users.

- Red = Severe
- Amber = Warning
- Green = Success
- Grey = Not Run.

3. Batch Activity

Batch Activity monitors the execution and status of batch jobs and their interfaces with external systems. The graph shows the current overall status for the following batch activities:

- Batch - internal jobs that do not interface with external systems but act on CMP tables, for example Credit Management.
- Extract/Load - jobs that involve extracting data from records provided by an external systems and loading the data into CMP, or producing extracts of CMP data for consumption by external systems.
- Transform - jobs that translate data to and from its native format according to a JSON schema.
- Transmission - jobs that send extracts of CMP data to external systems.

The status of batch activities can be:

- Red = Error
- Green = Complete.

4. Process Steps

Clicking any row in the **Process** list opens the **Process Steps** panel for that process. The panel shows the jobs that comprise the process with their current execution status:

- Red = Failed
- Green = Complete
- Grey = Not Run.

Holding the mouse over a job launches a pop-up summary of job details, including the job name, execution, start and end times and job parameters. You can drill down into the **View Execution Details** screen for that job, which provides more details such as an exit code, exit message and logs.

For more information on how to use these features in the dashboard, see the online help for the Administration Console.

4.0 Daily Operations

Manage daily operations in the following screens:

- Jobs:

  Manage and manually execute jobs and view comprehensive execution status information.

- Probes:

  Enables probe configuration and manual execution.

- Daemons

  Provides comprehensive status information of all daemons.

- Interfaces

  Execution and status information on all inbound and outbound batch activity.

4. 1 Batch Audit

The **Batch Audit** screen provides execution and status information on batch activity, including inbound, outbound and internal, such as Statement Production.

The following batch details are available:

- Category

  The *category* of a batch job is the business module or process with which it is associated, for example Billing, Payments, Purge, Credit Management, Usage Processing, Number Management and so on.

- Type

  The *type* of the batch is the particular job within the category with which it is associated, such as Invoice Production, Mandates, Account Purge, Credit Control, Rated Usage, or Managed Numbers.

- Direction

  A batch can have the following directions:

  - Inbound
  - Outbound
  - None. The batch job acts internally on CMP tables only. No external systems are involved.

- Batch Count

  The batch count is the number of times the relevant batch job has been run. You can drill down into the iterations of a job and examine an individual execution, right down to the details of single interface items, which include:

- A sequence number
- A customer reference
- A transaction description
- Errors (if applicable)

- Last Stage Date/Time

  The date and time for the most recent stage of the batch.

- Last Stage

  Information about the stage of a batch includes the last stage it reached when the batch job was last run. Possible stages are:

  - Batch - A batch job acts only on CMP tables.
  - Extract/Load - Data is extracted from CMP tables to create outbound files, for example during the Invoice Analytics, Credit Reference or Bill Print jobs. Or data from inbound files is loaded into CMP tables, for example during the Recurring Payment Rejections, Managed Numbers or SIM Profiles jobs.
  - Transform - Data is transformed to and from JSON files, according to the CMP JSON schema, for example during the Rated Usage and Ledger jobs.
  - Transmission - Files are sent to third parties, such as during the Communications process.
  - Verification - Confirmation that files were sent or received.
  - Acknowledgement - This includes outbound acknowledgement of an inbound file, confirming CMP has processed a file from a third party or inbound acknowledgement of an outbound file, for example a third party or adaptor informing CMP whether it was able to transform and transmit a file.

- Status

  A batch can have the following statuses:

  - Complete
  - In progress
  - Error

4. 2 CMP Processes

In CMP, a process is a business activity such as Billing, Payments or Credit Management. A process can consist of a number of *jobs*, executed in sequence, or a single job such as Recurring Payments - Bank Mode. Also not all jobs are part of a process. A process can also include daemons and probes.

For more information, see the following sections:

- "Jobs" on page 10
- "Daemons" on page 11
- "Probes" on page 23

CMP processes include the following:

- Advance Notification

  The Advance Notification process executes the Advance Notification job followed by its associated alert probe for Batch Complete.

- Billing

  The Billing process executes the following jobs followed by their associated probes in this order:

  1. Invoice Production job
  2. Invoice Production alert probe for Batch Complete
  3. Statement Production job
  4. Statement Production alert probe for Batch Complete
  5. Bill Print job
  6. Bill Print alert probe for Batch Complete
  7. Invoice Posting job
  8. Invoice Posting alert probe for Batch Complete
  9. Usage Archiving job
  10. Usage Archiving alter probe for Batch Complete

- Billing Analytics

  The Billing process executes the following jobs and associated probes in sequence:

  1. Hierarchy Analytics job
  2. Invoice Analytics job

- Credit Control

  The Credit Control process executes the Credit Control job followed by its associated alert probe for Batch Complete.

- Data Warehouse - Consumer Postpaid

  The Data Warehouse - Customer Postpaid process executes the following Data Warehouse jobs in sequence:

  1. Subscription Analytics job
  2. Subscription Services Analytics job
  3. Subscription Features Analytics job
  4. Account Analytics job
  5. Agreement Analytics job
  6. Unbilled Usage Analytics job
  7. Billed Usage Analytics
  8. Unallocated Usage Analytics job
  9. Invoice Detail Analytics job
  10. Payment Detail Analytics job
  11. Transaction Detail Analytics job
  12. Purchase Analytics job
  13. Postpaid Analytics Extract Complete probe that checks for the production of 12 files produced by the jobs above.

- Data Warehouse - Consumer Prepaid

  The Data Warehouse - Customer Prepaid process executes the following Data Warehouse jobs in sequence:

  1. Subscription Analytics job
  2. Subscription Features Analytics job
  3. Subscription Services Analytics job
  4. Account Analytics job
  5. Agreement Analytics job
  6. Prepaid Usage Analytics job
  7. Purchase Analytics job
  8. Payments Analytics job
  9. Unallocated Usage Analytics job
  10. Prepaid Analytics Extract Complete probe that checks for the production of 9 files produced by the jobs above.

- Manage Number Monitor

  The Number Monitor process executes the Managed Number Monitor job followed by its associated alert probe for low availability of SIMs and numbers.

For more information on processes and jobs, see the CMP Batch Jobs and JSON Schemas Guide.

4. 2. 1 Processes Screen

The **Processes** screen lists the CMP processes with the following information:

- The process name - for example Billing, Credit Control or Purge
- When the process is next scheduled to run
- When the process was last run
- The process status:
  - Red = Failed
  - Green = Completed
- The status of any relevant probe associated with the process jobs:
  - Red = Severe
  - Amber = Warning
  - Green = Success

Click any row in the **Process** list to open the **Process Steps** panel for that process.

4. 3 Jobs

In the Administration Console, jobs can be viewed and managed in the **Jobs** screen.

Jobs can be:

- CMP jobs - these jobs do not consume any external data from a third party, nor do they produce any. They operate on CMP tables.
- Inbound jobs - take a JSON file from a third party and processes it.
- Outbound jobs - produce a JSON file for a third party to consume.

For inbound and outbound jobs; the data inputs and outputs must be formatted as JSON files according to the JSON schemas defined by MDS Global. Adaptors need to be built for network/system interfaces in order to convert data from the native format into the required JSON format and vice versa. For more information, see the CMP Batch Jobs and JSON Schemas Guide.

The **Jobs** screen provides execution status information for all jobs. The jobs are listed in a table layout with the following columns:

Name

The name of the job. The job name is a hyperlink to further job details, which include the following:

- Details - the job description and any job parameters. The job details include the job priority, which can be LOW, NORMAL or HIGH. This setting allows CMP to give threads of execution priority. Priority is set through a `priority` property to the job metadata by MDS Global and would typically not be modified.
- Error and Exceptions - an explanation of errors and exceptions associated with the job, with advice for resolving them.
- Configuration - descriptions of the properties and business configuration that apply to the job. Configuration details include both properties that can be configured in the Modules section of the Administration Console and business configuration settings. Some business configuration settings are configured in the Business Configuration console, such as workflow event and system properties, account types or credit control procedures, for example. Links are provided to take you directly to the appropriate location in Business Configuration. Consult the Business Configuration online help for how to configure the settings.
- Notes - notes added by operators about the job to help the understanding of future users.

Module

The CMP module which the job belongs, such as `sabre-data-warehouse`, `sabre-comms` or `sabre-credit-control`.

Last Run

The date and time when the job was last run.

Last Batch

The batch ID for the last run of the batch job. This is a hyperlink that you can click to go to the batch audit details.

Last Run Progress

The progress of the job expressed as a percentage.

Last Run Status

The final status of the job when it was last run. Possible statuses are:

- COMPLETED
- FAILED

The status is a link to view the **Execution Detail**, which includes the job steps and log.

Recent Executions

The number of times the job has been run. The number is a link that allows you to drill down into the **Job Executions** and individual **Job Execution Detail**, which includes the job steps and log.

Enabled

For jobs that are not automatically triggered by system events (autorun jobs), a green check mark indicates an enabled job. A red cross indicates a disabled job.

For autorun jobs, a green symbol of a lightning bolt in a circle  means the trigger for the job is enabled. The lightning bolt in a red *stop* circle  indicates a disabled trigger.

Although most jobs will be scheduled or automatically triggered, it is possible to run jobs manually in **Jobs** screen. You can also enable or disable jobs.

For information on individual jobs and their associated daemons and probes, see the CMP Batch Jobs and JSON Schemas Guide.

4. 4 Daemons

Jobs can have associated *daemons* that perform lightweight background tasks without user intervention, such as the loading, extraction, transformation, and transmission of data to and from external systems and the acknowledgement and verification of such data.

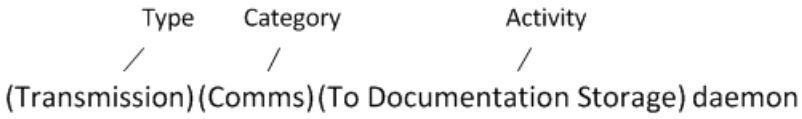
In the Administration Console, daemons can be viewed and managed in the **Daemons** screen. The following information is provided:

Name

Daemons are named using their type, category and activity, for example:

- Load Rated Charges From Generic Format daemon

- Transmission Comms To Documentation Storage daemon



The *type* of a daemon depends on the task it performs. Daemon types include the following:

- Batch - A batch job acts only on CMP tables.
- Extract - Extract daemons extract data from CMP tables to create outbound files, for example during the Bill Print job.
- Load - Load daemons load data from inbound files into CMP tables, for example during the Recurring Payment Rejections, Managed Numbers or SIM Profiles jobs.
- Transformation - Transformation daemons convert data is transformed to and from JSON files, according to the CMP JSON schema, for example during the Rated Usage job.
- Decrypt - Decrypt daemons convert encrypted files.
- Transmission - Files are sent to third parties, such as during the Communications process.
- Acknowledge - This includes outbound acknowledgement of an inbound file, confirming CMP has processed a file from a third party or inbound acknowledgement of an outbound file, for example a third party or adaptor informing CMP whether it was able to transform and transmit a file.

The *category* of a daemon is the business activity or job with which it is associated, such as Bill Print, Comms, Managed Numbers, and so on.

The *activity* of a daemon describes what it does according to its type. For example, a **Load** type daemon with the activity **From Generic Format**, collects and decrypts generic CMP files and creates CMP batches, which are available for processing into CMP by the appropriate batch job, whereas an **Transformation** type daemon with the activity **From ADDACS Format** converts ADDACS (Automated Direct Debit Amendment and Cancellation Service) files into the format required by CMP.

The daemon name is hyperlink to the following details for that individual daemon:

- Description - a description of the task that the daemon performs.
- Configuration - what parameters or properties must be set for the daemon to execute correctly.

Module

The screen lists the CMP module to which the daemon belongs, such as `sabre-data-warehouse`, `sabre-comms` or `sabre-credit-control`. The module name is a link to the **Modules** screen for that module.

Direction

Like jobs, daemons can have direction:

- Inbound - the file/data on which the daemon act is received by CMP
- Outbound - the file/data on which the daemon acts goes to an external system/third party.
- Batch - The daemon acts on CMP database tables only. Files are neither received from or sent to external systems/third parties.

Status

A daemon can have the following statuses:

- Idle
- In progress

In addition to the information above, the console provides the date when the daemon last ran and whether the daemon is currently active.

5.0 System Management

Manage system processes in the following screens:

- Outages:

  Configure planned outages.

- Schedules:

  Create schedules for jobs and probes.

- Exclusion Calendars:

  Configure exclusions for schedules such as public holidays and weekday-only exclusions.

5. 1 Outages

In the **Outages** screen you can:

- Schedule and manage global outages.

  Global outages occur when all processes, probes and jobs are stopped for a period of time, for example for a deployment, upgrade, or system repair or maintenance. In the Outages screen you can see the:

  - Descriptive name for the outage.
  - Date and time from which the outage is effective.
  - Date and time to which the global outage is effective.
  - Whether the status has not started yet  or is in progress  .

  To schedule a global outage, you need to configure the following:

  - A start date and time for the global outage.
  - The date and time the outage ends.
  - A meaningful descriptive name for the outage.
  - Set post-outage actions for any affected jobs, probes, or daemons. For example, you can choose whether a job should be run immediately after the outage, or when next scheduled.

- View individual outages

  Individual outages are configured as part of a schedule and refer to individual probes, processes or jobs that are stopped for a period of time. For example, you may want to stop certain jobs and probes over weekends or Bank holidays. You cannot create individual outages in the **Outages** screen; they are created when you create a schedule. However, they are listed in this screen and you can see the:

  - Name of the schedule that includes the outage
  - Type of item to which the outage applies: a process, job, or probe.

- Name of the process, job, or probe affected by the outage.
- Date and time from which the outage is effective.
- Date and time to which the global outage is effective.

5. 2 Schedules

Wherever possible, operational tasks should be automated. In CMP, you can do this by creating schedules for processes, jobs and probes. The **Schedules** screen allows operators to view, add, suspend/resume, import, export, and delete schedules.

5. 2. 1 View details for schedules

The screen displays all the schedules for jobs, probes, and processes. The following details are supplied:

- The name of the schedule.
- The type of item being scheduled: a probe, process or job.
- The reference for the schedule, which is the name of the probe, process or job to which the schedule applies.
- A text description of the schedule, for example, *At 04:00, only on Monday, Tuesday, Wednesday, Thursday and Friday*.
- The date and time when the item will next be run, according to the schedule.
- Whether the schedule is currently active.

You can also drill-down into individual schedules for more details, such as notes, schedule settings and any exclusion calendars, outages, and pre- or post-requisites that apply.

5. 2. 2 Add a new schedule

When you create a schedule, you need to configure the following:

- The name, and type of the schedule.
- The reference for the item scheduled (the name of the probe, job or process).
- Any notes to help console users understand the schedule.
- Whether the schedule is active and the date from which it is active.
- The schedule itself: the days and times that the item is run, according to the schedule. The schedule options are very flexible, allowing you to easily configure daily, weekly, monthly, and yearly schedules. As well as schedules that run items every specified number of minutes or hours.

  The following table describes the schedule options and when to use them:

Schedule Option	Description
Daily	
Every <number> day (s) at	Use option to schedule the item to run every specified number of days each week at a certain time. For example: **Every 1 day(s) at 04 30 00**.
Every week day (Monday through Friday) at <HH><MM><SS>	Use this option to schedule the item to run every week day at a certain time. For example: **Every week day (Monday through Friday) at 23 59 00**.
Weekly	
Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday	Choose the weekly schedule when you want the item to run every week on a specific day or days at a set time - for example, every Monday and Friday at 13:00:00.
Start time	Set the start time in hours, minutes and seconds.
Monthly	
On the <number> of every <number> month(s) at <HH><MM><SS>	Choose this option when you want the item to run on a specific day of the month every specified number of months at a certain time, for example on the last day of every second month at noon. For example: **On the 1st Day of every 1 month(s) at 01 00 00**.
On the <number> <day> of every <number> month(s) at <HH><MM><SS>	Use this option when you want the item to run on a specified day of the week every specified number of months at a certain time, for example every second Wednesday every month at midnight. For example: **On the First Monday of every 1 month(s) at 23 59 59**.
Yearly	
Every <month> on the <numbered day> at <HH><MM><SS>.	Select this option to schedule an item to run every year on a certain day (first, last, 15th etc.) of a specified month at a set time.
On the <number> <day of the week> of <month> at <HH><MM><SS>	Select this option to run every year on a certain day of the week (last Friday, first Monday etc.) of a specified month at a set time. For example: **On the First Monday of January at 01 30 00**.
Minutes	
Every <number> minute(s) on second <number>	Use this option to run an item every specified number of minutes, for example every 10 minutes.
Hourly	
Every <number> hour(s) on minute <number> and second <number>	Use this option to schedule an item to run every specified number of hours, for example every 2 hours on minute 1 and second 30.

Schedule Option	Description
Advanced	
Cron expression	You can enter a cron expression[1] for a schedule. **Tip:** A link to a cron expression tutorial is provided in the console.

- Any exclusion calendars associated with the schedule.

  You can configure exclusion calendars to prevent items running on particular days such as weekends and public holidays. Exclusion calendars must be added to a schedule to become effective. In the Exclusion Calendar section, you can view the calendars that apply to a schedule and add calendars to the schedule.

- Any individual outages included in the schedule.

  You can add outages to a schedules - time periods where the scheduled item will not run, for example during deployments, upgrades or maintenance.

- Any pre- or post-requisites required by the schedule.

  Some jobs or processes may be dependent on the output or result of previous jobs, or must be run in a particular sequence. You can add prerequisites to a schedule to ensure that the scheduled item will not be run unless the requisite input is available or operation is complete. Similarly, you can configure post-requisites to ensure that a scheduled item has run correctly or that jobs and processes dependant on the scheduled item run in the required sequence.
  - For pre-requisites, you can select probes that must be run.
  - For post-requisites, you can select probes, jobs, or processes.

5. 2. 3 Suspend/Resume a schedule

You can activate or deactivate a schedule by resuming or suspending it.

5. 2. 4 Export schedule(s)

You can export individual or multiple schedules at a time as a JSON file with the naming convention `Export_Schedules YYYY-MM-DD.json`.

5. 2. 5 Import schedule(s)

You can import a schedule in the form of a JSON file.

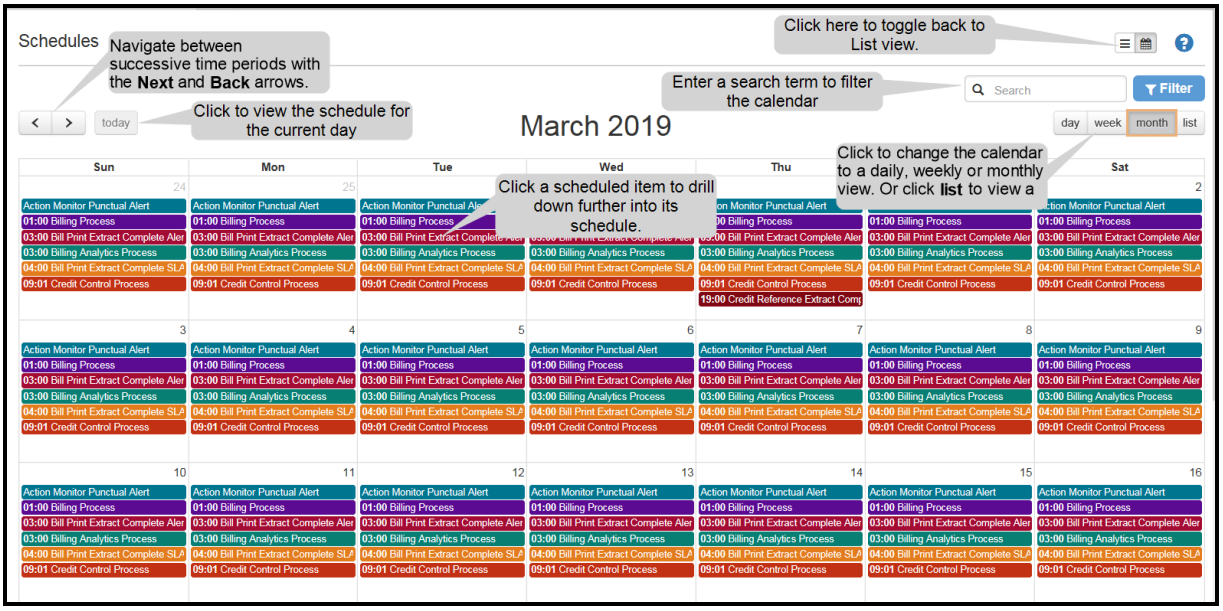
[1] A cron expression is a string consisting of fields separated by white space. The string represents a set of times that make a schedule for a routine.

5. 2. 6 Delete schedule(s)

Only inactive schedules can be deleted. You can delete multiple schedules at a time.

5. 2. 7 Schedules Calendar View

The calendar view displays the schedules in a calendar format that you can view by day, week, month or in the form of a daily list.



*The **Schedules** calendar view, showing the schedules for a month.*

5. 3 Creating a Schedule

Wherever possible, operational tasks should be automated. In CMP, you can do this by creating schedules for processes, jobs and probes.

When assembling a production schedule, consider the following:

- What is coming into CMP from third parties and how often?
- What is produced by CMP for third parties and how often?
- What sort of alerts are required?
- Will it be necessary to monitor all stages of a process, for example batch, extraction, transformation and transmission?
- What sort of Service Level Agreements (SLAs) are required?
- Are exclusion calendars necessary? For example, BACS does not accept files on non-banking days, which impacts the Mandate Registrations job.
- Which jobs must run constantly throughout the day, such as Workflow Monitor, for example?

It is recommend that start times for jobs are not scheduled between the hours of the morning when *daylight savings* changes occur in your locale because the time shift can cause a job to be skipped or repeated depending on whether the time moves back or jumps forward.

5. 3. 1 Production Schedule for Inbound Files

Operations for inbound files involve the following:

- A load daemon polling for new files.
- A job being triggered if a file is successfully loaded.
- An acknowledgement daemon that informs the third party that CMP has processed the file; or whether there are issues with the file.
- Probes.

Scheduling considerations for inbound files include the following:

- What is scheduled?

  Daemons and jobs are triggered by the presence of an inbound file, so these cannot be scheduled.

- Should probes be scheduled?

  Daemons and jobs are not scheduled, but probes can be scheduled based on the frequency of the inbound files.

- Why are probes required?
  - To alert operators if no files are presented by the third party.
  - To alert operators if files are loaded but have errors. Some errors may be fixable, but some not.
  - To gather SLA information about a job. For example an SLA can be that a file cannot contain more that a configurable amount of errors.

5. 3. 2 Production Schedule for Triggered Jobs

Triggered jobs are jobs that are initiated by the presence of a record in a particular state in a table. These include jobs such as Workflow Monitor, Action Monitor, Email Monitor and Ledger Monitor.

Scheduling considerations for triggered jobs include the following:

- What is scheduled?

  All jobs are triggered by the presence of a record in a table, so they cannot be scheduled.

- Should probes be scheduled?

Probes are needed to check whether the triggered jobs are functioning as expected, so they can be scheduled to run every 10 minutes, for example.

- Why are probes required?
  - To alert operators if there is a build up of errors, for example workflows all ending in a processing error. This type of probe is monitoring for normal execution of the job.
  - To alert operators if a backlog of requests is building up, for example ledger transaction entries in a New state. This type of probe is monitoring for punctual execution of the job.

5. 3. 3 Production Schedule for Processes

A process is a business operation consisting of one or more jobs and alerts(s) executed in sequence. The end goal of a process is typically a file for a third party. A process can also include extraction, transformation, transmission and acknowledgement daemons.

- What is scheduled?

  The process itself is scheduled. Jobs are executed in sequential order once the first job ends.

- Should probes be scheduled?

  Probes can be linked to the process to check whether a job executed as expected. However, probe scheduling can also take into account downstream activity. For example, the Bill Print job is the final job in the Billing process. The output of the job is entries in the interface tables. Various daemons are then executed to get the billing batch to the third party. Probes should be scheduled for this.

- Why are probes required?

  - To alert operators if no file was presented to the third party.
  - To gather SLA information. For example, the SLA for the Billing process is to produce a file for the print bureau. If no file is produced, the SLA is breached.

For an example of a production schedule, see "Appendix A: Sample Production Schedule" on page 35.

5. 4 Exclusion Calendars

You can configure exclusion calendars that specify days and times when processes, jobs or probes will not be run, for example public holidays or weekends. Exclusion calendars can be configured as:

- Weekly - to exclude days of the week. For example porting does not take place on weekends so you may want to create an exclusion calendar for weekends and

apply it to porting schedules. You can also configure hours to be excluded when you configure a Weekly exclusion calender.
- Holiday - for public holidays that fall on different days on the year, Good Friday in the UK, for example.
- Recurring Holidays - for public holidays that occur on the same date every year, for example Christmas Day on 25 December.

The **Exclusion Calendars** screen allows operators to view, add, copy, export, import and delete exclusion calendars.

5.4.1 View details for exclusion calendars

The following details are supplied:

- The name of the calendar.
- The description for the calendar.
- The type of calendar- if the calendar is a weekly, holiday or recurring holiday calendar.
- The console user who last altered the calendar.
- The date and time when the most recent change took place.

You can also drill down into individual exclusion calendar settings, such as days, times and dates.

5.4.2 Add an Exclusion Calendar

You create new exclusion calendars by providing a description and specifying the weekdays, times or dates of the exclusion.

If you are creating a Weekly calendar, you can use the Invert Hours function to reverse your settings and create an exclusion calendar that invests the exclusion so that the time period you specify is not excluded, but in fact is the only time that the scheduled item will run.

5.4.3 Copy an Exclusion Calendar

You can base a new exclusion calendar on an existing one by copying it. Once you supply a new name and description for the copied calendar, you can retain the original settings or adjust it as needed.

5.4.4 Export an Exclusion Calendar

You can export individual or multiple exclusion calendars as a time as a JSON file with the naming convention: `Export_Calendars YYYY-MM-DD.json`.

5. 4. 5 Import an Exclusion Calendar

Exclusion calendars can be imported as JSON files.

5. 4. 6 Delete an Exclusion Calendar

You can delete only one exclusion calendar at a time.

6.0 System Monitoring

Monitor the system in the following screens:

- Executions

  Enables rapid troubleshooting of unsuccessful executions and failures.

- Logs

  Provides detailed log records of all system and operational processes.

- Outage Misfire Logs

  Logs all misfires due to global outages.

  Network Requests

  Provides a view of all requests in the network request log.

- Messages Queues

  Provides a view of all messages in ActiveMQ queues

6. 1 Probes

In the Administration Console, probes can be viewed and managed in the **Probes** screen.

Probes provide functional monitoring of a job's health. A probe is a mechanism that allows the execution of predefined queries and the comparison of the query results against preconfigured targets. Each probe is very specific to the functionality of the job it is monitoring, for example indicating whether inputs have been received as frequently as expected or the percentage of rejections is within an acceptable tolerance.

There are three types of probe:

Alert

An *alert* probe warns operators when expected targets have not been met or are in danger of not being met. For example, an alert probe can detect whether:

- A job was executed punctually.
- An extract daemon has produced a file.
- A load daemon has processed an inbound file.
- A job has executed as expected.

For Alert probes you can configure email recipients to receive notifications.

Service Level Agreement (SLA)

An SLA[1] probe gathers statistics on a daily basis about all jobs that have SLA dependencies. For example, an SLA probe can detect:

- Whether a file was produced by a third party (if no file was produced, the SLA is breached).
- The number of configuration errors in a file produced by a third party (if the errors exceed a configurable value, the SLA is breached).

System

A *system* probe monitors the overall health of the batch server, for example, a system probe can detect any exception that causes a job to fail.

Standard alert, SLA, and system probes for CMP batch jobs are predetermined with Business Operations and configured prior to deployment. A CMP batch job can have as many probes as required by Business Operations.

Probes are identified by a name, which often includes the stage of a process and what the probe is testing for. For example a probe named **Completed** checks whether a daemon or job for a particular stage has completed successfully, and a probe named **Transmission** checks whether a file has been successfully transmitted. Examples of probe names include:

- System Activity Batch Complete.
- General Ledger Extract Complete.
- Comms Email Verification Normal.

Probes can check any stage and status of a process. Processes in CMP typically either:

- Produce an outbound file for a third party.
- Or, the reverse process - receive an inbound file from a third party and load the data from an inbound file into CMP.

Some processes in CMP, for example Purging, act only on CMP tables and do not involve files from external sources.

So processes can involve a number of stages, such as:

- Batch - A batch job acts only on CMP tables.
- Extract - Data is extracted from CMP tables to create outbound files, for example during the Invoice Analytics, Credit Reference or Bill Print jobs.
- Load - Data from inbound files is loaded into CMP tables, for example during the Recurring Payment Rejections, Managed Numbers or SIM Profiles jobs.

[1] A service level agreement (SLA) is a contract between a service provider and a client that defines the level of service expected from the service provider, for example the degree of availability and performance that can be expected and the responsibilities of the service provider and the client.

- Transform - Data is transformed to and from JSON files, according to the CMP JSON schema, for example during the Rated Usage and Ledger jobs.
- Transmission - Files are sent to third parties, such as during the Communications process.
- Verification - Confirmation that files have been sent or received.
- Acknowledgement - This includes outbound acknowledgement of an inbound file, confirming CMP has processed a file from a third party or inbound acknowledgement of an outbound file, for example a third party or adaptor informing CMP whether it was able to transform and transmit a file.

A probe can have the following statuses:

- Severe
- Warning
- Success
- Not Run.

In addition to the characteristics above, each probe can be viewed individually to see its:

- Definition - a description of what the probe does.
- Version - all probes that are initialised must have at least one version (see below).
- History - a history of all probes is kept for reporting purposes. The history of a probe includes its execution date, whether it's pending distribution and the result and status of the probe.
- Notes - Notes are made by the creators of probes and probe versions to help the future understanding of other operators.
- Recipients - alert probes can have recipients that are notified by email when a probe has a Warning or Severe status.

In order to initialise a probe, you must create a probe version. A probe version sets the conditions at which the probe status becomes Severe or Warning. This can include, for example:

- The number of job executions
- The number of files received
- The number of files transmitted
- The number of errors in inbound files.

MDS Global ships probe versions as part of the SQL deployment.

SLA Probe statistics are aggregated and viewed at month and year level in Administration Console. SLA information can be exported from Administration Console for reporting purposes.

6. 2 Executions

The **Executions** screen lists all the jobs in the Administration Console with their most recent status. You can see at a glance how many times a job has run, which jobs have

completed successfully, and which have failed.

The information supplied includes:

- The name of the job.
- The number of times the job has been run or the execution count. You can drill down into individual executions of the job to view job execution details such as the job duration, exit message and exit code, as well as drilling down into the job steps and viewing logs for the job.
- The date and time the job was last started.
- The date and time that the job last ended.
- The most recent status of the job - COMPLETED or FAILED. You can also drill down into the status to access job execution details, as you can for the execution count.
- The progress of the jobs last run, expressed as a percentage.

6. 3 Logs

The Logs facility allows users to interrogate the persisted log records. These logs are for the entire batch server and also the Administration Console. You can use the filter functionality to retrieve a subset of the logs to investigate a specific issue, job or daemon.

You can filter on:

- Date ranges.
- Jobs - you can search by job name or execution ID which you can retrieve from the job execution details.
- Logging Level - for example **Error** or **Debug**.

You can also search the logs for specific search terms.

6. 4 Outage Misfire Log

The outage misfire log lists all items that have misfired due to a global outage. This can include, for example, any scheduled items that could not run or dropped files. The following details are available:

- The name of the item that misfired
- What type of item misfired; a job, process, daemon
- What initiated the misfired item, for example daemons can be triggered by jobs, jobs can trigger other jobs, and so on
- When the misfire took place.

You can re-run the affected item manually from within this screen.

6. 5 Network Requests

Network Requests allows users to:

- View network requests from the network request log.
- Drill down into individual network requests for more details.

All network requests in the network request log are listed with the following details:

- The request ID number.
- The CMP subscription number to which the network request applies.
- The type of action requested:
  - Allowances
  - Connections
  - Disconnections
  - Network Services
  - Bars
  - Unbars
  - Number Changes
  - Tariff Changes
  - Other.
- The status of the network request.
  - UN - Unprocessed
  - PR - Processed
  - NS - Network Sent
  - NA - Network Accepted
  - NR - Network Rejected
  - NE - Network Error
  - NF - Network Failed
  - NC - Network Complete
  - PE - Processing Error.
- The timestamp (dd/mm/yyyy hh:mm:ss) for when the network request was created.
- The timestamp (dd/mm/yyyy hh:mm:ss) for when the network request was sent.
- The timestamp (dd/mm/yyyy hh:mm:ss) for when the network request was completed.

It is possible to drill down into the details for individual network requests. In addition to the ID, subscription number, network action type and status, the details provided include the following:

- Workflow Action Type - The code and description of the action type of the workflow event associated with the network request, for example RTC Provisioning (RTC).
- Workflow Action Code - The code and description of the action code of the workflow event associated with the network request, for example Connection (CONN).
- Network Command - The code and description for the network command associated with the network request, for example Connection (CONN).
- Workflow Event Number - the unique CMP number for the workflow event.

- Workflow Event Action Item Number - the unique CMP number for the workflow event actioned item associated with network request.
- Action Item Error Text - If the action item errored, any associated error text/message.
- Timestamps in dd/mm/yyyy hh:mm:ss format for when the network request was created, completed and sent.
- The history of the request as follows:
  - Sequence - 1 represents the first stage in the request history, 2 for the next and so on.
  - Status - Processed, Unprocessed, Network Error, etc.
  - Event Date/Time - Timestamps in dd/mm/yyyy hh:mm:ss format for when the event took place.
  - Extra Information - any additional information.

6. 6 Messages Queues

Message Queues allows you to:

- View ActiveMQ Artemis[1] message queues.

  For more information on ActiveMQ Artemis see https://activemq.apache.org/components/artemis/
- Purge message queues.
- Drill down into individual queues for more details.

All Artemis message queues are listed with the following details:

- The name of the queue, such as InboundSalesOrder or outboundDeviceEnrolment. It is a link that you can click to go drill down into the message queue for details.
- The number of pending messages in the queue.
- The number of consumers of the messages.
- The number of messages enqueued.
- The number of messages dequeued.

You can drill down further into a particular ActiveMQ message queue in the **Message Queues** screen.

Details for messages and consumers are displayed in the **Messages** and **Consumers** tabs.

In the **Messages** tab you can:

---

[1]Apache ActiveMQ is an open source message broker written in Java together with a full Java Message Service client. It fosters the communication from more than one client or server.

- View the messages in an ActiveMQ queue.
- View the **Message Details** and **Message Properties**.
- Delete a message.

The **Messages** tab lists the messages in the queue with the following information:

- The unique ID of the message, for example `D:beta21.mdsuk.com-36920-1613051754753-9:1:3:1:2`.
- A correlating ID for the message, if applicable.
- Whether the message is PERSISTENT or not.
- The priority of the message, expressed as a number, 1 being the highest priority.
- Whether the message has been redelivered - `true` or `false`.T
- The date and time the message was delivered, in the format `YYYY-MM-DD HH:MM:SS`.

You can also view **Message Details** and **Message Properties** for an individual message.

7.0 System Configuration

Configure the system in the following screens:

- Modules

  Enables configuration of system-wide parameters, application parameters and parameters for all modules installed on the system.

  Logging

  Add loggers and update their logging levels.

- Servers

  View server information for CMP, reboot servers and restart applications.

7. 1 Modules

Administration Console modules are JAR packages that contain the code for all the processes, jobs and daemons that make up the console functionality. In the **Modules** screen, you can configure system-wide parameters, application parameters and parameters for all modules installed on the system.

When you access the **Modules** screen, all groups of CMP modules for all CMP functional areas are listed with their descriptions, for example **Sabre Server**, **AgentView**, **Bulk Action**, **Database**, **Web Services**.

Expand the module to view a list of the properties and their current version numbers.

Click the module group name to go to the **Modules** screen for that group. The screen lists the properties by **Name**, **Version** and **Installation** date.

The **Sabre Server Modules** screen offers more functionality. Here you can:

- Edit module properties.
- Add module properties.
- Change the logging level for a module.
- Redeploy a module.

The **Sabre Server Modules** screen lists the properties in a table layout with the following columns:

- Name - the name of the module, for example sabre-workflow-monitor or sabre-mandate-revisions.
- Version - the currently deployed version number for the module, for example, 1.11.28.

- Description - a description of the module, for example *MDS Ledger Adapter* or *Generic Outbound Adaptor Activity Daemon*.
- Parent - the parent module to which this module belongs.
- Installation Date - the date and time the module was installed.
- Jobs - a link to the **Jobs** screen, if applicable.
- Daemons - a link to the Daemons screen, if applicable.
- Probes - a link to the Probes screen, if applicable.

Click the table row for any module to expand it for more information:

- Properties - The properties and their values are listed. They are grouped under headings for their relevant jobs or daemons so that you can locate them easily.

  Properties are editable. Hover your mouse over the info icon to display a pop-up window with a description of the property. You can also add predefined properties to modules. If you have edited a module's properties, you must redeploy the module for the changes to take affect.

You can use the **Revert to Original** function to undo any changes you made and restore the original parameter values.

- Logger - The name of the logger for this module. You can change the logging level. The following levels are available:
  - WARN
  - OFF
  - FATAL
  - ERROR
  - INFO
  - DEBUG
  - TRACE.

For more information, see "Logging" below.

7. 2 Logging

In the **Logging** screen, you can:

- View the loggers that monitor the console operations.
- Add new loggers.
- Configure the number of days to retain a log.
- Change the logging level for a logger.

The following logger details are available:

- The name of the logger, for example *com.mdscem.cmp.framework.probe.ProbeResultEvaluator*.
- The logging levels, which can be:
  - OFF

    Do not log anything at all.

- **INFO**

  INFO messages correspond to normal application behaviour and milestones, such as a service starting or stopping. This level of information is typically used to help run and manage the system.
- **DEBUG**

  Granular information to help with diagnosis of problems and troubleshooting. DEBUG messages and information are used by system administrators and developers.
- **TRACE**

  Very fine-grained information - even more granular than DEBUG. Use the TRACE level when you need to capture every detail you can about the application's behaviour. This level produces a great deal of a data that can overwhelm the system's resources in production, so should be used with caution.
- **WARN**

  Use the WARN log level to indicate that there might have a problem and that you've detected an unusual situation. This level is often used for handled exceptions and important log events. Warning should be investigated.
- **ERROR**

  An error is a serious issue and represents the failure of something important in the application. ERROR is used to log all unhandled exceptions.
- **FATAL**

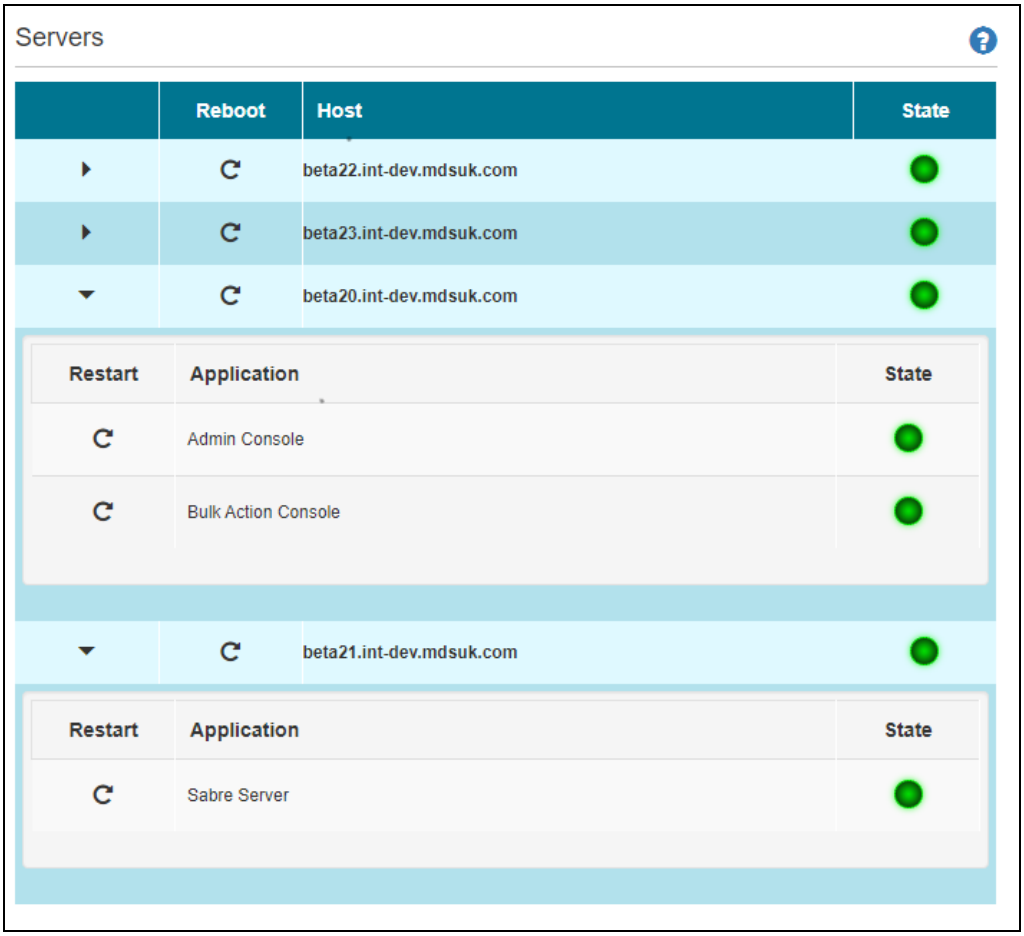
  FATAL represents a very serious situation that can cause the application to abort to prevent data loss, corruption or some other serious problem. Fatal is usually reserved for special exceptions/conditions where it is imperative that you can quickly pick out these events.

7. 3 Servers

In the **Servers** screen, you can:

- View server information for CMP.
- Display a list of modules installed on a server.
- Restart applications.
- Reboot the server.

The screen displays a set of collapsible panels - one for each of the hosts in a CMP system.



Each server panel displays the name of the host and the state of the host: green =active or red = inactive. There is also a Reboot option for the host.

The body of the server panel lists the CMP applications that are installed on each host. Each application also has a State and a Restart option.

8.0 System Administration

Administer the system in the following screens:

- Users

  Create users. Grant them access to applications and assign them roles.

8. 1 Users

In the **Users List** screen, you can:

- View a list of users and view details for individual users.
- Add a user and assign them access to CMP functional areas.
- Edit the details of individual users.

The **Users List** screen lists CMP users in a table layout with the following headings:

- Username - the username of the user, for example annag.
- First Name - the first name of the user, for example Anna , for Anna Green.
- Last Name - the surname or family name of the user, for example Green, for Anna Green.
- The email address - for example anna.green@mdsglobal.com.
- Security Level - the security level of the user.

Clicking the hyperlink for a username opens the **View User** screen, where you can view user details and the applications that they have access to.

To create a user, you need to provide the following:

- First and last name
- Username
- Password
- Email address
- Contact number
- Security level.

When you create a user, you can grant them access to an application, after which you can assign them to a group (security roles and permissions) or grant them access to functionality such as bulk actions or web services.

9.0 Appendix

9. 1 Appendix A: Sample Production Schedule

All inbound files into CMP are monitored by distinct Load Daemons, which create Interface Batch Header records with a stage and stage status of *Batch - Complete* (assuming all is valid). Once these batches are created, the corresponding Java job will be triggered automatically, so these jobs are not included as scheduled processes. The table represents key internal jobs (for example, Invoice production, Credit Control) and jobs that produce a file for a third party, such as Bill Print and Credit Reference.
Also excluded from the table are jobs such as Workflow Monitor, Action Monitor, Letter Monitor, Email Monitor. These are triggered automatically

The table below shows a suggested production schedule for processes:

Seq	Scheduled Process	Process Content	Execution Frequency	Notes
1	Billing	Invoice Production Batch Complete (alert probe) Statement Production Batch Complete (alert probe) Bill Print Batch Complete (alert probe) Invoice Posting Batch Complete (alert probe) Usage Archiving Batch Complete (alert probe)	Daily 01:00	This job is kicked off 1 hour after midnight to allow for Rated Charge Job to run on cycle i.e. no point in invoicing if reliant on third party to supply the charges.
2	Recurring Card Payment	Recurring Payments - Card Mode Batch Complete (alert probe)	Banking Days 10:00	This job would only run once per day.
3	Recurring Bank Payments	Recurring Payments - Card Mode Batch Complete (alert probe)	Banking Days 10:00	This job would only run once per day.
4	Customer Purge	Account Purge Batch Complete (alert probe) Address Purge Batch Complete (alert probe)	Monthly 04:00	
6	Mandate Registrations	Mandate Registrations Batch Complete (alert probe)	Banking Days 09:00	This job would run only once per day.
7	Billing Analytics	Hierarchy Analytics Extract Produced (alert probe) Invoice Analytics Extract Produced (alert probe)	Daily 03:00	This job would be scheduled to run after the Billing process.
8	Unbilled Usage Analytics	Unbilled Usage Analytics Extract Produced (alert probe)	Daily 03:00	This job would pick up on usage from the previous day.
9	Credit Control Process	Credit Control - Full Mode Batch Complete (alert probe)	Daily 09:00	While this job can be scheduled, it is also

Seq	Scheduled Process	Process Content	Execution Frequency	Notes
				triggered automatically in event of a payment.
10	Debt Recovery New	Debt Recovery - new account type Batch Complete (alert probe)	Monthly 18:00	
11	Debt Recovery Existing	Debt Recovery - existing account Batch Complete (alert probe)	Monthly 18:00	This job would typically run once a month. Debt Recovery - New & Existing are purposely kept in separate process, as the job raises workflows asynchronously to change account types. If these ran immediately after each other, the second job may select accounts that it should not.
12	Credit Reference Process	Credit Reference Batch Complete (alert probe)	Monthly 18:00	

The following Alert probes need to be added to the schedule:

Seq	Scheduled Item	Execution Frequency
1	Workflow Monitor Normal	Daily - Every 10 minutes
2	Workflow Monitor Punctual	Daily - Every 10 minutes
3	Action Monitor Normal	Daily - Every 10 minutes
4	Action Monitor Punctual	Daily - Every 10 minutes
5	Ledger Monitor Normal	Daily - Every 10 minutes
6	Ledger Monitor Punctual	Daily - Every 10 minutes
7	Managed Number Availability	Daily - 09:00
8	Debt Recovery Extract Complete	Monthly Last Day - 19:00
9	Credit Reference Extract Complete	Monthly Last Day - 19:00
10	Rated Usage Normal	Daily - Every 10 minutes
11	Rated Usage Punctual	Daily - Every 10 minutes
12	Mandate Registrations Complete	Daily - Banking Days only 10:00
13	Comms Monitor Normal	Daily - Every 10 minutes
14	Comms Monitor Punctual	Daily - Every 10 minutes
15	Letter Monitor Normal	Daily - Every 10 minutes
16	Letter Monitor Punctual	Daily - Every 10 minutes
17	Notification Monitor Normal	Daily - Every 10 minutes
18	Notification Monitor Punctual	Daily - Every 10 minutes
19	Bill Print Extract Complete	Daily - After Billing Process (03:00)
20	Bill Print Transmission Complete	Daily - After Billing Process (04:00)
21	Invoice Extract Complete Sales Ledger	Daily - After Billing Process (03:00)
22	Invoice Extract Complete General Ledger	Daily - After Billing Process (03:00)
23	Invoices Posted CMP Ledger	Daily - After Billing Process
24	Recurring Payments Extract Complete (Card)	Daily - 12:00 (Noon)
25	Recurring Payments Extract Complete (Bank)	Daily - 12:00 (Noon)
26	Recurring Payments Posting Extract Complete	Daily - 12:00 (Noon)
27	Recurring Payments Posting Complete	Daily - 13:00
28	Managed Numbers Load Complete	Daily - 11:00
29	Managed Numbers Batch Complete	Daily - 12:00 (Noon)
30	SIM Profiles Load Complete	Monday to Friday - 11:00
31	SIM Profiles Batch Complete	Monday to Friday - 12:00 (Noon)
32	Mandate Revisions Load Complete	Monday to Friday - 10: 00
33	Mandate Revisions Batch Complete	Monday to Friday - 11: 00
34	Recurring Payment Rejections Load Complete	Daily - 11:00
35	Recurring Payment Rejections Batch Complete	Daily - 11:15
36	Non Recurring Payments Load Complete	Weekdays
37	Non Recurring Payments Load Complete	Weekdays
38	Debt Recovery Response Load Complete	Monthly - 22:00
39	Debt Recovery Response Batch Complete	Monthly - 23:00
40	Rated Charges Load Complete	Daily - 00:30
41	Rated Charges Batch Complete	Daily - 01:00
42	Email Monitor Normal	Daily - Every 10 minutes
43	Email Monitor Normal	Daily - Every 10 minutes

The following table lists the SLA probes that must be added to the schedule:

For outbound jobs, the SLA is that a JSON file was produced; it's all or nothing. For example, an SLA might be 100% in that CMP must produce a file for a Print Bureau each day. For inbound jobs, the SLA probe checks the volume of records that failed to load due to missing CMP configuration, for example Rated Usage, an SLA may fail if there are 5,000 errors due to missing usage classes at end of day.

Seq	Scheduled Item	Job Type	Execution Frequency
1	Mandate Registrations Produced SLA	Outbound	Daily - 23:00
2	Recurring Card Payments Extract Produced SLA	Outbound	Daily - 23:00
3	Recurring Bank Payments Extract Produced SLA	Outbound	Daily - 23:00
4	Debt Recovery Extract Produced SLA	Outbound	Monthly - 23:00
5	Credit Reference Extract Produced SLA	Outbound	Monthly - 23:00
6	Bill Print Extract Produced SLA	Outbound	Daily - 23:00
7	Invoice Posting Extract Produced SLA	Outbound	Daily - 23:00
8	Unbilled Usage Analytics Extract Produced SLA	Outbound	Daily - 23:00
9	Rated Usage SLA	Inbound	Daily - 23:00
10	Rated Charges SLA	Inbound	Daily - 23:00
11	Managed Numbers SLA	Inbound	Daily - 23:00
12	SIM Profiles SLA	Inbound	Daily - 23:00
13	Mandate Revisions SLA	Inbound	Daily - 23:00
14	Recurring Payments Rejections SLA	Inbound	Daily - 23:00
15	Non Recurring Payments SLA	Inbound	Daily - 23:00
16	Debt Recovery Response SLA	Inbound	Daily - 23:00
17	Notification Monitor SLA	Inbound	Daily - 23:00

9. 2 Appendix B - Run Book details

A Run Book details specific information useful in troubleshooting and can contain the information needed during a technical support call.

A typical run book should include:

Version details	For each piece of installed software including the installed version of CMP.
Structure	Detailing the servers and the environments hosted on it.
Clustering details	If clustering is used, list the deployment of applications on each server.
Commands	Commands to run scripts that start and stop the applications on each server and the order in which they should be executed should be listed.

Dependencies	Any co-dependent applications should be detailed.
Logging	The location of logs and the details recorded.
Administration	Functions and addresses of the administration console.
Server Locator	To enable or disable load balancing.