# Monitoring

26 Apr 2024

imagicle

# Table of Contents

imagicle

# Monitoring

## Monitoring service configuration

Imagicle UCX Suite includes a monitoring services which can send alerts to the system administrator when some important events occur. Examples of monitored events are:

- Insufficient disk space
- An Imagicle service failing
- Low database space
- Bad service performance
- License issues
- License overcome (e.g. calls dropped in Advanced Queuing because the licensed channels are too few)
- Authorization issues related to Webex Calling MT tokens

The monitoring service includes auditing features. The list of events can be displayed through a web page and can also be exported in CSV or XLS formats.

### Architecture

The monitoring service (MAM) is installed on the machine by the setup program together with Imagicle applications. It is runs automatically when the machine starts. The service performs two main operations:

- **ALARM**: It monitors the local machine. If some of the monitored parameters are out of range (low disk space, low memory, high CPU, low DB space...), it records an error or a warning in the application event log named "IAS"
- **NOTIFY:** When an error is logged in the event log, it notifies the System administrator through email. It can also generate a SNMP trap messages.

Other Imagicle services can log errors or warnings to the custom UCX Suite event log; the monitor service will take care of the notifications.

Specific event notification can be enabled or disabled through the web interface.

UCX Suite event log can also be browsed through the standard Windows Event Viewer.

The monitoring service is also in charge of deleting old log files (retention period is 30 days by default).

The MAM web interface can be accessed through the main Application Suite menu, selecting "Main" and then "Monitoring". It is available to the UCX Suite administrators only.

### Alarms status

On the **Alarms** tab you can quickly check the health of the system. You can selectively disable the alarms if you think they are not needed. Warnings and errors are displayed here. To read the details of the current status, move your mouse pointer over the little dot with the "i".

### Mail Configuration

Click con **Mail Configuration** to set the list of the recipients of the email notifications. Recipients addresses must be valid email addresses separated by comma (,).

Please make sure that Outgoing Email Parameters have been correctly set for the email notifications to run. See here for more details.

### Event History

The list of events raised by the monitoring service and other Imagicle service can be examined through the web interface in the **Events History** page. The controls on the top of the list will allow you to filter the displayed events by date, by type, by application and by category. Each event has an unique id.

The type of the event represents its severity: information, warning or error.

To enable or disable further notifications, use the checkbox in the event row.

**Warning**: the filter lists are dynamic. If an application, event type or category is not available in the list, this means that no event with that property has been raised yet. As a consequence, you can only disable events that have been notified once.

The list of events can be downloaded in CSV or XLS formats by clicking on the small icons in the upper right corner of the list.

## Monitored events details

The MAM monitors a lot of parameters and can raise a lot of events. Here are some relevant caveats and additional details.

**High Availability**: Replication link status and time alignment

**Service failing:** The error stating that an Imagicle service is failing is raised if the process disappears for more than 15 seconds from the process list.

**Low disk space**: when the disk space is low, the Monitor will warn the user and will also try to gain space by deleting old log files

**Database full**: if no space is left in the database, Imagicle Billing Miner service will be stopped. The call data will be stored in local files until the database is purged. This way no call will be lost.

**Call Recording**: Expired Digital Certificate or not reachable external storage

**Webex integrations authorizations**: Users' synch, Rich Presence, Call Control and Call Analytics authorization issues.

## Tuning and customizations

The monitoring service can run external processes if needed; its behavior can be fine-tuned and customized through XML files. Please ask Imagicle Technical Support team if you have specific needs.

## SNMP configuration

The SNMP configuration web page allows you to easily add the UCX Suite server to a SNMP monitor.

The Simple Network Monitoring Protocol **monitor** is a third party software able to receive the notifications, installed somewhere on your network. Optionally, the software may include a **master agent** which receives the notifications and makes them available to the monitor.

Imagicle MAM acts as a **monitored device**. There is no need to install a third party agent on the UCX Suite server to monitor it through SNMP.

**Warning**: Imagicle monitoring services only sends SNMP trap services. It does not respond to SNMP inquiries.

Here are the steps to activate the SNMP trap generation and receive them on a SNMP manager:

- **SNMP trap servers**: enter the SNMP manager IP address; if more than one manager must be reached, enter the ip addresses separated by commas. If your system includes a master agent, enter the master agent ip address.
- **SNMP trap community**: it is a common practice to put monitored devices in groups called *communities*. If this parameter does not match the configured community on the monitor, the trap messages could be discarded.

Press Save after the changes.

To enable the third party SNMP monitor to receive the SNMP trap messages from the MAM, youshould download the Imagicle MIB file by pressing "Download SNMP MIB" button, then load it to the SNMP monitor software. Please refer to your SNMP monitor documentation to know how to load the UCX Suite MIB file.

After configuration, whenever an alarm is raised, a SNMP trap is also sent to the SNMP monitor. SNMP traps can be selectively disabled from the Events history web page

Note: if the UCX Suite server fails (for example because of a power outage), no SNMP trap will be generated, because the MAM won't be running.

**Warning:** SNMP traps are sent towards UDP port 162. Please ensure the SNMP manager IP address and port can be reached over the network, and no firewall is blocking the communication.

## Technical details

SNMP OID used for TRAP messages associated to Imagicle alerts are located in the Imagicle branch:

.1.3.6.1.4.1.39801 (.iso.org.dod.internet.private.enterprise.imagicle)

Events are identified as follows, through SNMPv2 OIDs:

39801.2.0.[eventid] (imagicle.suiteEventNotifs.[enterprise-specific].[eventid])

Events include the following additional variables:

39801.1.1 (imagicle.types.eventText) (with a short text description of the events).

## Troubleshooting SNMP trap messages

- When you sent the test TRAP, the result displayed can be misleading. Check that you can actually ping the configured SNMP manager or master agent IP addresses from the UCX Suite server
- Verify that no firewall is blocking outgoing UDP connections FROM the IAS server towards port 162 of the SNMP monitor server
- To generate an actual alarm, please stop one of the licensed Imagicle services (e.g. Imagicle Attendant Console)