imagicle

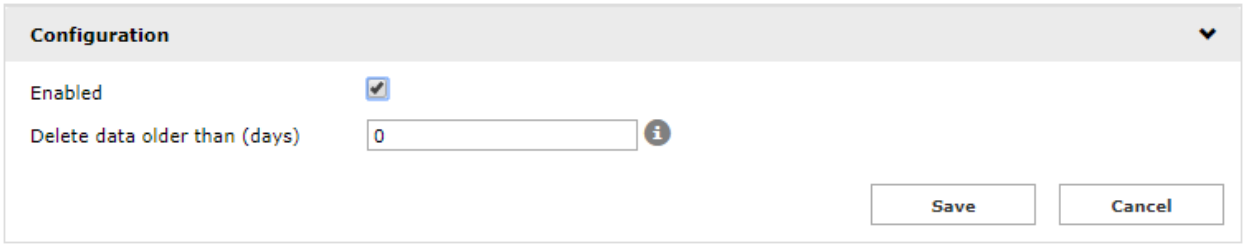
UCX Suite Audit Management

Introduction

Starting from In Spring 2019, a new page has been introduced in order to enable and download Auditing.
This page is accessible only by Users with Complete User Management role, by clicking on Administration â Audit Trail.

Enable UCX Suite Audit

Auditing is disabled by default. It can be enabled accessing the above mentioned page and flagging the related checkbox, then saving.



Once Auditing has been enabled, is it not possible to disable it, for security reasons.

Retention

Data retention (audit events and login/logout events) is performed by an automatic periodic job every 24 hours (not configurable) at 01:30 am (not configurable).
retention period, (maximum time allowed for audit data to be remain stored into the DB) can be configured by web through il Delete data older than (days) parameter in Configuration section into Administration â Audit Trail page.

Login/logout Audit Events

Auditing is tracking all accesses to Imagicle web portal, Imagicle gadgets and Attendant Console, including the following authentication type: SSO, AD/LDAP, CUCM, Windows Integrated, Local user

The login / login failed / logout auditing records the following info:

Audit event	Application	Action	Username	Client IP	Authentication type	Long session
Login from Suite Web portal or gadgets	Suite	User login	the username	client's IP address	the authentication type	true if a long session has been started, false otherwise
Login from Attendant Console	Attendant Console	User login	the username	AC's IP address	the authentication type	false
Login failed from Suite Web portal or gadgets	Suite	User login failure	the username entered for the login attempt	client's IP address	the authentication type	
Login failed from Attendant Console	Attendant Console	User login failure	the username entered for the login attempt	AC's IP address	the authentication type	
Logout from Suite Web portal or gadgets	Suite	User logout	the username	client's IP address		

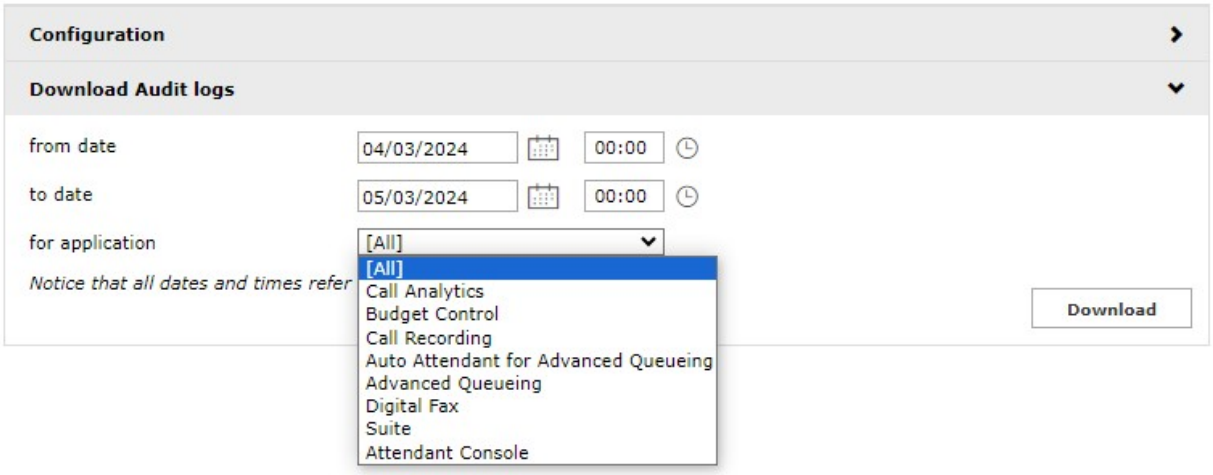
Logout from Attendant Console	Attendant Console	User logout	the username	AC's IP address

Notes

- There is no distinction between login events on the web portal and on the gadgets.
- Only actual logins are traced: no new events are audited if a user accesses the portal/gadget again within the session timeout (i.e. after the first time he doesn't need to log in again)
- Currently no login events are traced for Imagicle One Desktop or Print To Fax.
- Login failure events only track failed attempts for incorrect password, not for invalid user name
- Internal service-to-service authentications are not expected to be present in audit log

Download

In case audit is enabled, a new "Download audit logs" section appears in its configuration page, as per below.



from this page it is possible to download a CSV file containing all recorded audit events, that can be filtered by:

- time
- tenant (only in case of multi-tenant installations)
- applications

CSV file format as follows:

- Application Id: UCX application ID for the event
- Timestamp (Server Time Zone): time when the event occurred
- Username: Username of the event user
- First name: Name of the event user
- Last name: Surname of the event user
- Tenant: Tenant of the event user
- Action: Type of action (i.e. Play recording)
- Client IP: machine IP where the action causing the audit event was made
- UCX Suite Node: node where the action causing the audit event was made
- Details: Details of the particular event. "Details" column format changes according to the specific event (i.e. for an "Un-preserve recording" event the format is as follows:

```
Recording Id {c333d58a-7ba6-4d69-91e4-175816aa5d0b}, Recording PBX Call Id {28787197}, Recording duration {00:00:01.
```

Please note that in case of scheduled reports audit is generated only in case UCX Suite outbound email notifications are enabled and an actual email is sent.