

KAKAPO

SYSTEMS

ABANDONED CALLS GUIDE

CAPTURING ABANDONED CALLS

Unity can capture the CLI of abandoned calls into the call center using the Unity Abandoned Call Logger, which is a cloud service.

This is configured at the Group level in the Unity portal, as shown below:

kakaposystems Details

Broadworks ID: kakaposystems

Business Name: [Empty]

Timezone: (UTC+12:00) Auckland, Wellington

Language: Default

Use Business Name In Client Directory: OFF

Trial Duration (In Days): 1

Use Trial Licenses Until Expiration: OFF

Beta Partner: ON

Allow License Assignment: ON

Call Logging

Call Logger Login ID: [Empty]

Call Logger Password: [Empty]

Connectivity

Replacement OCI Server FQDN: vip.kakaposystems.com

Replacement VoIP Domain: [Empty]

Use OCI protocol over TLS: OFF

OCI over TLS server port: 2209

OCI over TLS certificate host: apps.voice2000.com

OCI over TLS security protocol: TLS 1.2

Use CTI instead of CAP protocol: ON

CTI Server Address: apps.voice2000.com

CTI Port: 8011

Use CTI protocol over TLS: OFF

CTI over TLS server port: 8012

CTI over TLS certificate host: apps.voice2000.com

CTI over TLS security protocol: TLS 1.2

All you need to do is enter the logger details, this will typically be a group or enterprise admin account in BroadWorks, they only need read-only access.

The portal will then instruct the logger engine to connect to that provider and login. It uses the CTI server address of the system provider, as shown below. This must be set or when you try to enter login details at the reseller/group level it will fail.

Once the engine is connected you will see the logging state, as shown below:

The screenshot shows the 'kakaposystems Details' page with various configuration options. The 'Call Logging' section is highlighted with a red box and contains the following information:

- Call Logger Login ID: receptionuser@kakaposystems.com
- Call Logger Password: [Empty field]
- Restart button
- Status: Call logging online since 2020-08-18 @ 06:10:13 GMT

If there was an issue and the engine couldn't automatically reconnect, then you can manually restart the logger instance by clicking the Restart button shown above.

BROADWORKS CALL LOGGER PERMISSIONS

Below are the BroadWorks admin permissions required for the Unity [abandoned] call logger platform.

This is only used to get the group name during setup.

Group Profile Access:

- Full Access to modify group's profile
- Read-Only Access to group's profile
- No Access to group's profile

This is used to load a list of users to include when logging, or when events are received for a previously unknown user. We only need the name, location and department.

User Access:

- Full Access to users
- Restricted from adding or removing users; full access to user profile
- Restricted from adding or removing users; read-only access to user profile
- Restricted from adding or removing users; no Access to user profile
- No Access to users

This is not used by the call logger.

Administrator Access:

- Full Access to add/modify/delete Group and Department Administrators
- Read-Only Access to Group and Department Administrators
- No Access to Group and Department Administrators

This is used to get any parent departments (if nested departments are used) as the user profile only includes the bottom-level department name.

Department Access:

- Full Access to add/modify/delete departments
- Read-Only Access to department list
- No Access to department list

This is not used by the call logger, but 'None' is not an option.

Device Access:

- Full Access to devices
- Read-Only Access to devices; may associate users to existing devices
- Read-Only Access to devices and user associations

This is not used by the call logger, but 'None' is not an option.

Enhanced Services Instance Access:

- Full Access to add enhanced services
- Restricted from adding or removing enhanced services instances; may only modify existing ones

This is used to lookup the FAC description when an event is received, for example when using account codes etc.

Feature Access Code Access:

- Full Access to feature access codes
- Read-Only Access to feature access codes

This is not used by the call logger, but 'None' is not an option.

Phone Number/Extension Access:

- Full Access to phone numbers/extensions
- Read-Only Access to phone numbers/extensions

We don't need to access the CLID number, as this is included in the CTI event for calls.

Calling Line Id Number Access:

- Full access to calling line id number
- Read-only access to calling line id number

Below are the remaining settings required.

Service Access:

- Full Access to assigning resources to the group or users
- Read-Only Access to service assignments

Trunk Group Access:

- Full Access to add/modify/delete trunk groups
- Restricted from adding or removing trunk groups; full access to trunk group resources
- Restricted from adding or removing trunk groups; read-only access to trunk group resources
- No Access to trunk groups

Session Admission Control Access:

- Full access to group session admission control
- Read-only access to group session admission control
- No access to group session admission control

Office Zone Access:

- Full access to user office zone control
- Read-only access to user office zone control

Number Activation Access:

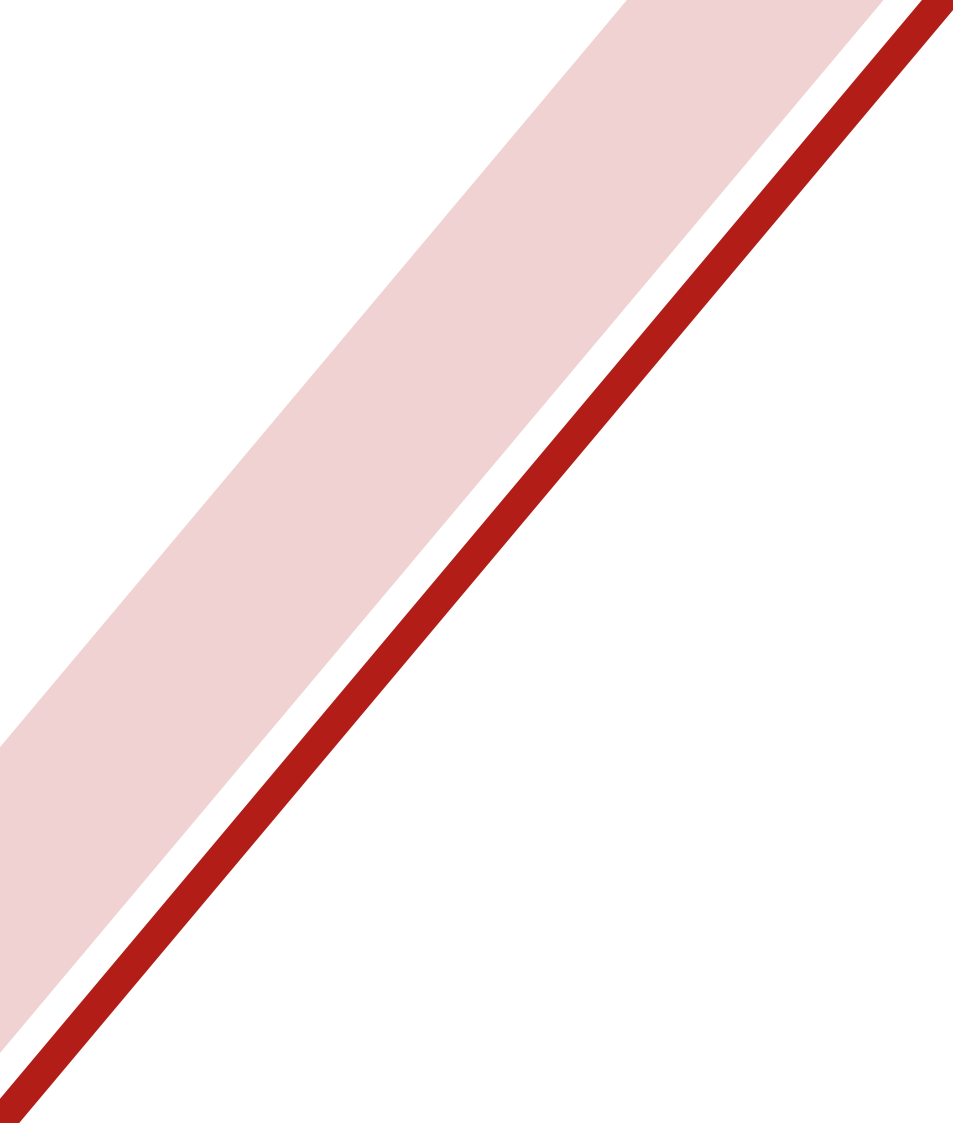
- Full access to number activation
- Read-only access to number activation
- No access to number activation

Dialable Caller ID Access:

- Full access to Dialable Caller ID criteria
- Read-only access to Dialable Caller ID criteria
- No access to Dialable Caller ID criteria

Verify Translation and Routing Access:

- Full access to Verify Translation and Routing
- No access to Verify Translation and Routing



KAKAPO

SYSTEMS

© Kakapo Systems 2023

T +44 (0)207 084 6845

E tellmemore@kakaposystems.com

W www.kakaposystems.com

International House | 36-38 Cornhill | London | EC3V 3NG

FIND US ON  