Logging

Before continuing a POS installation, you must create the logging key used to track log events for the client. This step should be performed by a network administrator – these instructions are for the network admin to follow.

> Most log events generated for a client will be tracked using their specific logging key. An exception to this rule is for events generated by the client's tenant in a cloud installation of Kensium POS, where the logging key is specific to the cloud instance.

a) Log Server

The network admin should login to the Kensium Log server.

> Always use the Kensium password manager to access log server credentials. Do not store or transmit these in files, email or other communications, and do not share your credentials with others.

b) Create Logging API Key

Enter settings and create a new logging API key.

- Title should be the `Organization ID` as entered in the pre-install checklist.
  - This should be lower-case.
  - If deploying a staging site for the client, this can be appended with `STG`.
- Leave Token as `auto-generated`; you will record this value later.
- Leave Permissions as `Ingest`.
- Add an applied property of the format `Site = Title`, e.g. `Site = xmsqa1`.
  - Keep consistent casing! This will help querying for log entries easier. `Site` starts with an uppercase letter, and the organization ID is all lowercase.
  - This will apply a `Site` property to all incoming log entries for the client.

    - This makes it easier to filter only log entries for the specific client.
- Minimum Level should be `Information`.
    - The level can be ***temporarily*** increased to `Debug` to diagnose problems, but should not be kept there as a default as it can result in the creation of millions of log entries over a short period of time.
    - `Verbose` level should never be used, unless required by development to diagnose a specific bug.

c) Record API Key

After creating the new logging key, record the logging API key in the client checklist.