Auth Server

The next steps are to configure the license and devices that are used by the client with the Kensium Authorization server.

a) Authorization Server

Login to the Kensium Authorization server.

- Use your Kensium email address as the username.
- Enter your password.

> Only use your own email address to login to the Authorization server. If you do not have an account, request one from the services administrator. Also, always store your password securely (i.e. in the Kensium password manager).

b) Create Organization

After logging in, you should see the Organizations page. Choose Create New to create a new organization.

- For the ID, enter the client's Organization ID as entered in the pre-install checklist (e.g. xmsqa1).
- For the name, enter, the client's Site Title as entered in the pre-install checklist.

Once the organization is created, choose Manage to continue.

> When creating an organization, the ID you entered is prepended with an *organization group prefix*. Organization groups enable Kensium to separate clients/organizations managed by different resellers and Kensium itself. The fc organization group is for clients managed directly by Kensium.

c) Server License

Create a license for the RMS servers that will be used by the client. This is typically a cloud server, possibly a corporate server, and a server for each store location.

- Name should be RMS Servers.
- Count should indicate the number of servers that are licensed, from the pre-install checklist.
- Expires on should be the license renewal date, as entered in the pre-install checklist.
- Licensed Features should be xms.
- Is Active should be selected.

d) Register License

Create a license for each Windows Register that will be used by the client. This step can be skipped if the client is not using Windows Register integration.

- Name should be Registers.
- Count should indicate the number of registers that are licensed, from the pre-install checklist.
- Expires on should be the license renewal date, as entered in the pre-install checklist.
- Licensed Features should be pos.
- Is Active should be selected.

e) Servers

For each licensed server, create a server record.

- Id should be a unique value for the server.
    - Use only lower-case, alphanumeric characters.
    - The first character should not be numeric.
    - Do not use punctuation.
    - By convention these are:
        - cloud for a Cloud installation of RMS.
        - corp for a Corporate installation of RMS.
        - The lower-case ID of the store.
- Name should be a friendly name for the server, e.g Cloud, Corporate, or the name of a store.
- EndpointUrl is the URL to the server.
    - Always use HTTPS for cloud installations.
    - HTTPS should also be used for corporate and store installations, where IT infrastructure permits.
- LoggingKey is the log server API key for the client.

Saving the server record will add a prefix value to the ID to ensure that the ID is unique across all servers.

f) Server Devices

While server records identify individual cloud, corporate and store servers, we also need to configure *device* records for each server. A device record enables an RMS server to communicate with other RMS servers.

Example server-to-server communications include:

- A Corporate tenant sends purchase records to the Cloud tenant.
- A Store tenant retrieves orders from the Cloud tenant.

When one server attempts to communicate with another server, it passes its device information (and license status) to the other server. The other server validates the license to ensure that it can permit the communications.

The server device settings are:

- Id ***must*** be the same as the ID you entered for the server record.
  - E.g. cloud, corp or the lowercase store ID.
  - Do not include the prefix that the Authorization server adds to the server ID (e.g. use cloud, not fc.myorg.cloud).
- For consistency, Name should be the same as you entered for the server record. This will make it easier for you to match the Server and server Device records.
- License should be set to the RMS Servers license you created above.
- ServerId should be the name of the 'hub' server that the server communicate with.
  - This is normally the Cloud tenant server.
  - If the server does not communicate with other servers, the ServerId should be itself.
  - Review the RMS Deployment Scenarios document to understand server communications.
- LocalServerId should be the name of the local server that the server communicates with, if applicable.
  - This is typically only set for the Store server devices.
  - You should leave this empty for Corporate and Cloud server devices.

The following table summarizes the typical settings for each server device, given the tenant role:

Tenant	(Hub) Server	Local Server
Cloud	Cloud	–

Tenant	(Hub) Server	Local Server
Corporate	Cloud	–
Store	Cloud	Store

> The device ID **must** be the same as the server ID. If the server and device IDs do not match, you will get an error similar to the following in the logs: XMS license token for {Device} is intended for a different server(s).

g) Register Devices

Device records should also be created for each register to communicate with their store server and the 'hub' server.

The register device settings are:

- Id should the register ID.
  - Use only lower-case, alphanumeric characters.
  - The first character should not be numeric.
  - Do not use punctuation.
  - Try to use the register IDs entered in the Kensium database.
- Name should be the register ID as entered in the Kensium database.
- License should be the Registers license you created above.
- ServerId should be the ID of the cloud server.
  - The register uses this server for certain centralized operations, like gift card and member lookups.
- LocalServerId should the ID of the store server.
  - The register uses this server for most communications.