


# AWS Resources

 This section is a technical reference to AWS resources that are shared amongst multiple clients/tenants.

Kensium POS uses AWS resources in two ways:

- Some AWS resources are configured for each organization.
- Other AWS resources are configured to handle multiple organizations - a shared resource - and through its multi-tenant support, the POS software itself partitions usage of the shared resources for each organization.

As some of these resources are shared, they are not governed by a client install checklist. Instead, they are managed by their own checklists.

Before proceeding with a client installation, ensure that you review and understand this topic. In particular, Kensium uses strict naming and configuration conventions to manage the complexity of the AWS environment.

If a client installation requires the provisioning of new shared AWS resources, ensure that you follow the checklist for those resources.

## Production vs QA

While the naming conventions and instructions in this installation documentation applies to both production and non-production AWS services, we ensure that production services are separated from non-production.

Any Kensium POS services that are provisioned for a client's production or staging environments should be created under the POS Production AWS account. This is a clean environment that has access controls for personnel, and should not be used for non-production purposes.

The POS Production account should not host services for:

- QA

- Development
- Demonstrations
- Other applications or hosting (at this time)

## IAM

Do not use AWS root accounts to provision AWS services. Instead, use the IAM account that is created for you:

- Use only your IAM account.
- Do not share the IAM account with another person, or use another person's IAM account.
- Keep your IAM credentials in safe place; do not store or communicate these credentials in files, email, or other messaging.

## Password Manager

Any and all credentials that you create for AWS services must be stored using the Kensium Password Manager.

- Do not share these credentials to other people.
- Do not store or communicate these credentials in files, email, or other messaging.

## AWS Services

- [Virtual Private loud](#)
- [RDS Instance](#)
- [RabbitMQ Instance](#)
- [EC2 Instance](#)
- [Install POS](#)
- [POS Tenant Manager](#)
- [AWS Reference](#)