Manage POS / AWS

AWS Core

Cloud, Corporate, Store

Kensium POS uses Amazon Web Services (AWS) to implement certain features, including cloud-based media gallery, data synchronization, and mobile phone notifications.

These services must be installed and configured properly, for both the organization as a whole and for each POS tenant. Most configuration details are handled automatically through the AWS Provisioning that is run as part of the Setup Guide.

Once AWS services are provisioned, you should ensure the following POS features are enabled on the tenant:

- AWS Core
- AWS S3

AWS settings must also be entered.

> After making changes, run POS Diagnostics to confirm that the new settings are correct.

This is the organization ID of the client, used when configuring the tenant and provisioning AWS services. An example organization ID is xmsqa1.

Kensium POS uses this value to identify various AWS entities that are dedicated to the client.

© 2025 Kensium LLC

[illegible]

These values reflect the access key that was created for the client's IAM user account.

The provisioning process will create an IAM account that is dedicated to the client, and restricts the client POS installations to see only the AWS services and data that is specific to the client.

A Kensium administrator will create and manage access key(s) to the IAM account, which provides programmatic access from POS to the AWS services. The access key information should be entered in these fields.

> Ensure the access keys are for the client's IAM account. Do not enter credentials to an account with higher permissions, such as an admin IAM account.

[illegible]

Enter the AWS Region where AWS services were provisioned for the tenant. An example is us-west-2.

[illegible]

Enter the name of the S3 bucket that was provisioned for the client. POS uses the S3 bucket to store media and sync files.

By default, POS provisions the AWS account to use a bucket name following the format fusion-rms-orgid (e.g. fusion-rms-xmsqa1). The bucket name may be different if you provided an alternate name for the S3 bucket.

[illegible]

Enter the URL to the CloudFront distribution that was provisioned for the client. An example is https://d3e1c7wv8lf5bq.cloudfront.net

> Always use HTTPS for the URL.

© 2025 Kensium LLC



AWS Provisioning

© 2025 Kensium LLC