



KENSIUM
POS



Acumatica



M Comms / RabbitMQ (Provision)



M AWS Core



M Cloud, Corporate, Store

This feature is for development preview only. It is not intended for production, QA, or demonstration at this time.

Kensium POS uses the RabbitMQ message broker to coordinate communication amongst an organization's POS servers and tenants. RabbitMQ Provisioning ensures that the necessary RabbitMQ components are configured to enable this communication.

The provisioning process requires that you enter access and credential information for the RabbitMQ servers that should have been installed along with POS. For instructions on how to install RabbitMQ, see the following topics:

- [AWS \(Hub\) Installation](#)
- [On-site Installation](#)

All tenants will provision components in the hub RabbitMQ server. Additionally, corporate and store tenants also require an on-site (local) RabbitMQ server, and will provision components in that local server.

Most provisioning details are handled by POS automatically. See [RabbitMQ Provisioning](#) for a detailed reference on how the components are provisioned.



You can skip provisioning (e.g. during setup) if you know that provisioning has already

been performed.

However, it is not a problem to run provisioning multiple times.



Local node settings are only shown for corporate and store tenants. Cloud tenants do not communicate with a local RabbitMQ server.



Enter the host name for the local RabbitMQ server. This is localhost if RabbitMQ is installed on the same server as POS, or another host name of a server within the corporate or store LAN.



This value refers to the TCP/IP port where RabbitMQ communications take place. This is typically 5672 but may differ according to your RabbitMQ server settings.



This value refers to the TCP/IP port where RabbitMQ management tasks are performed. This is typically 15672 but may differ according to your RabbitMQ server settings.



Check this value if communications to RabbitMQ should be protected by secure sockets layer (SSL). This is typically unchecked for the local RabbitMQ server, but may differ according to your RabbitMQ server settings.

It's recommended to use SSL on your local network, but this step requires additional configuration of SSL certificates on your local RabbitMQ server.

These credentials refer to your local RabbitMQ administrator username and password. They are used only during provisioning to create the necessary RabbitMQ components, and are not stored outside the provisioning process.

Provisioning creates a non-administrative RabbitMQ user account for the sole purpose of sending messages via the local RabbitMQ server. You must enter a password for this account.

Use the Kensium password manager to generate and record a secure, random password value.

If provisioning detects that the user account already exists, its password will be reset to the value you enter here.

Hub node settings are show for all tenant types, and correspond to the hub RabbitMQ server which are typically installed in the Kensium cloud.

Enter the host name for the hub RabbitMQ server.

This value refers to the TCP/IP port where RabbitMQ communications take place. This is typically 5671 but may differ according to your hub RabbitMQ server settings.

This value refers to the TCP/IP port where RabbitMQ management tasks are performed. This is typically 443 but may differ according to your RabbitMQ server settings.



Check this value if communications to RabbitMQ should be protected by secure sockets layer (SSL). This is typically checked for the hub RabbitMQ server.

It's highly recommended to use SSL for the hub RabbitMQ server, as communication is typically performed over the public internet.



These credentials refer to your hub RabbitMQ administrator username and password. They are used only during provisioning to create the necessary RabbitMQ components, and are not stored outside the provisioning process.



Provisioning uses a non-administrative RabbitMQ user account for the sole purpose of routing messages to and from local RabbitMQ servers via the hub RabbitMQ server. This user account is shared amongst all of your organization's tenants.

You must enter the password for this account.



This option should be selected if this is the first time you are provisioning the hub RabbitMQ server. Selecting this option will ensure that necessary shared components are created, including the user account used for normal communications.

If this option is selected, the password you enter above will be used to create or update this user account's password.

Use the Kensium password manager to generate and record a secure, random password value.



KENSIUM

POS



Acumatica



If provisioning detects that the user account already exists, its password will be **h** to the value you enter here. The changed password is **h** communicated to other tenants that use the original password.

For this reason, you must re-provision and supply the new password to any tenants that are configured with the original password.