Using Custom Licensing for Applications Managed by Horizon Application Manager

VMware Horizon Application Manager simplifies IT by enabling you to manage access to your enterprise's applications from a single portal. Typically, enterprises use a variety of workflow, license management, and back office systems to manage licenses for these applications. With the Application Manager 1.5 release, you can improve the efficiency of your existing license workflows while managing applications centrally from Application Manager. This article describes how to plug your license-management workflow into Application Manager. To integrate per-device licensing for Windows applications captured as ThinApp packages into your license management workflow, also see *Per-User-Device Licensing Using VMware Horizon Application Manager*.

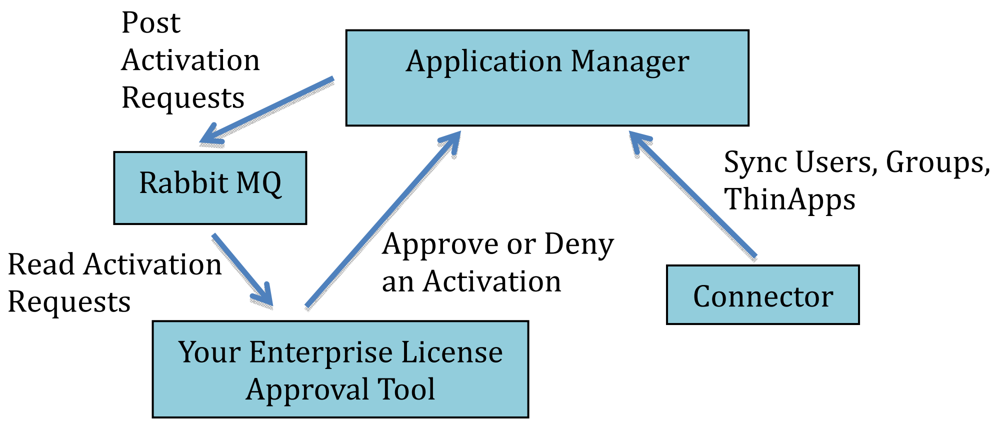
Post Activation Requests
Application Manager
Rabbit MQ
Sync Users, Groups, ThinApps
Approve or Deny an Activation
Read Activation Requests
Connector
Your Enterprise License Approval Tool

Figure 1 – Component Diagram for an Application Manager License Approval Process

High Level Overview

The following list illustrates the sequence of actions that typically take place to activate an application using custom licensing:

1. You, as an organization administrator, enable external licensing for an application.
2. You entitle users or groups to the application.
3. Users view the application in their catalogs and request use of the application.
4. Application Manager posts the activation request as a message to a RabbitMQ queue (For more information on Rabbit MQ server, refer to http://www.rabbitmq.com/)
5. Your custom built license approval tool polls the queue and reads the message, sending the request to your back office system to approve or deny

the request.
This process might include sending an email to the system administrator, posting a SOAP request to a back office system, or other actions.

6. If the license workflow process approves the activation request, the approval tool will approve the request using Application Manager's SDK.
7. Application Manager shows the activated application in users' portals.
8. Users can click the application icon and access or download the application.

Enable External Approvals

To plug in custom licensing, enable external approvals with the Application Manager Administrator Web interface.

Application Manager posts the activation requests to a RabbitMQ queuing server, which is an implementation of the AMQP specification. An AMQP server is message-oriented middleware that you can use to integrate different back office systems. These servers reliably and securely allow publishing and subscribing to messages, message orientation, queuing, and routing.

The Application Manager virtual appliance ships with an installation of RabbitMQ server. This server can be used for trial and initial deployment purposes. For larger installations, you might want to install an external RabbitMQ server and add load balancing and other components.

1. To specify the RabbitMQ server, in the Administrator Web interface, click **Settings** > **Approvals**.

2. Provide information on the Approvals page as follows:
    - **Username** and **Password**. Enter the username and password to connect to the RabbitMQ server. For the RabbitMQ server shipped with the Application Manager virtual appliance, use guest as the username and guest as the password.
    - **Rabbit MQ Address**. Enter the host name or IP address of your RabbitMQ server. If you do not specify a port number, the default port number is used. To use the server installed locally in the Application Manager virtual appliance, enter localhost.
    - **Exchange Name**. For the RabbitMQ server shipped with the Application Manager virtual appliance, leave this text box blank. When left empty, this text box is automatically populated with a default value. Refer to your RabbitMQ server installation to define this attribute, if needed. Exchanges match and distribute messages across queues.
    - **Queue Name**. Enter the queue name defined in the RabbitMQ server. Application Manager posts activation approval requests to this queue. If no queue is specified, a queue with a default name, *HorizonCalloutQueue* is created.

- **Routing Key**. For the local RabbitMQ server, you can leave this text box empty. When left empty, this box is automatically populated with a default value. This attribute is optional and is related to the Exchange Name attribute. Some exchanges might require a routing key to route messages. Refer to your RabbitMQ server installation to define this attribute, if needed.

Enable External Licensing for the Application

1. In the Administrator Web interface, click the **Applications** tab.
2. Click the icon of a SaaS or ThinApp application for which you want to enable external licensing.
3. Click **Edit** in the License Management section.
4. Select External in the Approval drop-down menu to set the license approval policy.

Entitle User or Groups

Entitle users and groups to this application. If you previously entitled users or groups to this application, you might want to remove the entitlements for those users first and then re-entitle them.

User Interaction

When application licensing has been configured, entitled users see the **Request** button on the application icon in the User application catalog. When they click the **Request** button, Application Manager sends the request to the RabbitMQ server.

Build a License Approval Tool

Use the Horizon Application Manager SDK to build a license approval tool.

1. Download the horizon-sdk-1.5.0.zip from the download site.
   This SDK contains the REST API (api folder), REST client (javaClient folder) and a sample license approval tool.
2. Read the `readme.txt` file included in the ZIP file.
3. Obtain the required dependencies
   - If you use maven, you can import the `pom.xml` from the top folder. All the appropriate dependencies are loaded.
   - If you do not use maven, each folder contains a `target/lib` folder that contains all the required dependencies.
4. Verify that your license approval tool does the following:
   - **Connects to RabbitMQ server:** Be aware that for security purposes the default RabbitMQ server included in the Horizon Application Manager virtual appliance server does not accept external requests by default.

     If applicable, enable external requests for the default RabbitMQ server as follows:

    - Access the Application Manager virtual appliance interface.
    - Select **Login** and log in to the Linux operating system.
    - Access the `/etc/sysconfig/rabbitmq-server` file and add/edit the following line:
      ```
      set RABBITMQ_NODE_IP_ADDRESS="0.0.0.0"
      ```
    - Restart the RabbitMQ server with the following command:
      ```
      /etc/rc.d/rabbitmq-server restart
      ```
    - Check the main method in the `RabbitMQUtils.java` file for a sample to connect to the RabbitMQ server.
- **Reads the queue:** For an example, see the `batchConsume` method in the `RabbitMQUtils.java` file in the included sample. Each message in the queue contains the details in JSON format. The JSON data includes operation type (activation for activation request or deactivation when a user is no longer entitled to the application), a unique identifier for the request, application details, and user details as follows:

  ```
  {"operation":"activation",

  "requestId":"c5fa602d-739a-4832-a378-
  c429a70a1d11",

  "applicationId":"1011",
  "applicationName":"AdAware",

  "userId":"224",
  "userName":"denise",
   }
  ```

- **Connects to Horizon Application Manager:** The SDK uses OAuth based authentication to connect to Application Manager. You must get a `clientId` value and `clientSecret` value from Application Manager and store it for future use. Hardcoded usernames and passwords are not used. As an administrator you can revoke these OAuth clients if you suspect misuse.

  Get the `clientId` value and `clientSecret` value by configuring an identity provider in Application Manager:

    A. In the Application Manager Administrator Web interface, Click the **Settings** tab and then click **Identity Providers**.
    B. Click **Add Identity Provider**.

C. Enter a provider name and description and click **Save**. Application Manager displays an activation code.

D. Use this activation code in your license approval tool to generate `clientId` and `clientSecret` values, using the `RestClient.java` in SDK. For example:

```
ConnectorActivationDetails testCad =
restClient.activateConnector(activationCode
);

String client_id =
testCad.getOauth2ClientId();
String client_secret =
testCad.getOauth2ClientSecret();
```

- For subsequent requests to Application Manager, login using the `clientId` and `clientSecret` parameters

  ```
  OAuth2AccessToken accessToken =
  restClient.generateAccessTokenWithClien
  tCredentials(client_id, client_secret);

  userSession
  =restClient.loginWithAccessToken(access
  Token);
  ```

- Approve or deny the activation request. For example:

  ```
  CalloutService callouts =
  userSession.createCalloutServiceProxy()
  ;

  CalloutResponse response = new
  CalloutResponse("<requestId>", true, "
  approving request as it has been
  approved by back office system");

  callouts.updateApprovalWithResponse(res
  ponse);
  ```