Paris Customer Service Management

Last updated: July 10, 2021

Some examples and graphics depicted herein are provided for illustration only. No real association or connection to ServiceNow products or services is intended or should be inferred.

This PDF was created from content on docs.servicenow.com. The web site is updated frequently. For the most current ServiceNow product documentation, go to docs.servicenow.com.

If you have comments about this documentation, submit your feedback to: docfeedback@servicenow.com

Company Headquarters
2225 Lawson Lane
Santa Clara, CA 95054
United States
(408)501-8550

PDF generated on July 10, 2021

Install Vaccine Administration Management

Vaccine Administration Management (VAM) is available on the ServiceNow Store.

Before you begin

Vaccine Administration Management requires the ServiceNow® Customer Service Management Professional application, the Appointment Booking plugin (com.snc.appointment_booking). The Virtual Agent plugin (com.glide.cs.chatbot) can optionally be installed to enable chatbot conversations in the self-service portal.

If you don't have a Customer Service Management Professional license, contact your ServiceNow account representative.

Note:

- The customer is responsible for configuring the implementation to meet local compliance rules, regulations, and laws.
- If your instance is already set up to use encryption contexts for column-level encryption, migration is required to use encryption modules. Contact Now Support for assistance with the migration.
- Customers can use column-level encryption (CLE), (CLE + KMF), or a third-party encryption solution at no additional cost.
- For further details on installing CLE with Encryption support for Vaccine Administration Management, see Installing CLE with Encryption support for VAM [KB0952557].

  Note: Records under the sys_platform_encryption_configuration table are added as part of VAM that encrypts fields which contain sensitive data. But these records must be activated to enable encryption on the corresponding fields.

Role required: admin

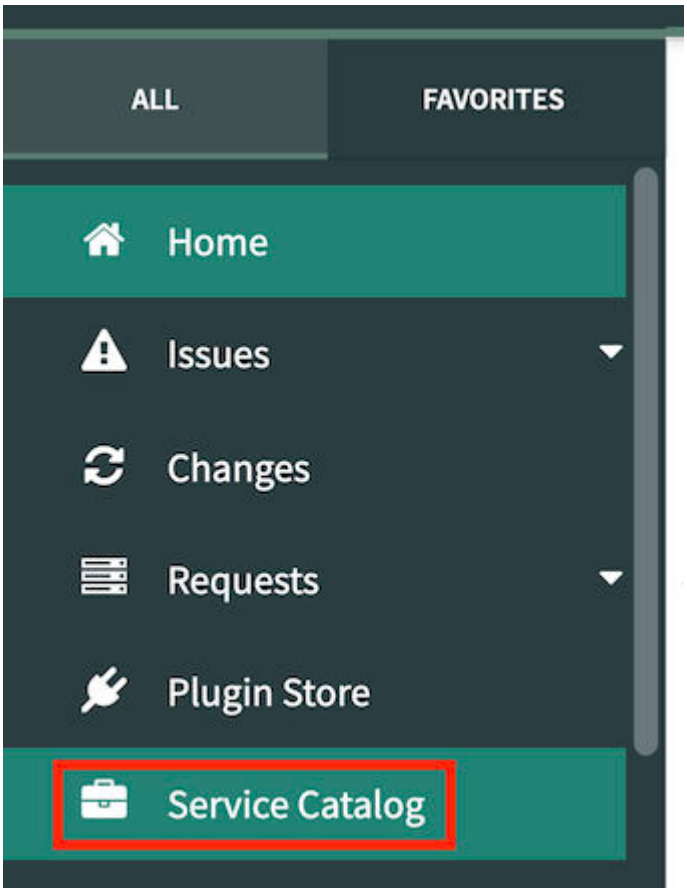
Procedure

1. Navigate to **System Applications > All Available Applications > All**.

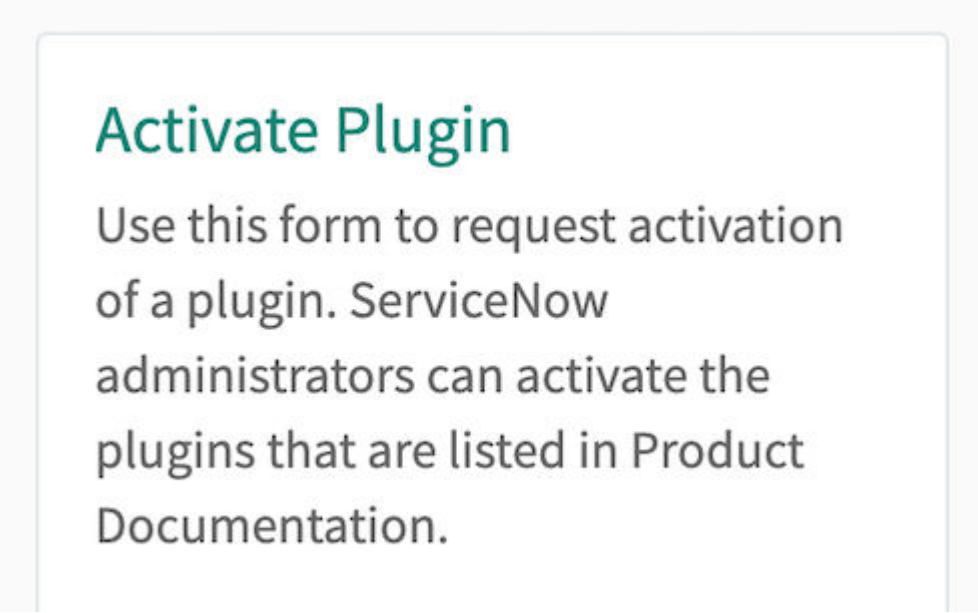
2. Search for `Vaccine Administration Management`.
3. Click **Install**.

   The Application installation dialog box opens.
4. Click **Activate**.

   Note: The customer is responsible for configuring the implementation to meet local compliance rules, regulations, and laws, including to address protecting sensitive data on its production and non-production instances. This Vaccine Administration Management app is designed to utilize the CLM and KMF encryption that is enabled by installing the plugin. The customer may determine that it desires to skip this step for its instances that do not contain sensitive data (such as an instance for testing that contains only dummy data).
5. Navigate to **System Definition > Plugins**.
6. Check whether the Encryption Support plugin (com.glide.encryption) is activated. If not, click **Install**.
7. Enable Key Management Framework and column-level encryption.
   a. Go to Now Support and click **Service Catalog** in the menu.



b. Click **Activate Plugin**.



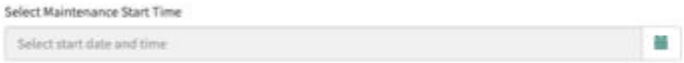
c. In the **What is your target instance** field, specify your instance.

d. Select **Plugin I'm looking for is not listed**.

e. Under **Specify the name of the plugin**, enter `Key Management Framework plugin (com.glide.kmf.global).`

f. In the **the Reason/Comments** field, state that you need the Key Management Framework plugin (com.glide.kmf.global) for Vaccine Administration Management.

g. In the **Select Maintenance Start Time** field, select a start date and time value.



h. Click **Submit**.

8. Contact Customer Service and ask them to set the **glide_encryption.cle_replatforming_with_kmf** property to **opt_in**.

9. If you're using the CLE and KMF plugins, generate a key so that fields can be encrypted.

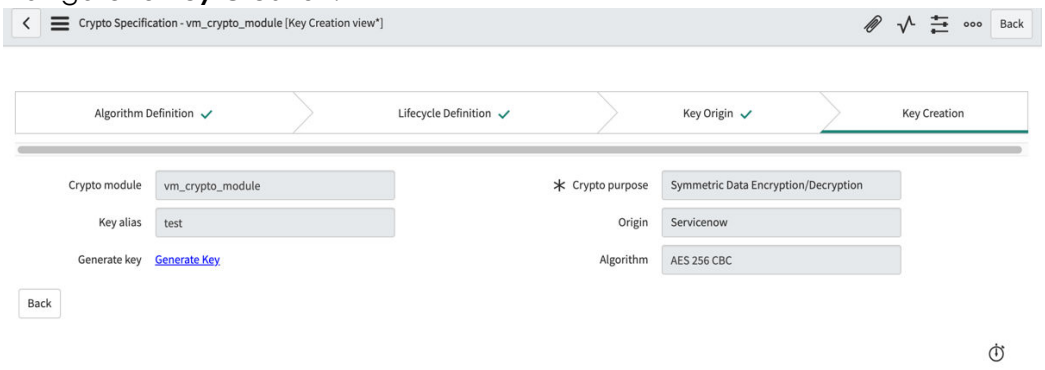
   Important: Make sure that the admin has the sn_kmf.cryptographic_manager role to get access to the required tables.

   a. Navigate to **Key Management > Cryptographic Modules > All**.

   b. Click the sn_vaccine_sm.vm_crypto_module crypto module record.

   c. In the Crypto Specifications related list, click the first crypto specification record.

   d. Navigate to **Key Creation**.



   e. Click **Generate Key**.
   A key is created in the Module Keys related list on the sn_vaccine_sm.vm_crypto_module crypto module record.

   Note: To view the fields that are encrypted, navigate to **System Security > Field Encryption > Encrypted Field Configurations**.

   Important: The admin must have elevated roles to access the Field Encryption menu.

   You can encrypt additional data fields based on your requirements and configurations. For information about additional encryption capabilities including edge encryption, database encryption, and full disk encryption, see the Data encryption white paper.