AppViewX

Symantec Migration Workflow Guide

Trademarks

Contact Information

AppViewX, Inc.
500 Yale Avenue North, Suite 100
Seattle, WA 98109
Tel: +1 (206) 207 7541
Email: info@appviewx.com
Web: www.appviewx.com

Document Information

Software Version: 12.3.0

Document Version: 1.1

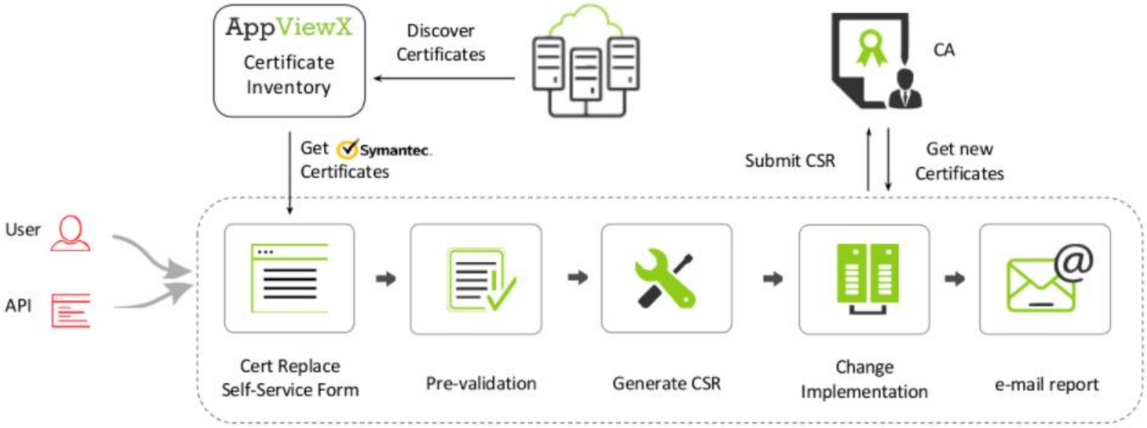
Last updated on: April 06, 2018

Contents

Description

The Symantec Migration workflow will migrate the Symantec certificate to the other CAs such as DigiCert, Entrust, Trustwave, and Comodo certificate manager, which are currently managed in the AppViewX instance. You can migrate up to 10 Symantec certificates using a single request.

The flow diagram of Symantec Migration workflow is shown in the image below:



Prerequisites

To run this workflow, ensure that the following pre-requisites are met:

- Free AppViewX or AppViewX version 12.3.0 has been downloaded and installed.
- The Symantec certificate must be discovered and managed in the AppViewX.
- The DigiCert, Entrust, Trustwave, and Comodo certificate manager accounts are configured on AppViewX.
- Each CA must have the appropriate credentials.
- The SMTP is configured in AppViewX for sending emails.
- “Approval required” parameter in the policy of the selected Certificate group must be unchecked for the auto-implementation of this workflow.

Compatible Software Versions

The automation temple has been tested and validated on the following software versions:

- AppViewX – Free AppViewX and AVX 12.3.0
- CAs - DigiCert, Entrust, Trustwave, and Comodo certificate managers

Limitations

- App connector will not handle duplicate certificate for the same CA and CA cert type.
- The inputs to generate the CSR may differ for Symantec and the migrated CA.
- In a single request, up to 10 Symantec certificates can be migrated.

Log In to AppViewX

Log in to the AppViewX web interface. The standard format for a login URL is:

`https://hostname:portnumber`.

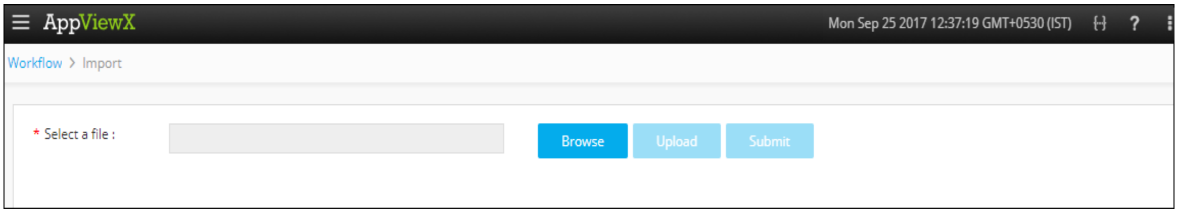
The hostname and port number are configured during deployment, with the default port number set to `5004` and the default web credentials set to `admin`/`AppViewX@123`.

Note: It is recommended that you access AppViewX using Internet Explorer, Firefox, or Google Chrome.

Import Visual Workflows

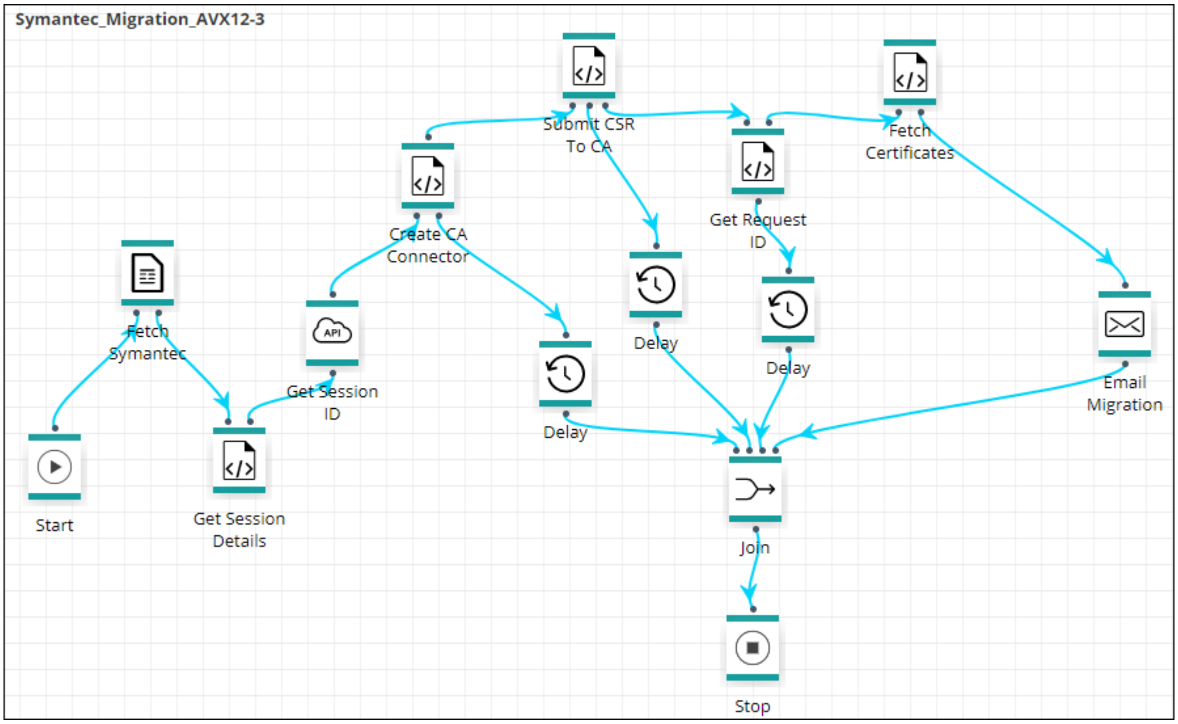
Note: Free AppViewX comes preloaded with visual workflows. You will only need to use the following import instructions when newer versions of the workflows are available.

1. Click the ☰ (**Menu**) button.
2. Navigate to **Workflow > Studio**.
3. Click the ⤓ (**Import**) button in the Command bar.



4. To import a workflow, complete the following steps:
    a. Click the **Browse** button.
    b. Select the zip file containing one or more workflows, then click **Upload**.
    c. In the table at the bottom of the *Import* page, select the check box beside the unzipped workflow file.
    d. Click **Submit** to deploy the workflow into your AppViewX environment.

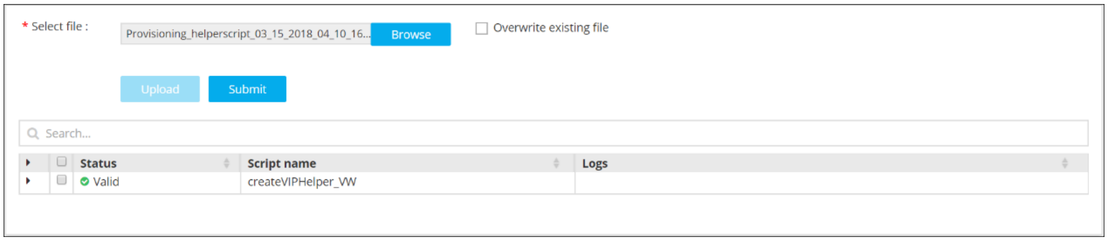
The Symantec Migration workflow is shown in the image below:



Import Helper Scripts

Note: Free AppViewX comes preloaded with helper scripts. You will only need to use the following import instructions when newer versions of the helper scripts are available.

1. Click the ☰ (**Menu**) button.
2. Navigate to **Workflow > Studio**.
3. Click on the </ (**Helper script**) button in the Command bar. The *Helper script library* screen appears.
4. Click the ⤓ (**Import**) button.
5. Click **Browse** and select the helper script zip file you want to import.
6. Click **Upload** to import the file and view its contents.



* Select file : Provisioning_helperscript_03_15_2018_04_10_16... Browse ☐ Overwrite existing file

Upload Submit

Search...

	☐	Status	Script name	Logs
▸	☐	✓ Valid	createVIPHelper_VW	

Note: Select the checkbox **Overwrite existing file**, only if the names of the new script file that you are trying to upload and the existing script file are the same.

7. In the table at the bottom of the *Import* page, select the check boxes beside each of the helper scripts.
8. Click **Submit** to deploy them into your AppViewX environment.

Discover a Certificate

The Discover function allows you to search for and display the list of all available certificates within the network of an organization in order to manage it in the AppViewX certificate inventory.

To discover a certificate by IP range, complete the following steps:

1. Click the ☰ (**Menu**) button.
2. Navigate to **Inventory** > **Certificate**.

   The ***Certificate*** screen opens.
3. If the **Server** tab is not displayed by default, click to open it.
4. Click the (**Discover**) button in the Command bar.

   The related screen opens with the **Discovery** tab selected by default.

   Note: To schedule a certificate discovery, click the **Scheduler** tab and do the following.
5. Click the ⊞ (**Create**) button in the Command bar.
6. Select the **On-demand** or **Schedule** radio button based on how you want to discover the certificates.
7. In the **Name** field, enter a name that clearly identifies the certificate discovery action that you are setting up.
8. (Optional) In the **Description** field, enter a description for the key discovery that makes it easy for a user to immediately determine when the key discovery is scheduled to take place.
9. (*Only necessary if you selected Schedule in Step 6*) From the **Occurrence** type dropdown list, select one of the following frequency for the certificate discovery process: **daily**, **weekly**, **monthly**, or **yearly**.

   The remaining fields in the Scheduler region populate depending on what you select here. At a minimum, complete all fields designated with a red asterisk (*) beside their names.

   Note: The time and date fields displayed next will depend on the selected option. For recurring discoveries, select the start and end dates that you want key discovery to begin and end respectively.
10. In the **Discover By** field, select the method by which you want to discover the certificates:
    - IP range
    - Subnet
    - URL
    - Upload
    - Managed ADCs
    - Managed Servers
    - Certificate Authorities

    The fields that appear will vary based on the discovery source you selected.
11. At a minimum, complete all fields designated with a red asterisk (*) and click Add.
12. To add all the details automatically, click the **Upload** button and navigate to the location of the file, then select it.

13. Click **Open**.

    This retrieves and displays all the details in the table at the bottom.
14. From the **Certificate group** dropdown list, select the group to which the discovered certificates must be associated.
15. Depending on how you want the status of the certificates to be displayed when they appear in the inventory, select one of the following radio buttons:
    - Do not move
    - Managed
    - Monitored
16. Click **Discover** to discover all certificates that match the criteria you entered.

Configure Certificate Manager Accounts

To configure DigiCert, Entrust, Trustwave, and Comodo certificate manager accounts, complete the following steps:

1. Click the ☰ (**Menu**) button.
2. Navigate to **Inventory > Certificate**.

   The ***Certificate*** screen opens.
3. If the **Server** tab is not displayed, click to open it.
4. Click the ⚙ (**Settings**) button in the Command bar.
5. The ***Settings*** screen opens, listing each certificate authority (CA) available in AppViewX in the left-hand column.
6. Click the vendor name for which you want to add a certificate manager account.

   Note: Click each vendor name to view the list of certificate manager accounts it contains. You can edit those accounts if required.
7. On the *Certificate authority* screen that appears, click the **Configure now** button or + (**Add**) button.
8. At a minimum, complete all fields designated with a red asterisk (*).
9. Click **Save**.
10. (Optional) Repeat steps 6-9 for any other vendors for whom you want to create certificate manager account details.

Configure the SMTP

To configure an SMTP server, complete the following steps:

1. Click the ☰ (**Menu**) button.
3. Navigate to **Settings** > **General** > **SMTP**.
4. In the **SMTP host** field, enter the host address of the SMTP server.
5. In the **SMTP port** field, enter the port number for the SMTP server.
6. In the **From address** field, enter the email address from which the notification must be sent.

7. If an SMTP server requires authentication to connect, click the (**Disabled**) button to enable it.
8. If you enabled authentication in Step 7, enter the user name and password that is used for authentication on the SMTP server.
10. In the **Send email to** field, enter an email address you want to use to test the configuration, then click **Test**. If the configuration is successful, a test email will be sent to this address verifying that everything is working correctly.
11. Click **Save** to save the changes you have made to the system settings.

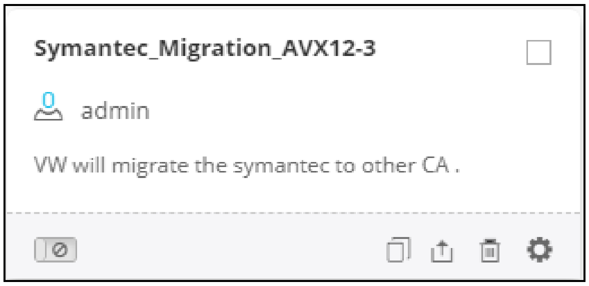
Enable a Workflow

To enable the Symantec Migration workflow, complete the following steps:

1. Click the ☰ (**Menu**) button.
2. Navigate to **Workflow** > **Studio**.

   The *Workflow* screen opens.
3. Click the □ (**Select**) button on the Symantec Migration workflow to enable. If the workflow is already selected, a ☑ (**Deselect**) button appears.
4. Click the 🔒 (Enable) button in the Command bar.

   Note: You can also enable the Symantec Migration workflow from the Card view by clicking the ⊘ (**Disable**) button.



Symantec_Migration_AVX12-3 □

admin

VW will migrate the symantec to other CA .

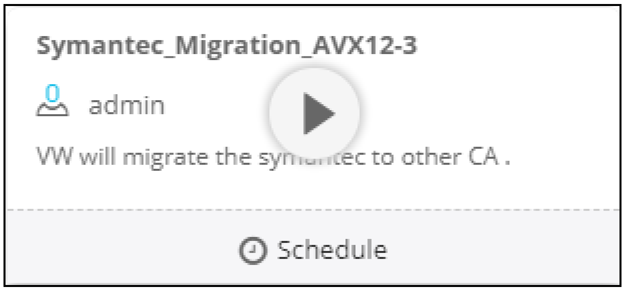
5. On the *Confirmation* screen that appears, click **Yes**.

Symantec Migration Workflow

To submit the Symantec Migration workflow, complete the following steps:

1. Click the ☰ (**Menu**) button.
2. Navigate to **Workflow** > **Request**.

   The *Request* screen opens with **My catalog** tab displayed by default. This screen displays all enabled workflows assigned to a specific user role.
3. Click the Play button on the Symantec Migration workflow to execute.

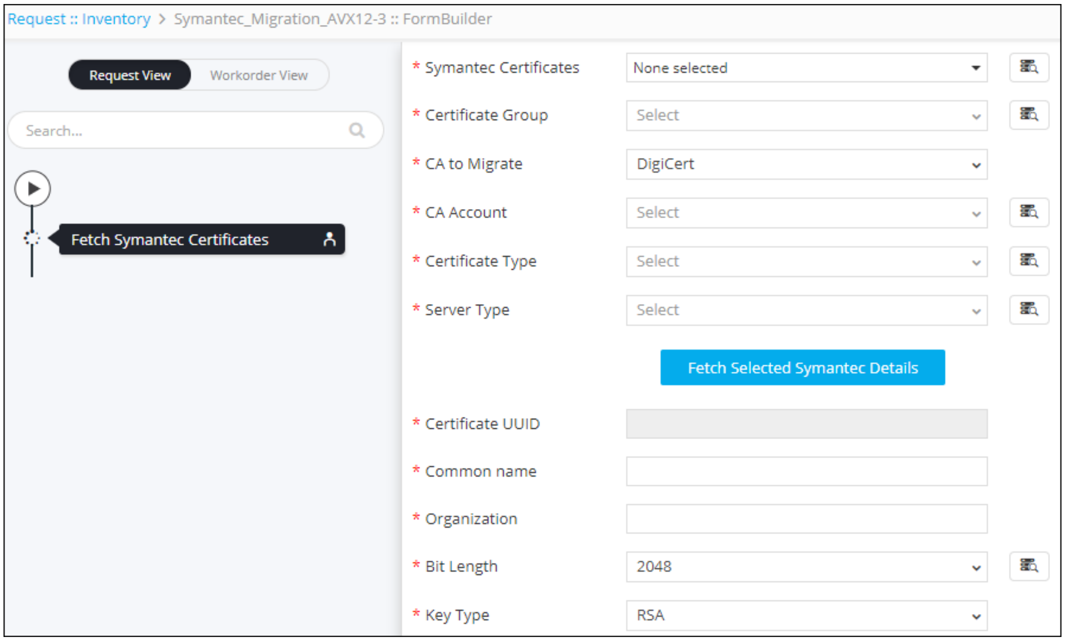


Symantec_Migration_AVX12-3

admin

VW will migrate the symantec to other CA .

4. The *Form Builder* screen opens with the **Request View** tab displayed by default.



Request :: Inventory > Symantec_Migration_AVX12-3 :: FormBuilder
Request View
Workorder View
Search...
Fetch Symantec Certificates
Fetch Selected Symantec Details

* Symantec Certificates	None selected
* Certificate Group	Select
* CA to Migrate	DigiCert
* CA Account	Select
* Certificate Type	Select
* Server Type	Select
* Certificate UUID	
* Common name	
* Organization	
* Bit Length	2048
* Key Type	RSA

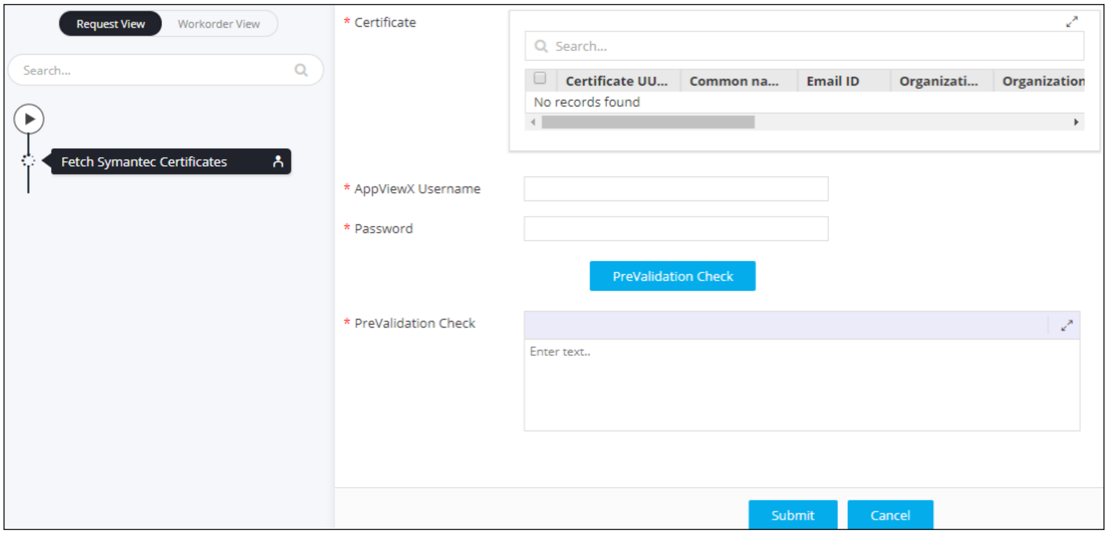
5. In the **Symantec Certificates** field, retrieve the list of Symantec certificates managed in AppViewX by clicking the (**Retrieve field values**) button and select the certificates that must be migrated.

   Note: It is recommended that you select only up to 10 certificates. Though this workflow has been limited to migrate only 10 certificates, Workflow is capable of migrating more certificates in one request.

6. In the **Certificate Group** field, retrieve the list of certificate groups available by clicking the (**Retrieve field values**) button and select the certificate group to which the migrated certificates must be assigned to.
7. In the **CA to Migrate** dropdown field, select the CA to which the selected Symantec certificates must be migrated.
8. In the **CA Account** field, retrieve the list of CA accounts available by clicking the (**Retrieve field values**) button and select the CA account with appropriate credentials, which will be used to create new certificates.
9. In the **Certificate Type** field, retrieve the list of certificate types based on the selected CA by clicking the (**Retrieve field values**) button and select the required certificate type.

10. In the **Server Type** field, retrieve the list of server types based on the selected CA by clicking the (**Retrieve field values**) button and select the required server type.
11. Click the **Fetch Selected Symantec Details** button to retrieve the certificate information selected in step 4 and load it in the table in **Certificate** field.

    Note: In the **Certificate** field, you can delete or modify the certificate details by selecting the check box beside the certificate UUID in the table and then clicking either the (**Update**) or (**Delete**) button.



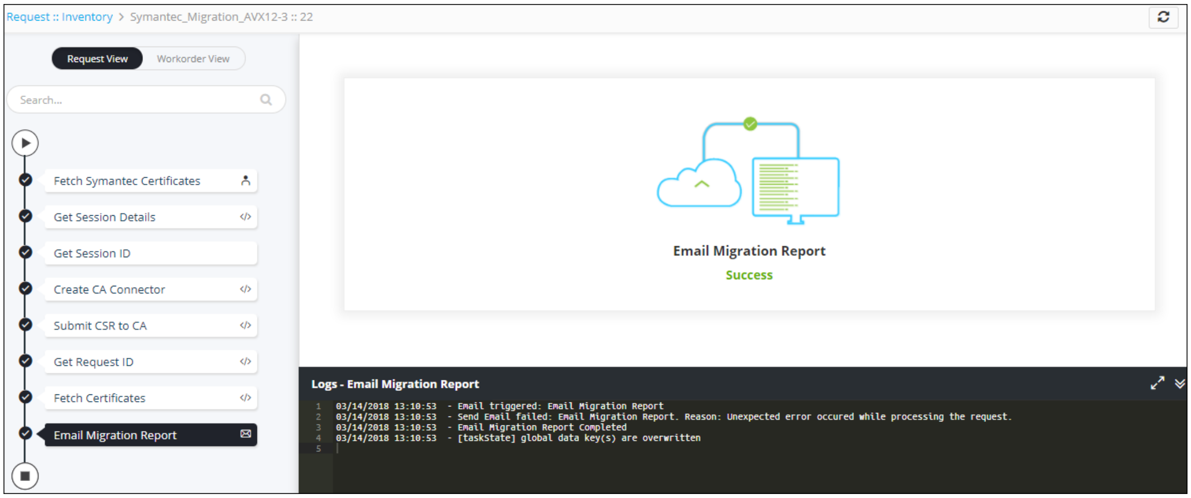
12. In the **AppViewX Username** and **Password** fields, enter the user name and password respectively for AppViewX Web login.
13. Click the **PreValidation Check** button to ensure the following:
    a. Only 1 to 10 Symantec certificates are selected for migration.
    b. Validity of the selected CA and certificate type are within the allowed range.
    c. The required information is provided for each certificate that is being migrated.

    The result of this validation is displayed in the **PreValidation Check** field.
14. Click **Submit** to trigger the workflow immediately.

WorkOrder flow

The following are the workorder tasks of Symantec Migration workflow.

Note: You can click each task to view its details. Wherever applicable, all logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.



```
03/14/2018 13:10:53  - Email triggered: Email Migration Report
03/14/2018 13:10:53  - Send Email failed: Email Migration Report. Reason: Unexpected error occured while processing the request.
03/14/2018 13:10:53  - Email Migration Report Completed
03/14/2018 13:10:53  - [taskState] global data key(s) are overwritten
```

1. **Fetch Symantec Certificates —** The Symantec certificate details are retrieved after they are enrolled successfully.
2. **Get Session Details —** The session details and ID will be generated to issue the required API commands.
3. **Get Session ID —** The session ID is retrieved for issuing API commands for creating CA connector, submitting CSR to CA, and checking the work order status.
4. **Create CA Connector —** The CA connectors for the new certificates with common names are created.
5. **Submit CSR to CA —** The CSR is created and submitted to the CA
6. **Get Request ID —** The request ID of the triggered workflow is retrieved.
7. **Fetch Certificates —** After successful completion of workflow execution the certificates are retrieved from the corresponding CA.
8. **Email Migration Report —** An email is sent to the administrator with the status, common name, and request ID of the migration.

Rollback a workflow

A rollback action can be performed only on the completed workflows. To trigger a rollback action, complete the following steps:

1. Click the ☰ (**Menu**) button.
2. Navigate to **Workflow** > **Request**.

   The *Request* screen opens with **My catalog** tab displayed by default.
3. Click the **Request Inventory** tab.

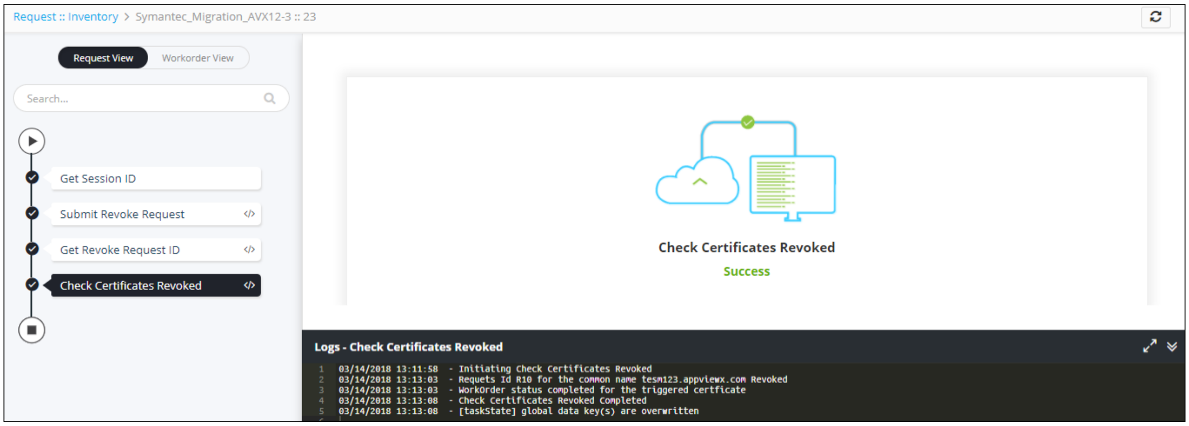
   This displays all workflows that have been triggered. On the **Request Inventory** screen, you can search for a request created for Symantec Migration workflow using the **Search** field and/or click the (**Filter**) button.
4. Right-click the request and select **Rollback**.
5. On the Confirmation screen that appears, click **Yes**.

6. Select the **Request** or **Workorder** radio button based on how you want to set the rollback type.
7. Click **Rollback** to trigger the action.

WorkOrder flow

The following are the workorder tasks of Symantec Migration workflow, when you perform a rollback action:

Note: You can click each task to view its details. Wherever applicable, all logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.


Request :: Inventory > Symantec_Migration_AVX12-3 :: 23
Request View
Workorder View
Search...
Get Session ID
Submit Revoke Request
Get Revoke Request ID
Check Certificates Revoked
Check Certificates Revoked
Success
Logs - Check Certificates Revoked

```
03/14/2018 13:11:58  - Initiating Check Certificates Revoked
03/14/2018 13:13:03  - Requets Id R10 for the common name tesm123.appviewx.com Revoked
03/14/2018 13:13:03  - WorkOrder status completed for the triggered certficate
03/14/2018 13:13:08  - Check Certificates Revoked Completed
03/14/2018 13:13:08  - [taskState] global data key(s) are overwritten
```

1. **Get Session ID —** The session ID is retrieved for issuing API commands for revoking the certificates.
2. **Submit Revoke Request —** The request to revoke the enrolled certificate is created and submitted to the corresponding CA**.**
3. **Get Revoke Request ID —** The request ID of the triggered workflow is retrieved
4. **Check Certificates Revoked —** The enrolled certificate will be revoked and a validation is done to check the workflow status.

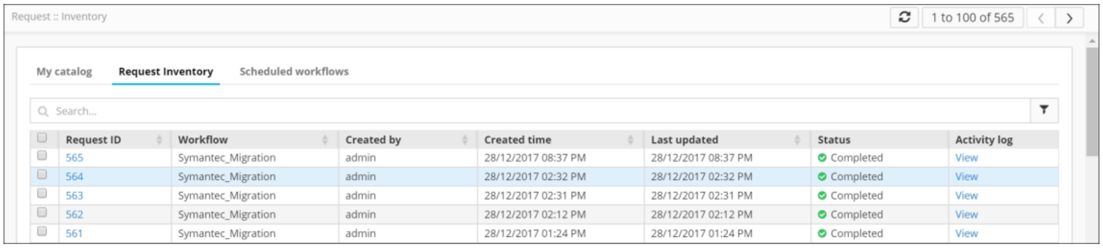
Request Inventory

To go to the Request inventory, complete the following steps:

1. Click the ☰ (**Menu**) button.
2. Navigate to **Workflow** > **Request**.

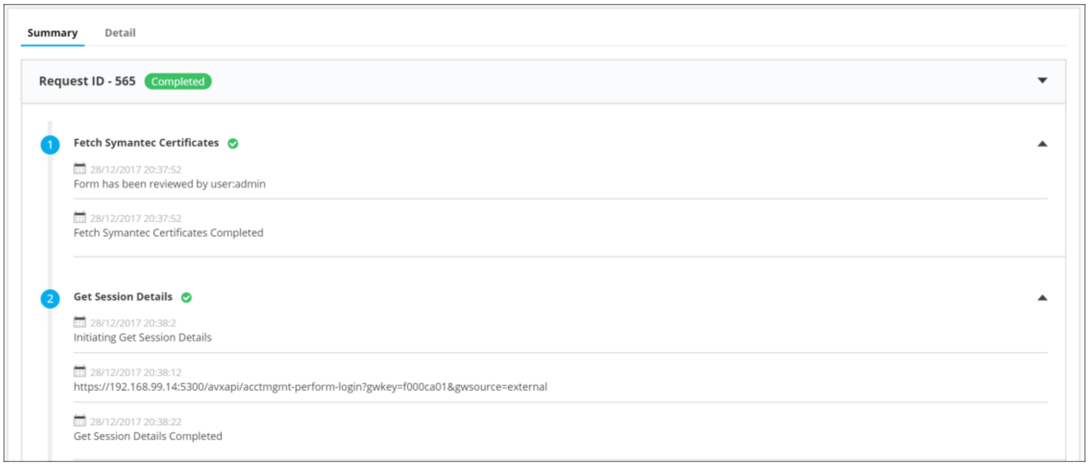
   The *Request* screen opens with **My catalog** tab displayed by default.
3. Click the **Request Inventory** tab.

   This displays all workflows that have been triggered. On the **Request Inventory** screen, you can search for a request using the **Search** field and/or click the ⏷ (**Filter**) button to select the options you want to use to sort the requests.



□	Request ID	Workflow	Created by	Created time	Last updated	Status	Activity log
□	565	Symantec_Migration	admin	28/12/2017 08:37 PM	28/12/2017 08:37 PM	✓ Completed	View
□	564	Symantec_Migration	admin	28/12/2017 02:32 PM	28/12/2017 02:32 PM	✓ Completed	View
□	563	Symantec_Migration	admin	28/12/2017 02:31 PM	28/12/2017 02:31 PM	✓ Completed	View
□	562	Symantec_Migration	admin	28/12/2017 02:12 PM	28/12/2017 02:12 PM	✓ Completed	View
□	561	Symantec_Migration	admin	28/12/2017 01:24 PM	28/12/2017 01:24 PM	✓ Completed	View

4. Click the **Request ID** created for Symantec Migration to view its details. The screen opens with the **Request View** tab selected by default.
   a. After the workflow execution is complete, the **Request View** tab displays the tasks or phases of a request in a tree view. For more details, refer to the WorkOrder flow section of this guide.
   b. Click the **Workorder View** tab to view the work order details such as work order ID, date and time when the work order was created and updated, status, RFC ID, and RFC status.
5. In the *Request Inventory* screen, you can also view the following details of the request: request creator, request time, last updated time, status, and activity log.
6. Click the **View** link in the **Activity log** column to display the request in a stage view. In the **Summary** tab, click the ▼ (**Expand**) icon to view the details of each task. Click the **Details** tab to view log messages and other particulars of a request.



Fetch Symantec Certificates ✓

28/12/2017 20:37:52
Form has been reviewed by user:admin

28/12/2017 20:37:52
Fetch Symantec Certificates Completed

Get Session Details ✓

28/12/2017 20:38:2
Initiating Get Session Details

28/12/2017 20:38:12
https://192.168.99.14:5300/avxapi/acctmgmt-perform-login?gwkey=f000ca01&gwsource=external

28/12/2017 20:38:22
Get Session Details Completed

Schedule a Workflows

To schedule a workflow, complete the following steps:

1. Click the ☰ (**Menu**) button.
2. Navigate to **Workflow** > **Request**.

   The *Request* screen opens with **My catalog** tab displayed by default.
3. Click the 🕒 (**Schedule workflow**) button on the Symantec Migration workflow.
4. On the Symantec Migration window that opens, select the frequency of the policy migration process: once, hourly, daily, weekly, monthly, or yearly. The remaining fields in the Scheduler region update depending on what you select.
5. Click **Save**.

View Scheduled Workflows

To go to the scheduled workflow screen, complete the following steps:

1. Click the ☰ (**Menu**) button.
2. Navigate to **Workflow** > **Request**.
3. The *Request* screen opens with **My catalog** tab displayed by default.
4. Click the **Scheduled workflows** tab.
5. On the Scheduled workflow screen that appears, you can perform the following tasks:
   - In the **View log** column, click **View** to display the details of a scheduled workflow.
   - Click the ⏸ (Pause) or ▶ (Resume) button to temporarily stop or continue the execution of a workflow.

Troubleshooting

I cannot find the Symantec Migration workflow in the Request Catalog

You must enable the workflow from the Studio section. For more details on how to enable a workflow, refer to the Enable a Workflow section of this guide.

The Symantec certificates are not fetched

You must ensure the Symantec certificates are discovered and added in the AppViewX inventory as managed certificates. Also, check if your user account has the required access permissions defined in RBAC to manage the Symantec certificates.

The CA accounts are not fetched

You must create the CA accounts to fetch them. For more details on how to configure the CA accounts, refer to Configure Certificate Manager Accounts section of this guide.

The pre-validation check fails

Select the certificate to check all the required inputs to generate the new CSR are passed. Additional inputs are required to generate CSR for few CA's. You must select less than 10 certificates for migration in single request.

The certificate migration to the new CA fails

Check if the selected CA account has enough credits to create new certificates for migration. Ensure the AppViewX instance can communicate with external CA's.