Symantec Migration Workflow Guide

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: 12.2.0

Document Version: 1.0

Last updated on: January 08, 2018

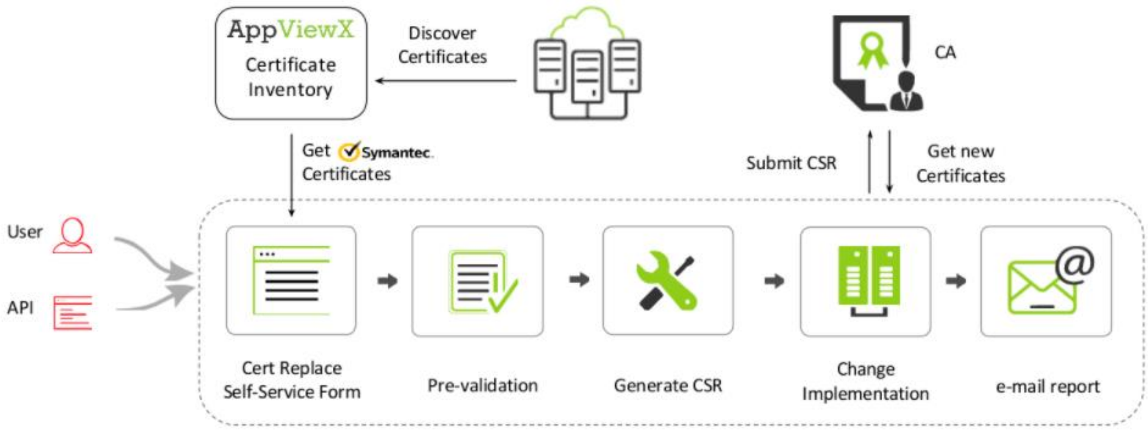
Contents

Description 1
Prerequisites 1
Compatible Software Versions 1
Log In to AppViewX 2
Import Visual Workflows 2
Import Helper Scripts 2
Enable a Workflow 3
Discover a Certificate 3
Configure Certificate Manager Accounts 4
Configure the SMTP 5
Symantec Migration Workflow 6
WorkOrder flow 7
Request Inventory 7
Schedule a Workflows 8
View Scheduled Workflows 8
Troubleshooting 9

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:

- 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:

- AVX 12.2.0
- 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.`

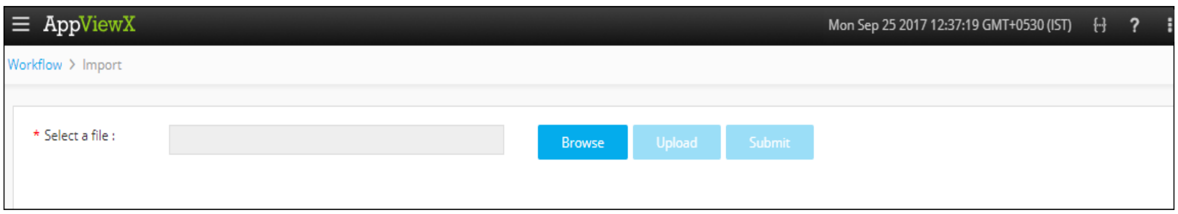
The hostname and port number are configured during deployment, with the default port number set to `5004` and the default web credentials set to `admin`/`AppViewX@123`.

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

Import Visual Workflows

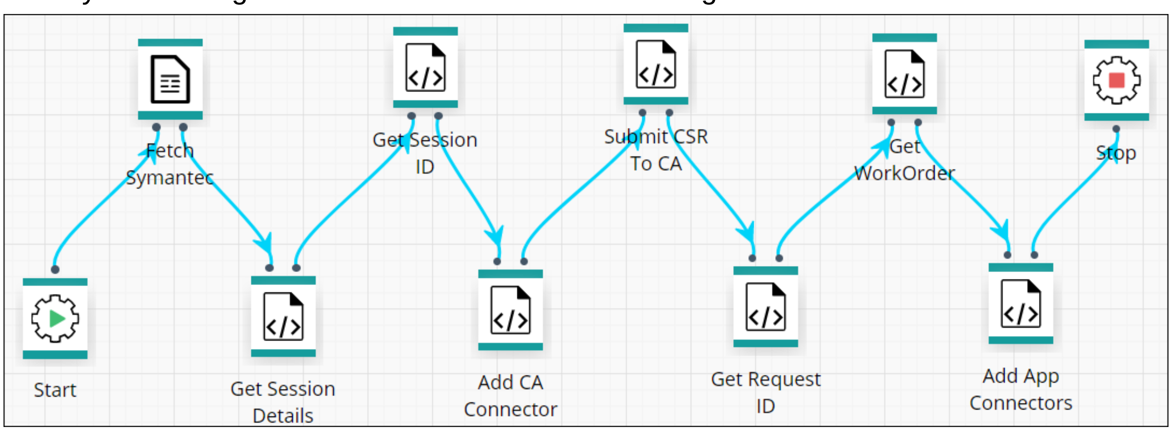
Note: Free AppViewX comes preloaded with visual workflows. You will only need to use the following import instructions when newer versions of the workflows are available.

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



4. On the *Import* screen that opens, 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.

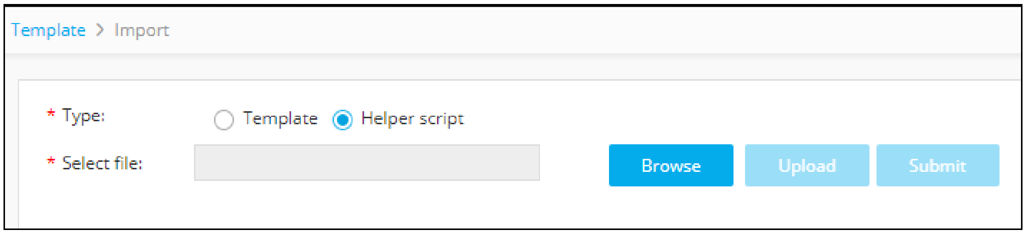
The Symantec Migration workflow is shown in the image below:



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 **Provisioning > Templates**.
3. Click the (**Import**) button in the Command bar.
4. On the *Import* screen that opens, complete the following steps:
   a. Select the **Helper script** radio button.
   b. Click **Browse** and select the helper script zip file you want to import.
   c. Click **Upload** to import the file and view its contents.



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

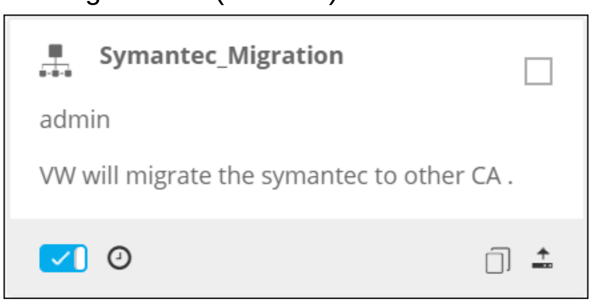
Enable a Workflow

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

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

   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.



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

Discover a Certificate

Note: This functionality is available only for server certificates.

The Discover function allows you to search for and display the list of all available SSL certificates within the network of an organization in order to manage it in the AppViewX certificate inventory. The certificate discovery search engine in AppViewX allows you search by any of the following six methods:

- IP range
- Subnet
- URL
- Upload
- Managed devices
- Certificate authorities

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.
5. On the ***Discover*** screen that opens, select one of the following tabs in the left-hand column:
   - **IP range** – Select this tab if you want to discover a certificate by IP range.
   - **Subnet** – Select this tab if you want to discover a certificate by subnet.
   - **URL** – Select this tab if you want to discover a certificate by URL.
   - **Upload** – Select this tab if you want to discover a certificate by upload.
   - **Managed devices** – Select this tab if you want to discover a certificate by managed devices.
   - **Certificate authorities** – Select this tab if you want to discover a certificate by CAs.

   Note: The fields that appear in the step 9 will vary based on the tab that you have selected.

9. At a minimum, complete all fields designated with a red asterisk (*).
10. Click **Discover** to discover all certificates that match the criteria you entered.
11. In the results field at the bottom of the screen, select each certificate you were looking for and then click one of the following buttons in the Command bar:
    - (**Monitor**) – Select this button if you want to be able to monitor the existence and validity of the certificate.
    - (**Manage**) – Select this button if you want to be able to execute actions on the certificate.

Configure Certificate Manager Accounts

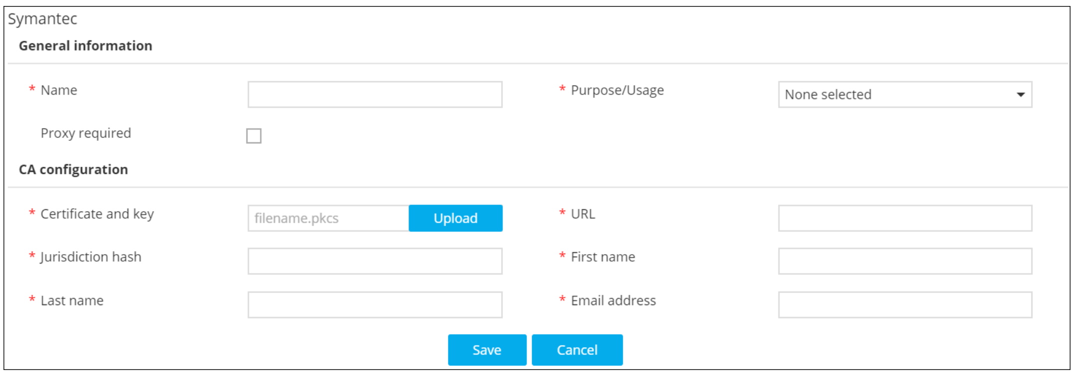
To configure DigiCert, Entrust, Trustwave, and Comodo certificate manager accounts, complete the following steps:

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 in the left-hand column each certificate authority (CA) available in AppViewX.
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 (**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.
2. Click the **Settings** option.
3. On the ***Settings*** screen, click the **System** tab.
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.
9. In the **Send Email to** field, enter any email address. If the configuration is successful, a test email will be sent to this address verifying that everything is working correctly.
10. Click **Save** to save the changes you have made to the system settings.

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 (**Run workflow**) button on the Symantec Migration, the respective Form Builder screen opens.
4. In the **Symantec Certificates** field, retrieve the list of Symantec certificates managed in AppViewX by clicking the (**Fetch**) 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.
5. In the **Certificate Group** field, retrieve the list of certificate groups available by clicking the (**Fetch**) button and select the certificate group to which the migrated certificates must be assigned to.
6. In the **CA to Migrate** field, retrieve the list of CAs available by clicking the (**Fetch**) button and select the CA to which the selected Symantec certificates must be migrated.
7. In the **CA Account** field, retrieve the list of CA accounts available by clicking the (**Fetch**) button and select the CA account with appropriate credentials, which will be used to create new certificates.
8. In the **Certificate Type** field, retrieve the list of certificate types based on the selected CA by clicking the (**Fetch**) button and select the required certificate type.
9. In the **Server Type** field, retrieve the list of server types based on the selected CA by clicking the (**Fetch**) button and select the required server type.
10. 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, select the certificate details you want to modify, make the required changes, and click the (**Update**) button.
11. In the **AppViewX Username** and **Password** fields, enter the user name and password respectively for AppViewX Web login.
12. Click the **PreValidation Check** button to ensure the following:
    - Only 1 to 10 Symantec certificates are selected for migration.
    - Validity of the selected CA and certificate type are within the allowed range.
    - The required information is provided for each certificate that is being migrated.

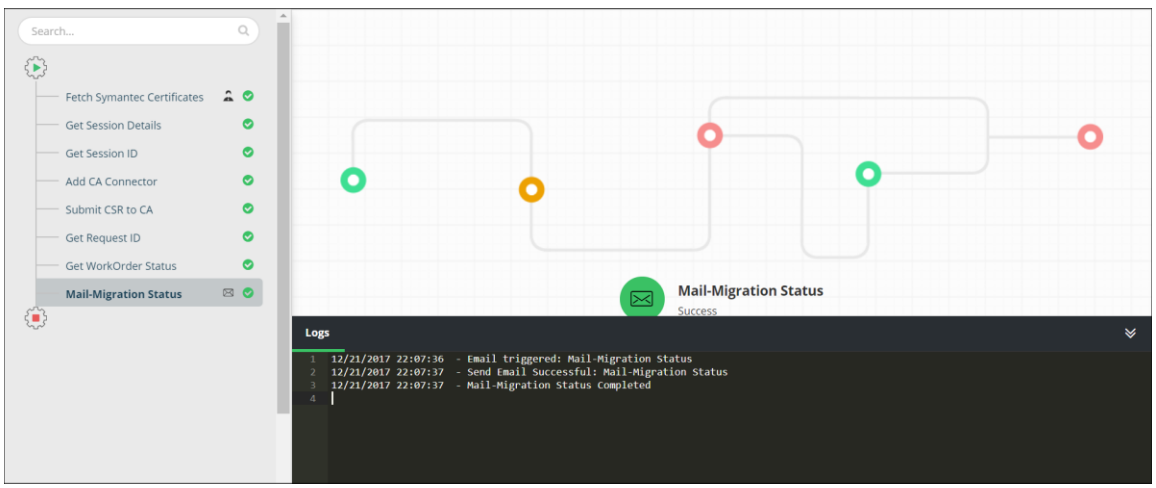
    The result of this validation is displayed in the **PreValidation Check** field.
13. Click **Submit** to trigger the workflow immediately.

WorkOrder flow

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.

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. **Add 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. **Get WorkOrder Status —** A validation is done to check the completion of the workflow execution.
8. **Mail-Migration Status —** An email is sent to the administrator with the status, common name, and request ID of the migration.



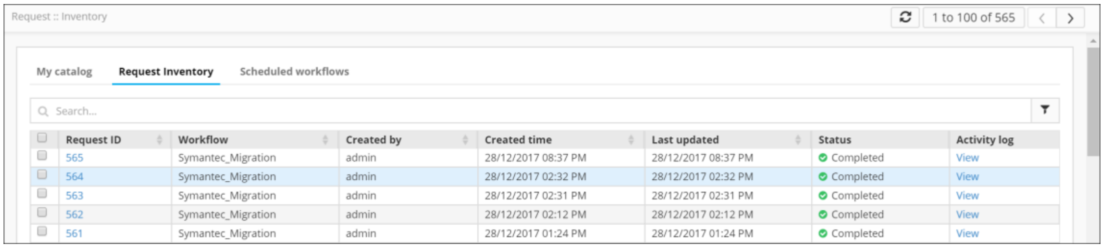
Request Inventory

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.



4. Click the **Request ID** created for Symantec Migration to view the tasks or phases of a request in a tree-view. For more details, refer to the WorkOrder flow section of this guide
5. You can also view the following details of the request that are created: 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.

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 Configurator 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.