



CA to CA Migration Workflow Guide

Copyright © 2018 AppViewX, Inc. All Rights Reserved.

This document may not be copied, disclosed, transferred, or modified without the prior written consent of AppViewX, Inc. While all content is believed to be correct at the time of publication, it is provided as general purpose information. The content is subject to change without notice and is provided “as is” and with no expressed or implied warranties whatsoever, including, but not limited to, a warranty for accuracy made by AppViewX. The software described in this document is provided under written license only, contains valuable trade secrets and proprietary information, and is protected by the copyright laws of the United States and other countries. Unauthorized use of software or its documentation can result in civil damages and criminal prosecution.

Trademarks

The trademarks, logos, and service marks displayed in this manual are the property of AppViewX or other third parties. Users are not permitted to use these marks without the prior written consent of AppViewX or such third party which may own the mark.

This product includes software developed by the CentOS Project (www.centos.org).

This product includes software developed by Red Hat, Inc. (www.redhat.com).

This product includes software developed by VMware, Inc. (www.vmware.com).

All other trademarks mentioned in this document are the property of their respective owners.

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: 1.0

Last updated on: May 10, 2018

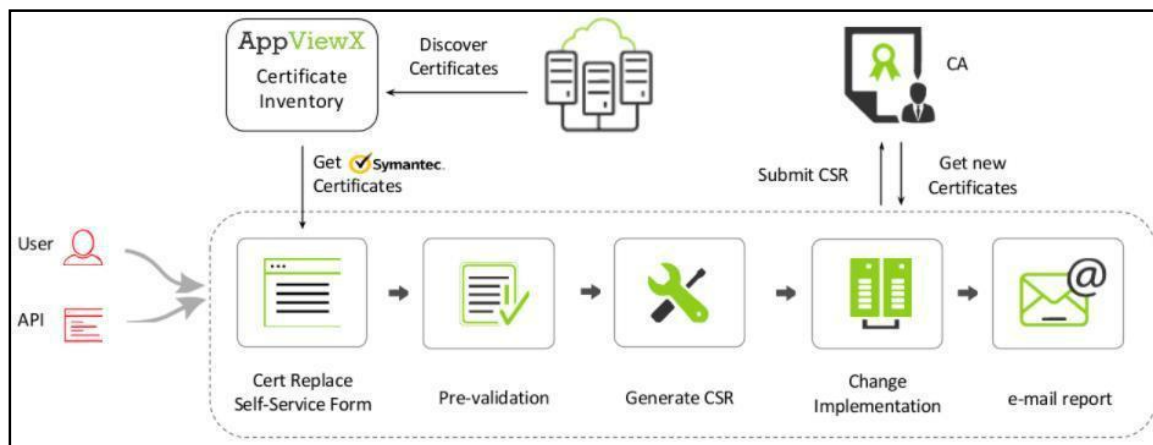
Contents

CA to CA Migration Workflow	1
Prerequisites	1
Compatible Software Versions	1
Limitations.....	1
Log In to AppViewX	2
Import Visual Workflows.....	2
Import Helper Scripts	3
Enable a Workflow	3
Discover a Certificate	4
Configure Certificate Manager Accounts.....	5
Configure the SMTP	5
Register an ITSM Device: ServiceNow	6
CA to CA Migration Workflow	6
Workorder Flow	8
Rollback a Workorder.....	9
Workorder Flow	9
Request Inventory	10
Schedule a Workflow	11
View Scheduled Workflows	11
Troubleshooting	11

CA to CA Migration Workflow

The CA to CA Migration workflow will migrate the certificate from one of the source CAs such as DigiCert, Entrust, EJBCA, Symantec, Trustwave, and Comodo certificate manager to the other target CAs (other than selected source CA) such as DigiCert, Entrust, Trustwave, and Comodo certificate manager, which are currently managed in AppViewX. The workflow provides an option to update the CSR generation parameters such as different key length or hash algorithm. The migration report is emailed to the user who has submitted the request. You can migrate up to 10 certificates from the selected source CA using a single request.

Note: The platform is capable of migrating more than 10 certificates in a single request. This is a sample workflow to showcase the platform capabilities.



Prerequisites

To run this workflow in your environment, the following prerequisites must be met:

- The selected source CA certificates must be discovered and managed in the AppViewX.
- The DigiCert, Entrust, EJBCA, 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

This workflow has been validated for the following software versions:

- AppViewX – Free AppViewX and AVX 12.3.0
- CAs – DigiCert, Entrust, EJBCA, Trustwave, and Comodo certificate manager accounts
- ServiceNow – Geneva, Eureka, Istanbul, and Jakarta

Limitations

This workflow has the following limitations:

- App connector will not handle duplicate certificate for the same CA and CA certificate type.
- The inputs to generate the CSR may differ for the migrated source and target CAs.
- In a single request, up to ten Symantec certificates can be migrated.
- Even if one certificate is successfully enrolled, retrieved from CA, and managed in Appviewx certificate inventory, the request and ServiceNow ticket will be considered complete.
- Start Time and End Time of ITSM has nothing do with the workflow implementation time. Once the ITSM ticket is approved, CA to CA migration will start working.

Log In to AppViewX

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



`http://hostname:portnumber`

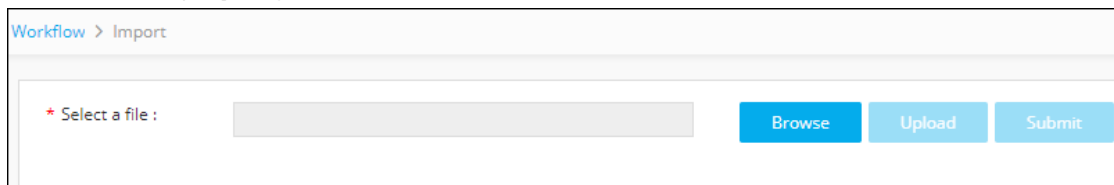
The hostname and port number are configured during deployment, with the default port number set to 5004 and the default web credentials set to `admin/AppViewX@123`.

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

Import Workflows

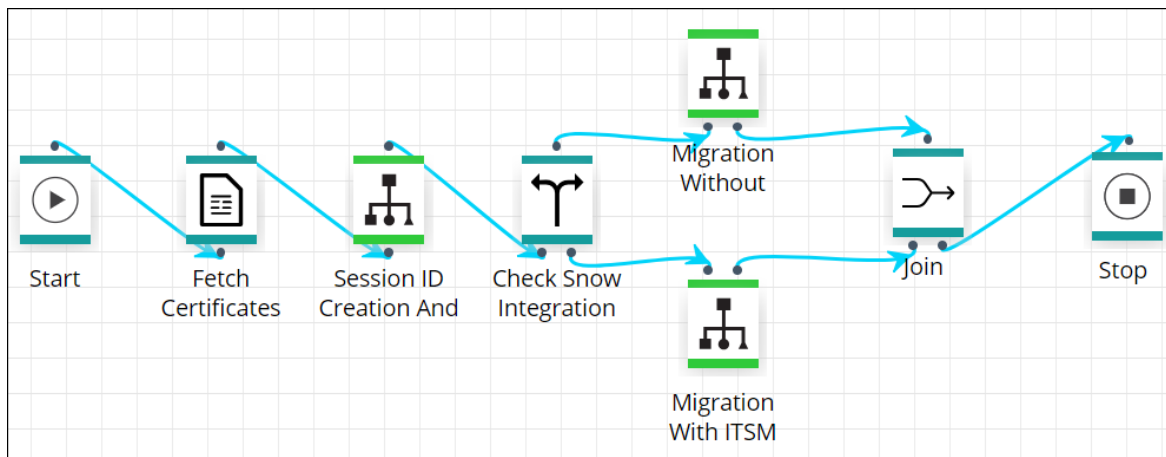
To import a workflow, complete the following steps:

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 sub-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 CA to CA Migration workflow is shown in the image below:



Import Helper Scripts

To import a helper script, complete the following steps:

1. In the navigation menu on the left-hand side of the AppViewX screen, navigate to **Workflow > Studio**.
2. Click on the  (**Helper script**) button. The *Helper script library* screen appears.
3. Click the  (**Import**) button.
4. Click **Browse** and select the helper script zip file you want to import.
5. Click **Upload** to import the file and view its contents.

* Select file: ☐ Overwrite existing file

Search...



Status	Script name	Logs
<input checked="" type="checkbox"/> 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.

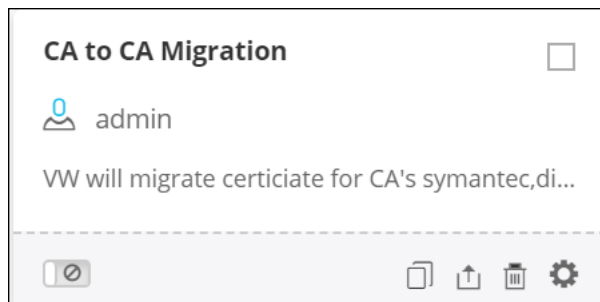
6. In the table at the bottom of the Import page, select the check boxes beside each of the helper scripts.
7. Click **Submit** to deploy them into your AppViewX environment.

Enable a Workflow

To enable the *CA to CA Migration* workflow, complete the following steps:

1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Configurator**.
3. The *Workflow* screen opens.
4. Click the ☐ (**Select**) button on the *CA to CA Migration* workflow to enable it. If the workflow is already selected, a ☒ (**Deselect**) button appears.
5. Click the  (**Enable**) button in the Command bar.

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



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



Discover a Certificate

Note: This functionality is available only for the 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 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, 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.

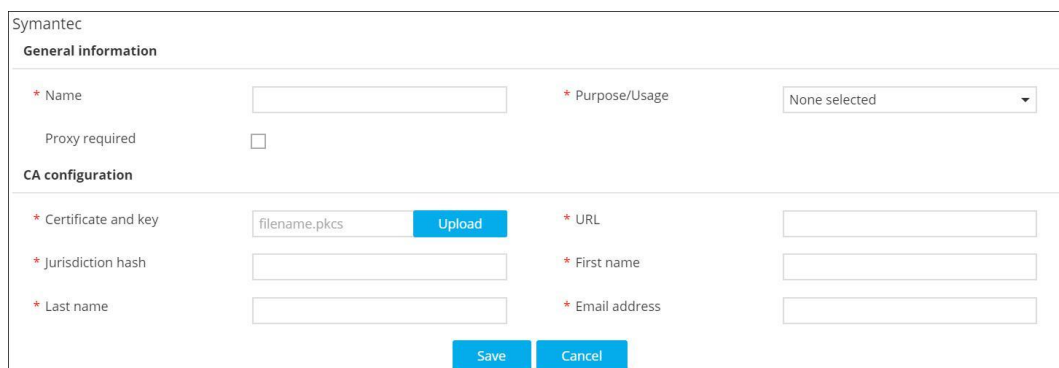
Note: The fields that appear in the step 6 will vary based on the tab that you have selected.

6. At a minimum, complete all fields designated with a red asterisk (*).
7. Click **Discover** to discover all certificates that match the criteria you entered.
8. 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, Ejbca, Trustwave, and Comodo certificate manager accounts in AppViewX, 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 **General** and then, click **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.
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.




Register an ITSM Device: ServiceNow

1. Click the  (**Menu**) button.
2. Click the **Settings** option.
3. On the **Settings** screen, click **Change Management**.
4. Click the ServiceNow plug-in.
5. On the *Vendor configuration* screen that opens, enter a valid web URL.
6. (Optional) Enter a **Description** of the vendor to help users identify it.
7. Enter the ServiceNow username and password credentials in the respective fields.
8. Click **Update** to save the changes made in the system.

CA to CA Migration Workflow

To submit the *CA to CA 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 *CA to CA Migration* workflow. The form corresponding to the workflow appears.

4. From the **Source CA** dropdown, select the CA to be migrated.
5. From the **Certificates to Migrate** dropdown, select the certificates to 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  (**Fetch**) button and select the certificate group to which the migrated certificates must be assigned to.
7. In the **Target CA** field, retrieve the list of CAs available by clicking the  (**Fetch**) button and select the CA to which the selected Source CA certificates must be migrated.
8. In the **CA Account** field, retrieve the list of CA accounts available automatically using auto trigger feature in VW 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 automatically using auto trigger feature in VW and select the required certificate type.
10. Click the **Fetch Certificate 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.

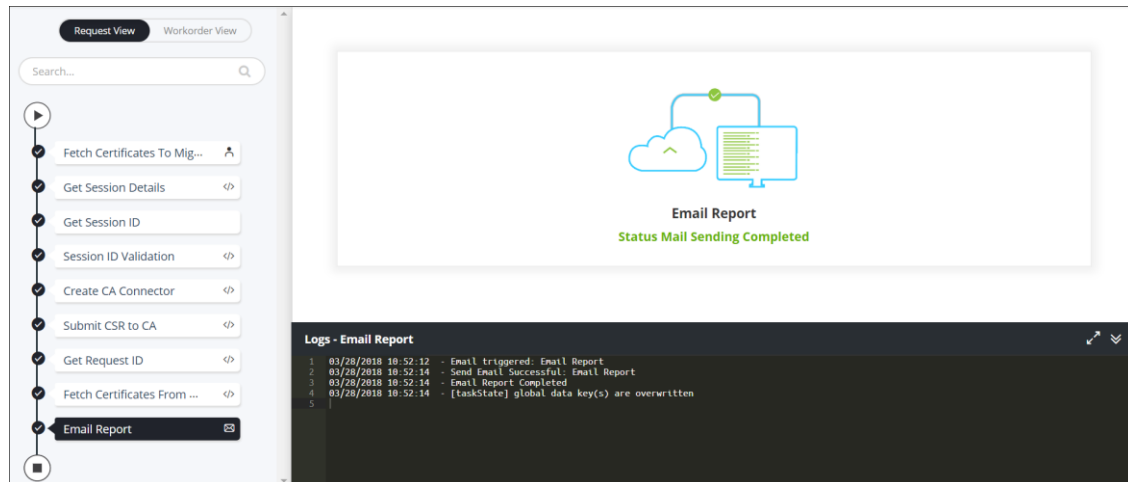
13. Radio button **Integrate ITSM** select **Yes**. This creates a ServiceNow change request ticket and binds it with the work order to update the ServiceNow status.
14. Select the **Time Zone** to be used.
15. Schedule the maintenance window time and date using the **Start Time** and **End Time** fields. The configuration changes will be implemented during this maintenance window.
16. Click the **Change ID** Fetch button to create a new ServiceNow ticket and auto-populate the Change Request ID field.
17. Click **Submit** to trigger the workflow immediately.

Workorder Flow

The following are the workorder tasks of *CA to CA 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 Certificates To Migrate** — The Source CA 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. **Session ID Validation** — Check valid session ID got created in the flow 3
5. **Get Sys ID** — The Sys-ID for the **CA to CA Migration** workflow is generated to track the ServiceNow request.
6. **Validate Ticket status** — To validate the ticket, log in to ServiceNow and manually approve the ticket.
Note: Validating of ticket is retried 50 times with an interval of 20 sec.
7. **Create CA Connector** — The CA connectors for the new certificates with common names are created.
8. **Submit CSR to CA** — The CSR is created and submitted to the CA.
9. **Get Request ID** — The request ID of the triggered workflow is retrieved.
10. **Fetch Certificates From CA** — A validation is done to check the completion of the workflow execution.
11. **Email Report** — An email is sent to the administrator with the status, common name, and request ID of the migration.
12. **Close complete** — After successful migration of the certificate, the status of the ServiceNow ticket is updated automatically.
13. **Close Incomplete** — If the migration of the certificate is not successful, the status of the ServiceNow ticket is updated automatically.



Rollback a Workorder

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 *CA to CA 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 *CA to CA 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. **Get Session Details** — The session details and ID will be generated to issue the required API commands.
2. **Get Session ID** — The session ID is retrieved for issuing API commands for submitting Revoke Request to CA, get Revoke request ID, and checking the revoke work order status.
3. **Session ID Validation** — Check valid session ID created in the flow
4. **Submit Revoke Request** — The revoke request of enrolled certificate is submitted to CA.
5. **Get Revoke Request ID** — The request ID of the triggered revoke request is retrieved.

6. **Check Certificates Revoked**— A validation is done to check the completion of the revoke request execution.

Check Certificates Revoked
Certificate Revoke Request Status Validation Completed

Logs - Check Certificates Revoked

```

1 03/28/2018 11:06:18 - Initiating Check Certificates Revoked
2 03/28/2018 11:07:16 - Requests Id R389 for the common name 123.appriver.com Revoked
3 03/28/2018 11:07:16 - WorkOrder status completed for the triggered certificate
4 03/28/2018 11:07:20 - Check Certificates Revoked Completed
5 03/28/2018 11:07:20 - [TaskState] global data key(s) are overwritten

```

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 Inventory								
Search...								
Request ID	Workflow	Created by	Created time	Last updated	Status	Ref. ID	Activity log	
523	var CA to CA Migration	admin	28/03/2018 00:12 PM	28/03/2018 00:12 PM	Completed	422	View	
515	DB CA to CA Migration	balaji	28/03/2018 11:05 AM	28/03/2018 11:05 AM	Completed	514	View	
505	var CA to CA Migration	admin	27/03/2018 07:20 PM	27/03/2018 07:20 PM	Failed		View	
504	var CA to CA Migration	admin	27/03/2018 07:15 PM	27/03/2018 07:15 PM	Completed	475	View	

4. Click the **Request ID** of the requested workflow to view the tasks or phases of a request in a tree-view.
5. You can also view the following details of the request that are created: by whom and when the Request was created, Last updated time, Status and the Activity log.
6. Click **View** 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.

Summary	Detail
Request ID - 514 Completed	
1	Fetch Certificates To Migrate ✓
2	Get Session Details ✓
3	Get Session ID ✓
4	Session ID Validation ✓
5	Create CA Connector ✓
6	Submit CSR to CA ✓
7	Get Request ID ✓
8	Fetch Certificates From CA ✓
9	Email Report ✓




Schedule a Workflow

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 respective workflow.
4. On the 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 the selections you make.
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 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.