



Easy Certificate Provisioning 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: 12.4.0

Document Version: WIP 1.0

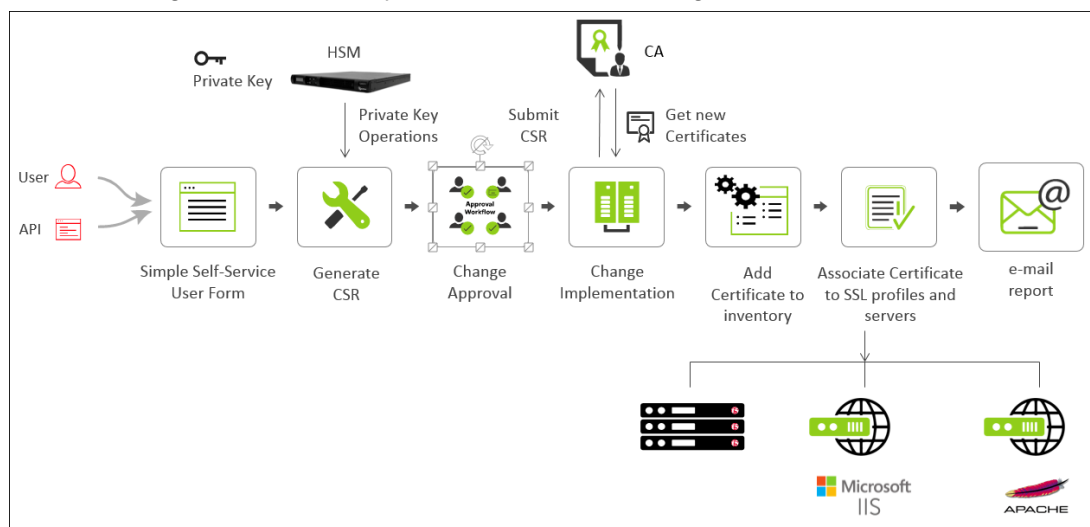
Last updated on: August 27, 2018

Contents

| | | |
|-----|---|----|
| 1 | Description | 1 |
| 2 | Prerequisites | 1 |
| 2.1 | Add an ADC Server: F5 | 1 |
| 2.2 | Add a Server | 3 |
| 2.3 | Configure the Certificate Manager Accounts | 5 |
| 3 | Compatible Software Versions | 6 |
| 4 | Limitations | 6 |
| 5 | Preliminary Tasks | 6 |
| 5.1 | Log In to AppViewX | 6 |
| 5.2 | Import a Workflow | 6 |
| 5.3 | Import Helper Scripts | 7 |
| 5.4 | Enable the Easy Certificate Provisioning Workflow | 8 |
| 6 | Easy Certificate Provisioning Workflow | 8 |
| 6.1 | Work Order Flow | 9 |
| 7 | Rollback a Workflow | 10 |
| 7.1 | Work Order Flow | 11 |
| 8 | Request Inventory | 11 |
| 9 | Schedule a Workflow | 13 |
| 10 | View Scheduled Workflows | 13 |
| 11 | Add a Credential | 13 |
| 12 | Troubleshooting | 14 |

1 Description

The Easy Certificate Provisioning workflow will enroll new certificate from one of the CAs such as AppViewX, DigiCert, CCM, or EJBCA based on the CA list specified in the certificate policy. Once the certificate is enrolled from the respective CA, certificate is pushed and/or pushed and bonded with the profile or application based on the user selection in the form. The supported device for certificate push or push and bind are ADC- F5 and Citrix Server – Apache/Tomcat. The flow diagram for the Easy Certificate Provisioning workflow is shown in the image below:





2 Prerequisites

To run this workflow, ensure that the following prerequisites are met:

- The DigiCert, EJBCA, AppViewX, and Comodo certificate manager accounts are configured on AppViewX.
- ADC devices F5 and Citrix are added in the inventory and managed.
- Apache/Tomcat server devices are added in the inventory and managed.
- Appropriate users, user groups, roles, and resources are created and mapped correctly.
- Certificate groups and policies are create and mapped with appropriate resources.
- The “Approval required” parameter in the policy of the selected certificate group must be unchecked for the auto-implementation of this workflow.
- The certificate policy must have correct values based on the CA selected for successful CSR generation and submission to the CA.
- Update the helper “easy_cert_helper” with appropriate EJBCA and Apache/Tomcat details.

2.1 Add an ADC Server: F5

1. Click the  (Menu) button.
2. Navigate to **Inventory > Device**.
3. The *Device* screen opens with the **ADC** tab displayed by default.
4. Click the  (**Add**) button in the Command bar.

5. On the *Add* screen that opens, click to select **F5** as the ADC vendor.

Device :: ADC > Add

Device details **Device group**

Vendors

- A10
- AVI
- AmazonELB
- BigIQ
- Cisco
- Citrix
- F5**
- HAProxy
- NginxPlus

General information

vCMP Host ☐

* Modules ☐ LTM ☐ GTM

vCMP Guest ☐

* Device name

Data center

Communication ☒ IP address ☐ FQDN

* IP address

* SSH Port

Cert sync ☒ Managed ☐ Monitored ☐ Ignored

AppViewX group sync ☒

6. Click the **vCMP Host** check box, if you want to add and manage the vCMP host devices
7. Select the module to be managed on the ADC device.
8. Click the **vCMP Guest** check box, if you want to add and manage the vCMP guest devices.
9. Create a **Device name** that is specific to AppViewX and that will identify the device in the AppViewX inventory.
10. Select the **IP address** or **FQDN** radio button based on how you want to establish the communication.
Enter the IP address or FQDN in their corresponding fields depending on what you selected.
11. Enter the SSH port number of the device.
12. (Optional) Specify a **Data center location** if you want to have the option later to filter devices based on their location.
13. In the **Cert sync** field, select the radio button for the kind of synchronization relationship you want to establish between SSL certificates on the ADC device and AppViewX: **Managed**, **Monitored**, or **Ignored**.
14. (Optional) Select the **AppViewX group sync** check box if you need AppViewX to sync the configuration changes from an active to standby F5 ADC device. This is required in older F5 versions like v10. The latest versions of F5 sync automatically.
15. From the **Credential type** dropdown list, select how you want to provide the credentials:
 - a. Select **Manual entry** if you want to manually enter the credential details (user name and the associated password) every time the device is accessed.

- b. Select **Credential list** if you want to retrieve the login details created in the credential template. For more details on how to add a credential to a device, refer to the [Add a Credential](#) section of this guide.

When you select the credential name from the dropdown list, the **user name** and **password** fields are auto-populated with the values provided in the credential template.
 16. In the **Secondary/Alternate** device field, select how you want to fetch the details of a backup device when the primary device becomes unavailable due to failure or scheduled down time:
 - a. Select **Auto detect** if you want AppViewX to automatically detect and retrieve the configuration of the secondary/alternate device, then click **Save** to add the device to AppViewX.
 - b. Select **Manual entry** if you want to manually provide the details of the secondary device. At a minimum, fill in all fields that contain a red asterisk beside their names.
 17. Click **Add** to add the secondary device to the list at the bottom of the screen.
- Note:** You can add more than one secondary device. The **Update** and **Delete** buttons are enabled only when you try to modify existing secondary devices.
18. Click **Save** to add the new ADC device. The device is then displayed in the table on the **ADC** tab.



| ADC | Server | DNS | Firewall | WAF | Switch | Router | Proxy | Cloud | Others |
|--------------------------|----------------|-------------------|----------|--------|----------|---------------------------|---------|-------|--------|
| Q Search... | | | | | | | | | |
| <input type="checkbox"/> | Name | FQDN / IP address | Port | Vendor | Modules | Object count | Status | | |
| <input type="checkbox"/> | 192.168.112.92 | 192.168.112.92 | 22 | F5 | LTM,GTM | 21 Virtual Servers,19 ... | Managed | | |
| <input type="checkbox"/> | 192.168.112.93 | 192.168.112.93 | 22 | F5 | LTM,GTM | 2 Virtual Servers,2 Wi... | Managed | | |
| <input type="checkbox"/> | 192.168.40.62 | 192.168.40.62 | 22 | A10 | SLB,GSLB | 6 Virtual Services,3 F... | Managed | | |
| <input type="checkbox"/> | 192.168.41.57 | 192.168.41.57 | 22 | AVI | SLB | 33 Virtual Services | Managed | | |
| <input type="checkbox"/> | 192.168.95.197 | 192.168.95.197 | 22 | Citrix | SLB,GSLB | 3 SLB Virtual Servers,... | Managed | | |

The device will display one of the following statuses:

- **In Progress** – Device configuration fetch is in progress.
- **Managed** - Device configurations are fetched and parsed successfully. This is the status a successfully added ADC device should have.
- **Unresolved** – Unable to communicate with device due to invalid login credentials.
- **Failed** – Device configuration fetch failed due to unsupported version.

2.2 Add a Server

To add a server, complete the following steps:

1. Click the  (**Menu**) button on the left-hand side of the AppViewX screen
2. Navigate to **Inventory > Device**.
The *Device* screen opens with **ADC** tab displayed by default.
3. Click the **Server** tab.
4. Click the  (**Add**) button in the Command bar.

The *Add* screen opens, with the **APACHE** tab selected by default.

5. Select the **Apache** or **Tomcat** radio button depending on what type of server you want to configure.
6. In the **Server name** field, enter a name for the server to help users identify it.
7. In the **IP address** field, enter the IP address for which the connection must be established.
8. (Optional) In the **Data center** field, enter the data center name in which the device resides.
9. In the **Cert sync** field, select the radio button for the kind of synchronization relationship you want to establish between SSL certificates on the ADC device and AppViewX: **Managed**, **Monitored**, or **Ignored**
10. From the **Credential type** dropdown list, select how to want to provide the credentials:
 - Select **Manual entry** if you want to manually enter the credential details (user name and the associated password) every time the device is accessed.
 - Select **Credential list** if you want to retrieve the login details created in the credential template. For more details on how to add a credential to a device, refer to the [Error! Reference source not found.](#) section of this guide. After you select the credential name from the dropdown list, the **user name** and **password** fields are auto-populated with the values provided in the credential template.
11. Enter the location, where the **certificate**, **key**, and **intermediate** CA are available in the server, in their respective fields.
12. Click **Add**. The Certificate location details are then added to the table at the bottom of the screen. You can delete the location details by clicking the (**Delete**) button beside the certificate location name and to modify, select the certificate location name in the table at the bottom of the screen.
13. Click **Save**. A new server is added to the AppViewX inventory and appears on the **Server** tab.

ADC

Server

DNS

Firewall

WAF

Switch

Router

Proxy

Cloud

Others

Q

Search...




| <input type="checkbox"/> | Name | IP address | Data center | Vendor | Status | Credential type |
|--------------------------|-------------------------------------|---------------|-------------|------------------------------|-------------------------------|-----------------|
| <input type="checkbox"/> | <div><div></div>192.168.98.27</div> | 192.168.98.27 | | <div><div></div>Apache</div> | <div><div></div>Managed</div> | Manual entry |
| <input type="checkbox"/> | <div><div></div>192.168.99.8</div> | 192.168.99.8 | | <div><div></div>Apache</div> | <div><div></div>Managed</div> | Manual entry |

The device will display one of the following statuses:

- **In Progress** – Device configuration fetch is in progress.
- **Managed** – Device configurations are fetched and parsed successfully. This is the status a successfully added ADC device should have.
- **Unresolved** – Unable to communicate with device, due to invalid login credentials.
- **Failed** – Device configuration fetch failed, due to unsupported version.

2.3 Configure the Certificate Manager Accounts

To configure the 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 (*).

Symantec

General information

* Name

* Purpose/Usage None selected

Proxy required ☐

CA configuration

* Certificate and key Upload

* URL

* Jurisdiction hash

* First name

* Last name

* Email address

Save
Cancel

9. Click **Save**. The certificate manager account you added will be displayed in the table.
10. (Optional) Repeat steps 6-9 for any other vendors for whom you want to create certificate manager account details.

3 Compatible Software Versions

This workflow has been tested and validated on the following software versions:

- AppViewX –12.4.0
- F5 – V11, 12, and 13
- Citrix – V11 and 12
- CAs - DigiCert, AppViewX, EJBCA, and Comodo certificate managers
- Server

4 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 are purely based on the certificate policy and “easy_cert_helper”. So, it is sole responsibility of the request owner to ensure proper data is provided.

5 Preliminary Tasks

Following are the preliminary tasks that needs to be performed before executing a workflow:

- [Log In to AppViewX](#)
- [Import a Workflow](#)
- [Import a Helper Script](#)
- [Enable the Easy Certificate Provisioning Workflow](#)

5.1 Log In to AppViewX

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



`https://hostname:portnumber.`

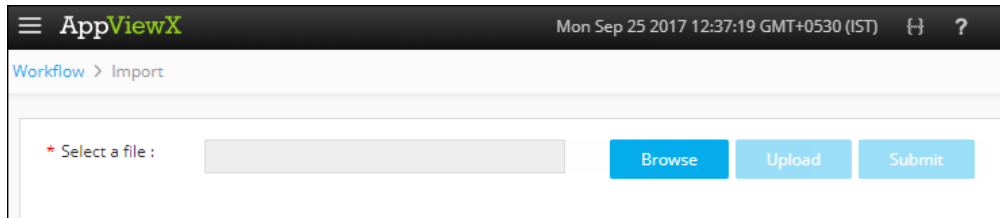
The hostname and port number are configured during deployment, with the default port number set to 5004 and the default web credentials set to `admin/AppViewX@123`.

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

5.2 Import a Workflow

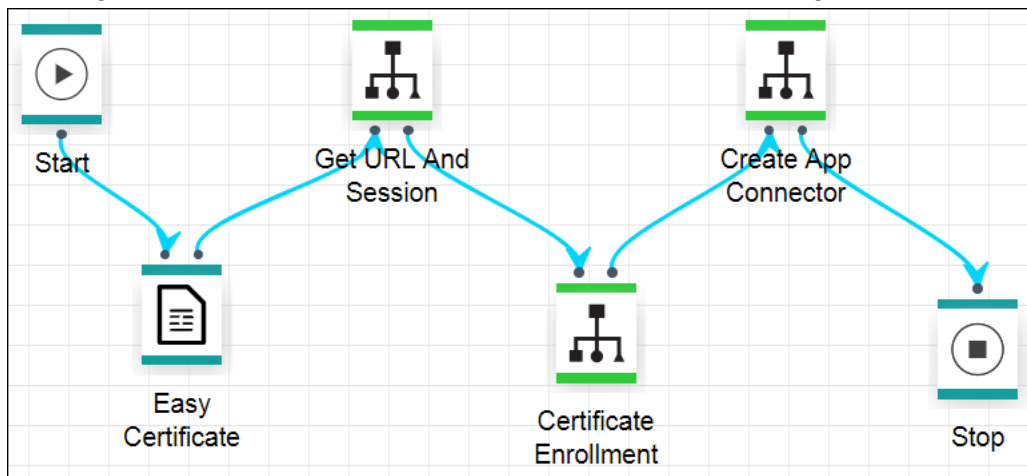
Note: Free AppViewX comes preloaded with visual workflows. You will only need to use the following import instructions when newer versions of the workflows are available.

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



4. Click the **Browse** button.
5. Select the zip file containing one or more workflows, then click **Upload**.
6. In the table at the bottom of the Import page, select the check box beside the unzipped workflow file.
7. Click **Submit** to deploy the workflow into your AppViewX environment.

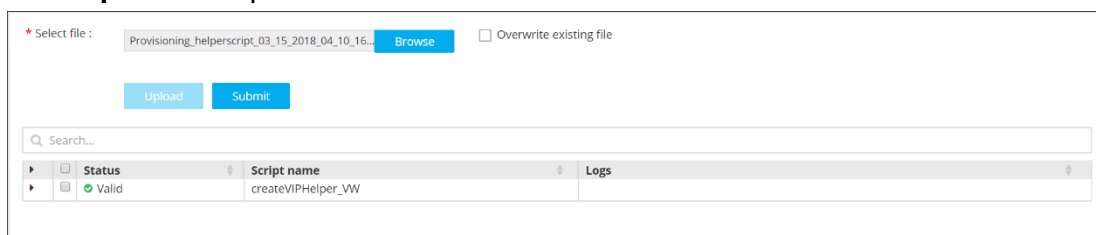
The DigiCert Certificate Creation workflow is shown in the image below:



5.3 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.






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.

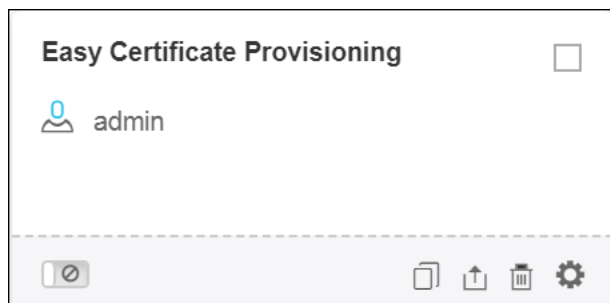
7. In the table at the bottom of the Import page, select the check boxes beside each of the helper scripts.
8. Click **Submit** to deploy them into your AppViewX environment.

5.4 Enable the Easy Certificate Provisioning Workflow

To enable the Easy Certificate Provisioning 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 **Easy Certificate Provisioning** 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 DigiCert Certificate Creation workflow from the Card view by clicking the  (**Disable**) button.

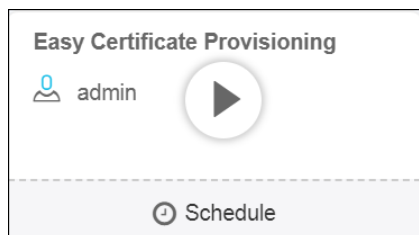


5. On the *Confirmation* screen that appears, click **Yes**.

6 Easy Certificate Provisioning Workflow

To submit the Easy Certificate Provisioning workflow, complete the following steps:



1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Request**.
3. The *Request* screen opens with the **Overview** tab displayed by default.
4. Click **View/Run** to display all the enabled workflows assigned to a specific user role.
5. Click the Play button on the Easy Certificate Provisioning workflow to execute.



The *FormBuilder* screen opens.

The FormBuilder screen contains the following fields and controls:

- * Common Name:** A text input field.
- * Device Type:** Radio buttons for ☒ ADC and ☐ Server.
- * Device:** A dropdown menu with a "Select" placeholder and a "Retrieve field values" icon.
- * SSL Profiles or Application:** A dropdown menu with a "Select" placeholder and a "Retrieve field values" icon.
- Buttons:** A row of four blue buttons: a plus sign (+), an eraser, a refresh (C), and a trash can.
- * Object Binding:** A search box with "Search..." and a table with columns "Device" and "SSL Profiles or Application". The table currently shows "No records found".
- Footer Buttons:** A row of four blue buttons: "Save draft", "Submit", "Discard", and "Cancel".

6. Enter the common name used to create certificate and push or push and bind to device.
7. Select the type of device which the certificates have to be pushed or pushed and bonded.
8. In the **Device** field, click the  (**Retrieve field values**) button to retrieve the list of ADC (F5/Citrix) or Server (Apache/Tomcat) devices.
9. Select the SSL profiles or application if you had selected ADC or server respectively in step 7.
10. Click the  (**Add**) button to bind the device objects.

6.1 Work Order Flow

The following are the workorder tasks of Easy Certificate Provisioning 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.

The screenshot shows the workflow interface with the following components:

- Header:** "Request > Easy Certificate Provisioning -- 617".
- Navigation:** Tabs for "Request View" and "Workorder View". A search bar and a list of tasks with checkboxes and expand/collapse icons.
- Task List:**
 - Easy Certificate Provisio...
 - Get URL Details
 - Session ID Validation
 - CSR Parameter Mapping
 - Create CA Connector
 - Submit CSR to CA
 - Get Request ID
 - Fetch Certificates From CA
 - Add Application Connector
 - Push Certificate to Device
- Workorder View:** A diagram showing a cloud connected to a server, with the text "Get WorkOrder Status" and "Workorder status obtained".
- Logs - Get WorkOrder Status:**

```

1 07/23/2018 16:49:41 - Initiating Get WorkOrder Status
2 07/23/2018 16:50:46 - WorkOrder status completed for the triggered certificate
3 07/23/2018 16:50:51 - Get WorkOrder Status completed
4

```



1. **Easy Certificate Provisioning** — Get the common name and detail of the type of device and profile or application to push the certificate.
2. **Get Session Details** — Get or frame the URL to be used for accessing the API.
3. **Session ID Validation** — Generate the session ID and valid session ID. If the session is generated correctly, move forward or the workflow will fail.
4. **CSR Parameter Mapping**: Based on the logged in user detail, the resource allocated is identified and using that, the certificate group and policy are identified. The CA connector payload is created using the certificate policy CSR mapping.
5. **Create CA Connector** — The CA connector is saved, which act as the CSR parameter to enroll with the CA.
6. **Submit CSR to CA** — The CSR is created and submitted to the CA.
7. **Get Request ID** — The request ID of the triggered workflow is retrieved.
8. **Fetch Certificates from CA**— A validation is done to check the completion of the workflow execution and the certificates are managed in the certificate inventory.
9. **Generate Application connector payload** — Based on the selected device and profile or application, the app connector payload is prepared.
10. **Add Application Connectors** — Create app connector API is triggered and the app connector is created for the enrolled certificate.

Note: In a single request, the app connector must be created only for a single vendor.

11. **Push Certificate to Device** — Based on the response received for the application connector, push to device API is triggered and workflows are raised based on the number of profiles or application that will be associated with the certificate.
12. **Get Request ID** — The request ID of the triggered workflow is retrieved.
13. **Get WorkOrder Status** — Get the status of the raised request for push and bind of the certificate.

7 Rollback a Workflow

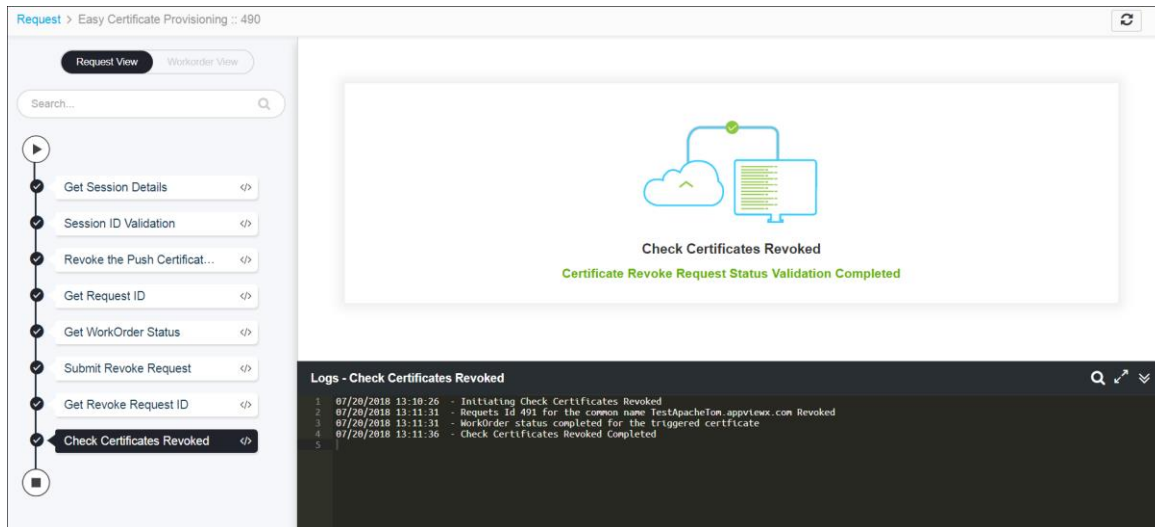
A rollback action can be performed only on the completed workflows. To trigger a rollback action, complete the following steps:

1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Request**.
The *Request* screen opens with **Workflow dashboard** displayed by default.
3. Click the **All** tab in **My requests** section.
This displays all workflows that have been triggered. On the request inventory screen, you can search for a request created for DigiCert Certificate Creation 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.

7.1 Work Order Flow

The following are the workorder tasks of Easy Certificate Provisioning 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.



1. **Get Session Details** – The session details and ID will be generated to issue the required API commands.
2. **Session ID Validation**– Generate and check valid session ID.
3. **Revoke the Push Certificate to Device** – Rollback the certificate push and bind with the profile or application, this is done using workflow. A new request is generated.
4. **Get Revoke Request ID**– The request ID of the triggered revoke request is retrieved.
5. **Get WorkOrder Status** - Get the status of the raised request for rollback push and bind of the certificate.

Note: Rollback of push and bind are not auto approved and hence, the raised request must be manually submitted.

6. **Submit Revoke Request** – The revoke request of the enrolled certificate is submitted to the CA.
7. **Get Revoke Request ID**– The request ID of the triggered revoke workflow request ID is retrieved.
8. **Check Certificates Revoked**– A validation is done to check the completion of the revoke request execution.


8 Request Inventory

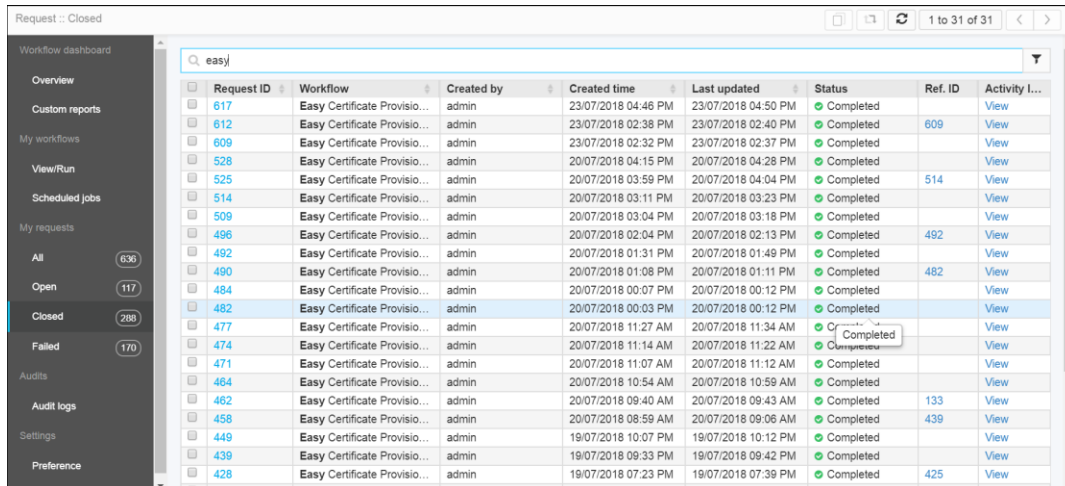
To go to the Request inventory, complete the following steps:

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

The *Request* screen opens with **Workflow dashboard** displayed by default.

3. Click the **All** 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 :: Closed

Workflow dashboard

Overview

Custom reports

My workflows

View/Run

Scheduled jobs

My requests

All (636)

Open (117)

Closed (288)

Failed (170)

Audits

Audit logs

Settings


Preference

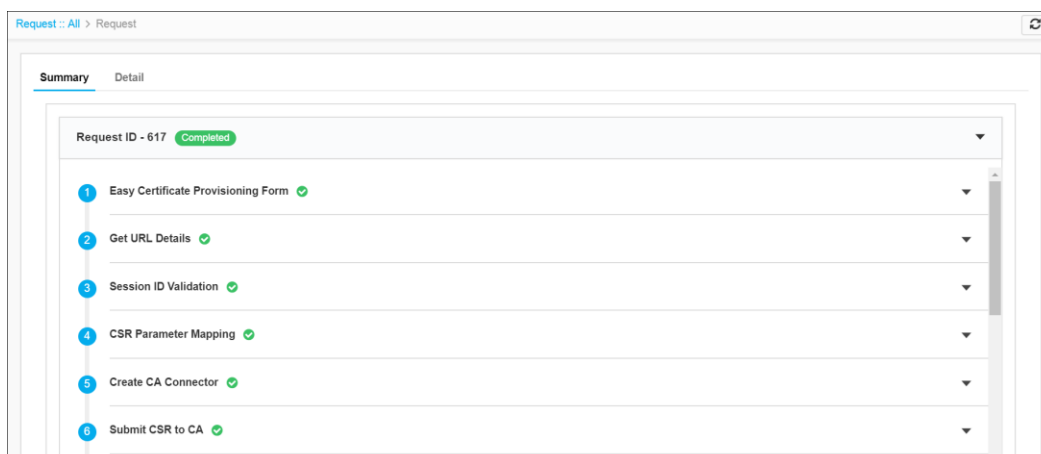
Q: easy

| Request ID | Workflow | Created by | Created time | Last updated | Status | Ref. ID | Activity L... |
|------------|------------------------------|------------|---------------------|---------------------|-----------|---------|---------------|
| 617 | Easy Certificate Provisio... | admin | 23/07/2018 04:46 PM | 23/07/2018 04:50 PM | Completed | | View |
| 612 | Easy Certificate Provisio... | admin | 23/07/2018 02:38 PM | 23/07/2018 02:40 PM | Completed | 609 | View |
| 609 | Easy Certificate Provisio... | admin | 23/07/2018 02:32 PM | 23/07/2018 02:37 PM | Completed | | View |
| 528 | Easy Certificate Provisio... | admin | 20/07/2018 04:15 PM | 20/07/2018 04:28 PM | Completed | | View |
| 525 | Easy Certificate Provisio... | admin | 20/07/2018 03:59 PM | 20/07/2018 04:04 PM | Completed | 514 | View |
| 514 | Easy Certificate Provisio... | admin | 20/07/2018 03:11 PM | 20/07/2018 03:23 PM | Completed | | View |
| 509 | Easy Certificate Provisio... | admin | 20/07/2018 03:04 PM | 20/07/2018 03:18 PM | Completed | | View |
| 496 | Easy Certificate Provisio... | admin | 20/07/2018 02:04 PM | 20/07/2018 02:13 PM | Completed | 492 | View |
| 492 | Easy Certificate Provisio... | admin | 20/07/2018 01:31 PM | 20/07/2018 01:49 PM | Completed | | View |
| 490 | Easy Certificate Provisio... | admin | 20/07/2018 01:08 PM | 20/07/2018 01:11 PM | Completed | 482 | View |
| 484 | Easy Certificate Provisio... | admin | 20/07/2018 00:07 PM | 20/07/2018 00:12 PM | Completed | | View |
| 482 | Easy Certificate Provisio... | admin | 20/07/2018 00:03 PM | 20/07/2018 00:12 PM | Completed | | View |
| 477 | Easy Certificate Provisio... | admin | 20/07/2018 11:27 AM | 20/07/2018 11:34 AM | Completed | | View |
| 474 | Easy Certificate Provisio... | admin | 20/07/2018 11:14 AM | 20/07/2018 11:22 AM | Completed | | View |
| 471 | Easy Certificate Provisio... | admin | 20/07/2018 11:07 AM | 20/07/2018 11:12 AM | Completed | | View |
| 464 | Easy Certificate Provisio... | admin | 20/07/2018 10:54 AM | 20/07/2018 10:59 AM | Completed | | View |
| 462 | Easy Certificate Provisio... | admin | 20/07/2018 09:40 AM | 20/07/2018 09:43 AM | Completed | 133 | View |
| 458 | Easy Certificate Provisio... | admin | 20/07/2018 08:59 AM | 20/07/2018 09:06 AM | Completed | 439 | View |
| 449 | Easy Certificate Provisio... | admin | 19/07/2018 10:07 PM | 19/07/2018 10:12 PM | Completed | | View |
| 439 | Easy Certificate Provisio... | admin | 19/07/2018 09:33 PM | 19/07/2018 09:42 PM | Completed | | View |
| 428 | Easy Certificate Provisio... | admin | 19/07/2018 07:23 PM | 19/07/2018 07:39 PM | Completed | 425 | View |

4. Click the **Request ID** created for **Easy Certificate Provisioning** to view its details.

The screen opens with the **Request View** tab selected by default.

- 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 Work Order Flow section of this guide.
 - 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.
- 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.
 - 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.



Request :: All > Request



Summary Detail

Request ID - 617 Completed

| | | |
|---|------------------------------------|---|
| 1 | Easy Certificate Provisioning Form | ✓ |
| 2 | Get URL Details | ✓ |
| 3 | Session ID Validation | ✓ |
| 4 | CSR Parameter Mapping | ✓ |
| 5 | Create CA Connector | ✓ |
| 6 | Submit CSR to CA | ✓ |


9 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 the **Workflow dashboard** tab displayed by default.
3. Click **View/run** in the **My workflows** section.
4. Click the  (**Schedule workflow**) button on the **Easy Certificate Provisioning** workflow.
5. 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 what you select.
6. Click **Save**.



10 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. Click the **Scheduled jobs** tab in **My workflows** section.
All the triggered workflows are displayed.
4. In the **Job ID** column, click the link to view the corresponding details.

11 Add a Credential

To add a credential to a device, complete the following steps:

1. Click the  (**Menu**) button.
2. Navigate to **Inventory > Device**.
The *Device* screen opens with the **ADC** tab selected by default.
3. Click the corresponding tab.
4. Click the check box beside the device name, then click the  (**Credential**) button in the Command bar.
5. On the *Add credential* screen that appears, enter the name of the credential you want to add to the device.
6. Enter the **username** and **password** associated with the credential.
7. (Optional) If a secondary credential password was created by a vendor in order to communicate with the device, thus allowing different levels of control over the credential, enter this password in the **Secondary password** field.
8. Click **Save**.
The credential is then added to the table at the bottom of the screen. You can delete a credential or modify its name, user name, or password by selecting the check box beside the credential name in the table at the bottom of the screen and then clicking either the **Modify credential** or **Delete** button in the Command bar.

12 Troubleshooting

I cannot find the Easy Certificate Provisioning workflow in the View/Run

You must enable the workflow from the **Studio** section. For more details on how to enable a workflow, refer to the [Enable the Easy Certificate Provisioning Workflow](#) section of this guide.