

DigiCert Certificate Creation Workflow Guide



Move Faster



Eliminate Errors



Reduce Cost

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 the VMware (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: <http://www.appviewx.com>

Document Information

Software Version: 12.2.0

Document Version: 1.0

Last updated on: February 20, 2018

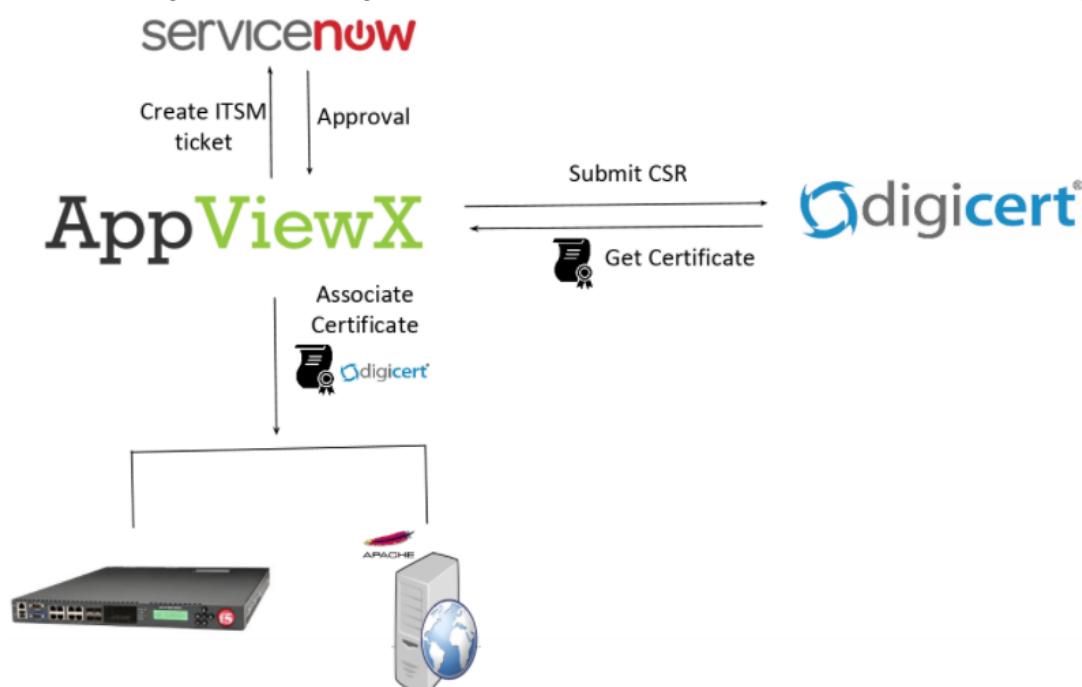
Contents

Description	1
Prerequisites	1
Compatible Software Versions	2
Limitations.....	2
REST API	2
Log In to AppViewX	2
Import Visual Workflows.....	2
Import Helper Scripts	3
Enable the DigiCert Certificate Creation Workflow	3
Add an ADC Device: F5.....	4
Add a Server	6
Configure Certificate Manager Accounts.....	7
Register an ITSM Device: ServiceNow	8
DigiCert Certificate Creation Workflow	9
Work Order Flow	12
Request Inventory	13
Schedule a Workflow	14
View Scheduled Workflows	14
Add a Credential	14
Troubleshooting	15

Description

The DigiCert Certificate Creation workflow is used to enroll the DigiCert Certificate Authority (CA) with all the relevant Certificate Signing Request (CSR) details. On successful enrollment, the certificate will be retrieved from the corresponding CA and managed in the AppViewX Certificate inventory. Based on the user input a new certificate will be pushed manually or automatically to the F5 or Apache server.

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



Prerequisites

To run the DigiCert Certificate Creation workflow in your environment, ensure that the following prerequisites are met:

- Free AppViewX or AppViewX version 12.1.0 and 12.2.0 has been downloaded and installed.
- Each ADC device is a managed entity in AppViewX.
- The DigiCert account information has been configured in AppViewX.
- The Apache server you use is a managed entity in AppViewX
- An ITSM tool (ServiceNow) has been configured under the Change Management section of the AppViewX Settings module
- The DNS server you use must resolve the certificate domain name.
- Uncheck the "Approval required" parameter in the policy of the selected Certificate group to allow auto-implementation of the DigiCert Certificate Creation workflow.
- The standalone script `push_file_to_apache.py` must have been loaded in `~/aps/helper`.

Compatible Software Versions

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

- AppViewX – Free AppViewX, AVX 12.1.0, and AVX 12.2.0
- F5 (both LTM and GTM) – version 11.x and 12.x
- ServiceNow – Istanbul, Geneva, and Jakarta

Limitations

The DigiCert Certificate Creation workflow has the following limitations:

- The duplicate certificates are not handled by an Application connector.
- User must approve F5 Apache Certificate Push and Apache Certificate Push provisioning template.

REST API

Not applicable

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.`

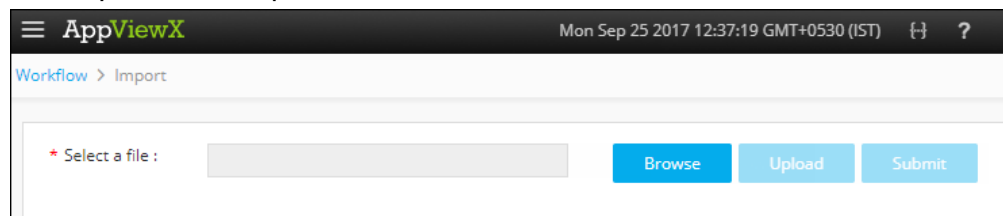
Note: It is recommended that you access AppViewX using Internet Explorer, Firefox, or Google Chrome.

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.

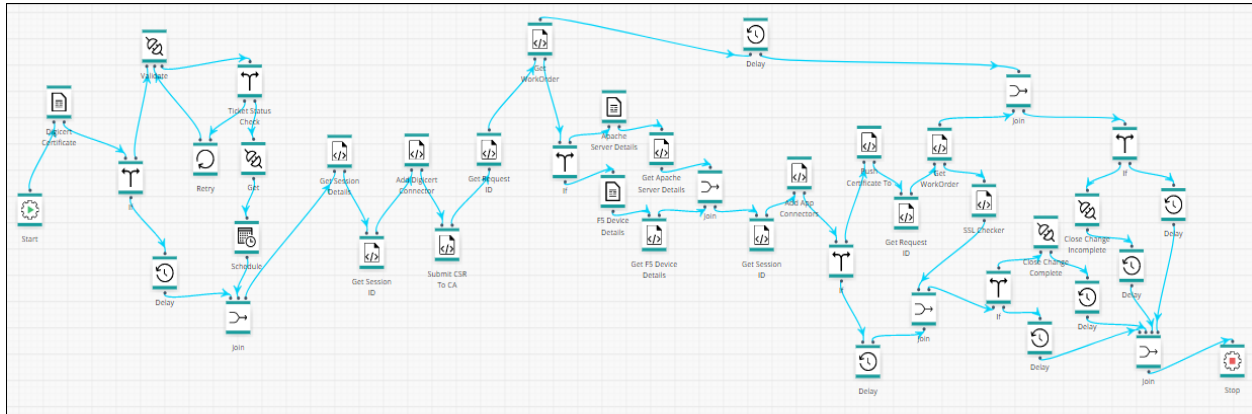
1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Configurator**.
3. Click the  (**Import**) button in the Command bar.

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:



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.


An *Import* screen opens.


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

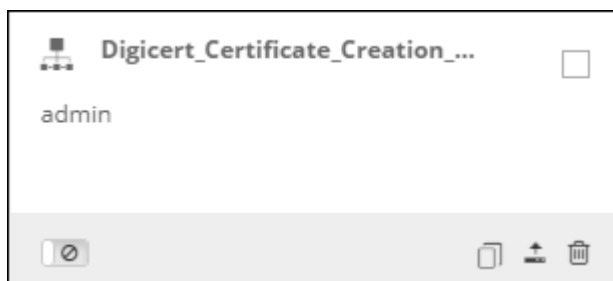
Enable the DigiCert Certificate Creation Workflow

To enable the DigiCert Certificate Creation 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 **DigiCert Certificate Creation** workflow to enable. If the workflow is already selected, a  (**Deselect**) button appears.



- Click the  (Enable) button in the Command bar.

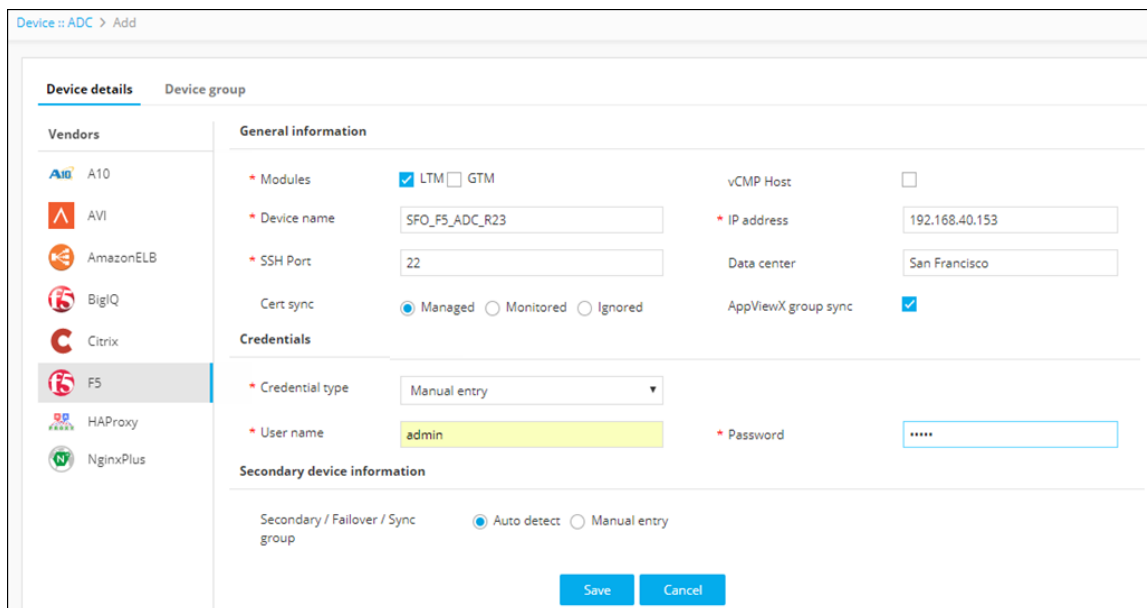
Note: You can also enable the DigiCert Certificate Creation workflow from the Card view by clicking the  (Disable) button.



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

Add an ADC Device: F5

- Click the  (Menu) button.
- Navigate to **Inventory > Device**.
- The *Device* screen opens with the **ADC** tab displayed by default.
- Click the  (Add) button in the Command bar.
- On the *Add* screen that opens, click to select **F5** as the ADC vendor.



- Select the module to be managed on the ADC device.
- Click the **vCMP Host** check box, if you want to add and manage the vCMP guest devices.
- Create a **Device name** that is specific to AppViewX and that will identify the device in the AppViewX inventory.
- Enter the **management IP address** of the device.
- Enter the default or custom defined **SSH port** number for the device.

11. (Optional) Specify a **Data center location** if you want to have the option later to filter devices based on their location.
12. 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**.
13. (Optional) Select the **AppViewX group sync** check box if you need AppViewX to sync the configuration changes of an active to standby ADC device.
Note: This is required in older F5 versions like v10. The latest versions of an F5 device will sync automatically.
14. 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.
15. 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.
16. 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.
17. 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.

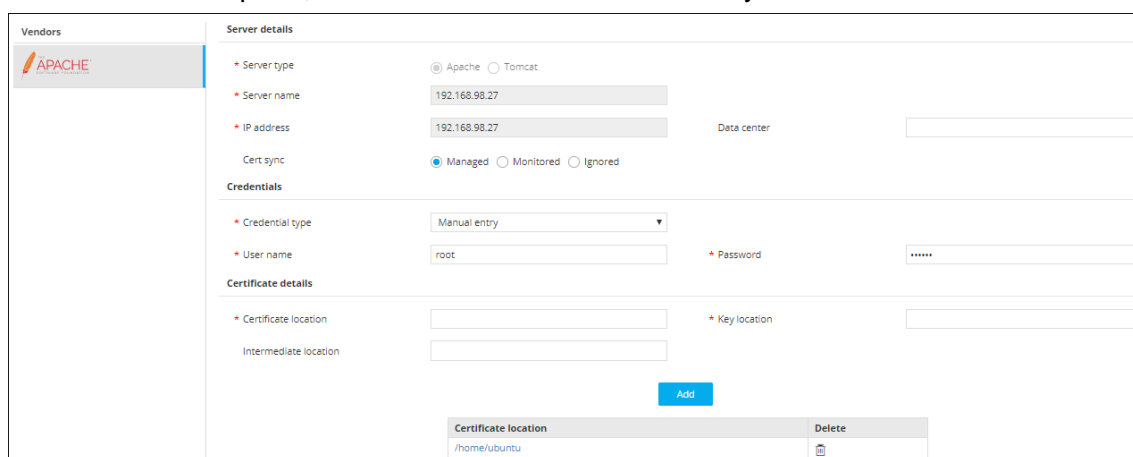
- **Unresolved** – Unable to communicate with device due to invalid login credentials.
- **Failed** – Device configuration fetch failed due to unsupported version.

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.



The screenshot shows the 'Add Server' form in AppViewX. The form is titled 'Server details' and is for an Apache server. It includes fields for Server type (Apache selected), Server name (192.168.98.27), IP address (192.168.98.27), Data center, Cert sync (Managed selected), Credentials (Manual entry selected), User name (root), Password (masked), Certificate location, Intermediate location, and Key location. An 'Add' button is at the bottom right. A table at the bottom shows the Certificate location as '/home/ubuntu' with a 'Delete' button.

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 [Add a Credential](#) 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...




<div><div></div></div>	Name	IP address	Data center	Vendor	Status	Credential type
<div><div></div></div>	<div><div></div>192.168.98.27</div>	192.168.98.27		<div><div></div>Apache</div>	<div><div></div>Managed</div>	Manual entry
<div><div></div></div>	<div><div></div>192.168.99.8</div>	192.168.99.8		<div><div></div>Apache</div>	<div><div></div>Managed</div>	Manual entry

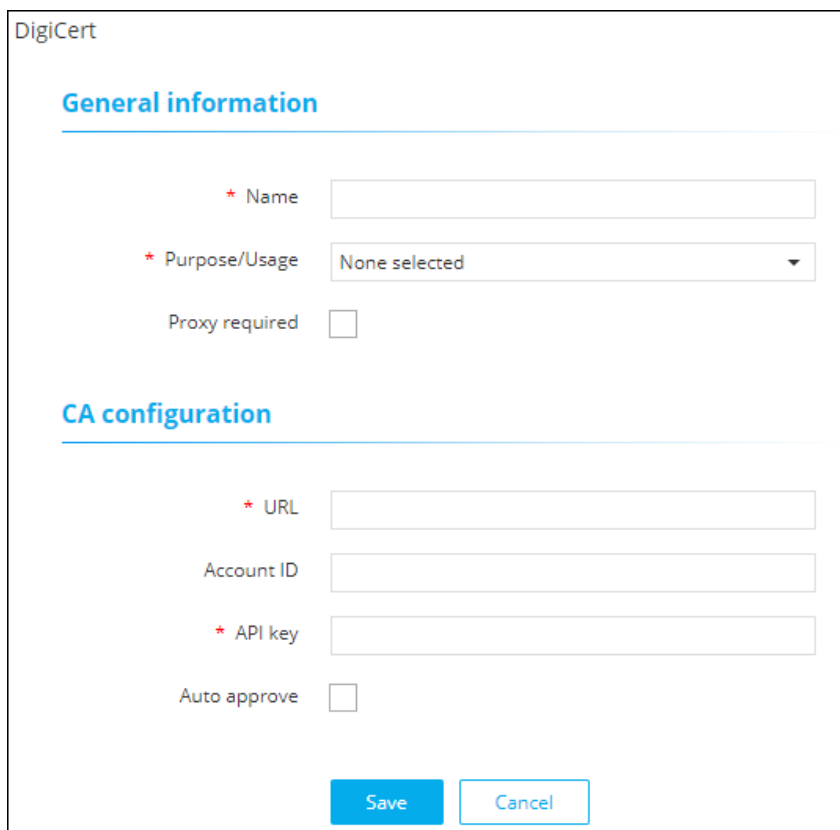
The device will display one of the following statuses:

- **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.

Configure the Certificate Manager Accounts

To configure DigiCert 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 **digicert** tab to configure the certificate manager account.
7. On the *Certificate authority* screen that appears, click the  (**Add**) button.
8. At a minimum, complete all fields designated with a red asterisk (*).



The image shows a DigiCert configuration form with two sections: 'General information' and 'CA configuration'. The 'General information' section includes a required 'Name' text field, a required 'Purpose/Usage' dropdown menu currently set to 'None selected', and an optional 'Proxy required' checkbox. The 'CA configuration' section includes a required 'URL' text field, an 'Account ID' text field, a required 'API key' text field, and an optional 'Auto approve' checkbox. At the bottom right of the form are 'Save' and 'Cancel' buttons.

DigiCert

General information

* Name

* Purpose/Usage None selected

Proxy required ☐

CA configuration

* URL

Account ID

* API key

Auto approve ☐

Save **Cancel**

9. Click **Save**. The DigiCert certificate manager account you added will be displayed in the table.

Register an ITSM Device: ServiceNow

1. In the navigation menu on the left-hand side of the AppViewX screen, navigate to **Settings**.
2. On the *Settings* screen that opens, click **Change Management** in the column on the left.
3. Click the **ServiceNow** plug-in.
4. On the *Vendor configuration* screen that opens, enter a valid web URL.
5. (Optional) Enter a **Description** of the vendor to help users identify it.
6. Enter the ServiceNow **username** and **password** credentials in the respective fields.
7. Click **Update** to save the changes made in the system.

The screenshot shows the 'Vendor configuration' page in ServiceNow, specifically the 'Change Management' section. The left sidebar lists various configuration areas: Authentication, SSH, Certificate, Provisioning, Change Management (selected), ADC, Backup & Restore, Log forwarding, License, System, and AppViewX. The main content area is divided into 'Information' and 'General settings'.

Information:

- Name: Change
- Description: (empty field)
- URL: https://ven01189.service-now.com
- Upload image: (button with 'X' icon)
- Username: admin
- Password: (masked field)

General settings:

- Active Provisioning Instance: ☒
- Device / CI validation: ☐
- Timezone: GMT
- Implementation mode: Stop
- Enable polling: ☐
- Polling interval (mins): 5
- Approve mode: Stop

Log / Configuration settings:

- Select configuration type: Pre validation, Post validation
- Consolidated logs: ☒



8. (Optional) The F5 LTM device you are configuring should be present in the ServiceNow LB Hardware inventory. You can check this by opening ServiceNow and clicking to open the **Load Balancers > LB Hardware** section shown below. The device name used in the ServiceNow inventory and AppViewX ADC device inventory should be the same.

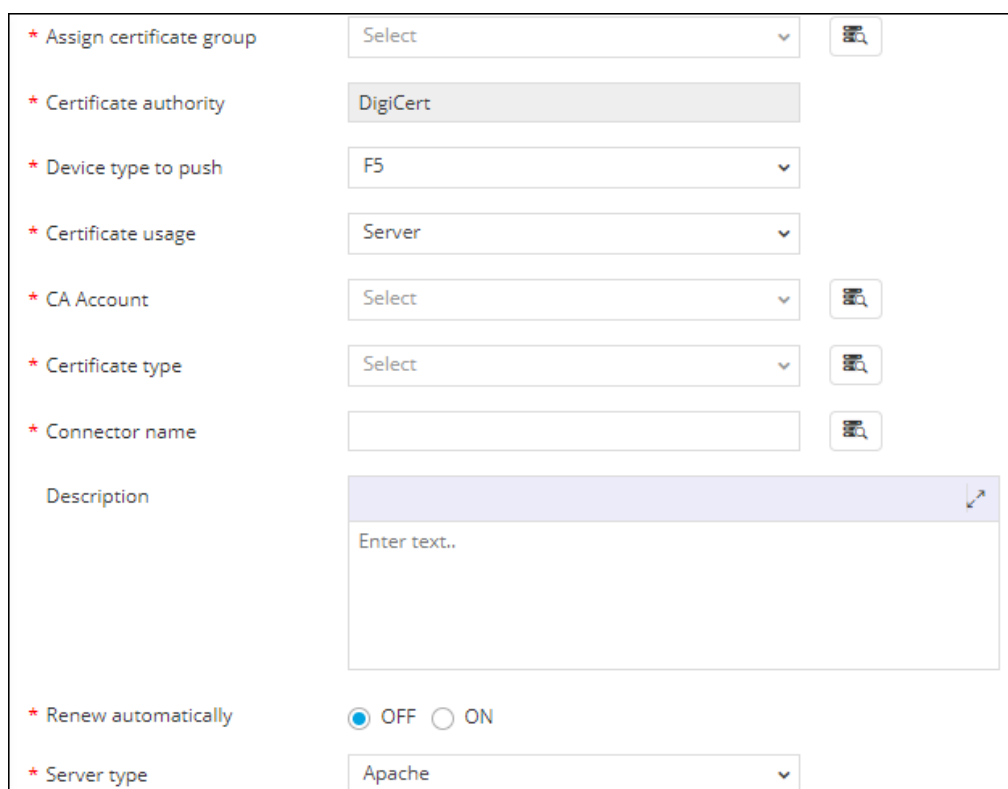
The screenshot shows the ServiceNow Service Automation interface. The top navigation bar includes the ServiceNow logo, 'Service Automation', a search bar, and a 'Logout' button. The main content area is titled 'Load Balancer - 112.40'. The left sidebar shows a 'Configuration' menu with 'Load Balancers' expanded, highlighting 'LB Hardware' and 'LB Applications'. The main content area displays the configuration for a specific Load Balancer:

- Name: SFO_F5_ADC_R23
- Company: (empty field)
- Asset tag: (empty field)
- Manufacturer: (empty field)
- Asset: (empty field)
- IP Address: 192.168.40.153
- Host name: (empty field)
- Serial number: (empty field)
- Model ID: (empty field)
- Assigned to: (empty field)





DigiCert Certificate Creation Workflow



To submit the DigiCert Certificate Creation workflow, complete the following steps:





1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Request**.
3. The *Request* screen opens with the **My catalog** tab displayed by default. This screen displays all enabled workflows assigned to a specific user role.
4. Click the  (**Run workflow**) button for DigiCert Certificate Creation. The *FormBuilder* screen opens.





The screenshot shows a form for creating a DigiCert certificate. It includes several dropdown menus and a text area. The fields are: 'Assign certificate group' (dropdown with 'Select'), 'Certificate authority' (dropdown with 'DigiCert'), 'Device type to push' (dropdown with 'F5'), 'Certificate usage' (dropdown with 'Server'), 'CA Account' (dropdown with 'Select'), 'Certificate type' (dropdown with 'Select'), 'Connector name' (text input), 'Description' (text area with 'Enter text..'), 'Renew automatically' (radio buttons for 'OFF' and 'ON'), and 'Server type' (dropdown with 'Apache'). Each dropdown menu has a 'Retrieve field values' button (represented by a small icon) to its right.

5. In the **Assign certificate group** field, click the  (**Retrieve field values**) button to fetch the list of available groups and select the required group to which the certificate will be assigned.
6. The Certificate authority is automatically displayed as DigiCert.
7. From the **Device type to push** dropdown list, select the device to which you want to push the certificate.
8. From the **Certificate usage** dropdown list, select the type of certificate you want to use for DigiCert creation.
9. In the **CA Account** field, click the  (**Retrieve field values**) button to fetch the list of CA accounts that are configured under AppViewX and select the required account from where you want the certificate to be generated.
10. In the **Certificate type** field, click the  (**Retrieve field values**) button to fetch the list of available certificates at AppViewX and select the required type of certificate which you want to be created.
11. In the **Connector name** field, click the  (**Retrieve field values**) button to fetch the connector that is associated with the type of certificate you selected.
12. (Optional) Enter a description for the connector. This description shows up when you hover your cursor over the connector within the Certificate topology.
13. If you want certificates to be renewed automatically select the **ON** radio button and enter the number of days you want the certificate to be valid.
14. From the **Server type** dropdown list, select the type of server to which you want the certificate to be pushed.

15. From the **Key type** dropdown list, select either RSA or DSA depending on the type of security algorithm you want to use.
16. In the **Bit length** field, click the  (**Retrieve field values**) button to fetch the list of dimensions corresponding to the selected key and choose the required length of the key you want to generate.
17. In the **Common name** field, enter the fully qualified domain name (FQDN) or common name that exactly matches your web browser.
18. Enter the name of the organization requesting the certificate.
19. The remaining fields are optional and can be used later to help distinguish between multiple policies within the system:
 - a. **Organizational unit** – The division for the organization requesting the certificate.
 - b. **Organization address** – The location for the organization requesting the certificate.
 - c. **City** – The city in which the organization is located.
 - d. **State** – The state in which the organization is located.
 - e. **Country** – The country in which the organization is located.
 - f. **ZIP Code** – The postal code of the organization.
 - g. **Email ID** – The email contact details for the person responsible for maintaining the certificate.
20. In the **Validity** field list, click the  (**Retrieve field values**) button to fetch the list of duration period (in years) and select how long you want the certificate to be valid.

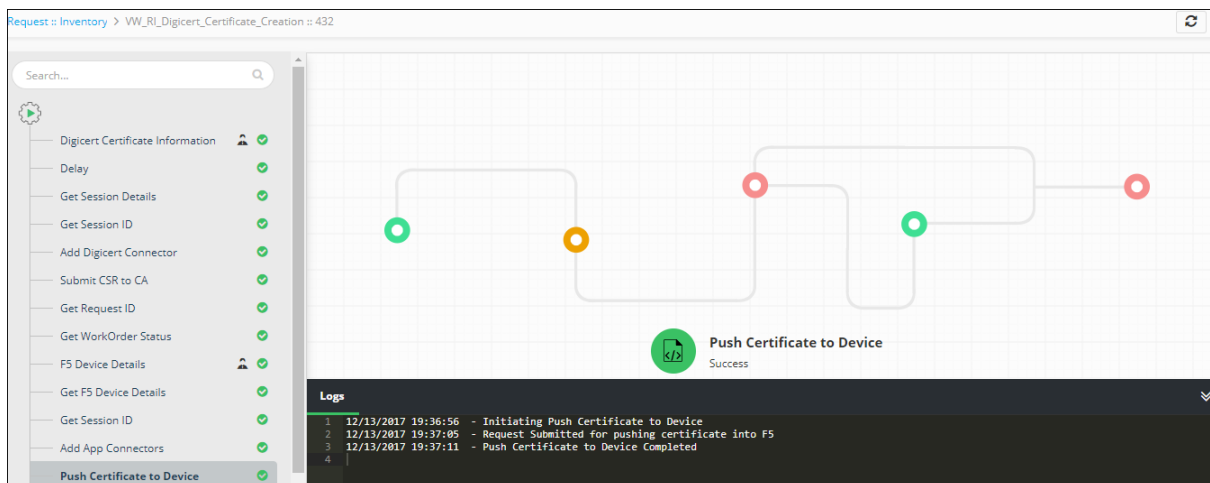
* Validity	Select	
Challenge password	<input type="text"/>	
Confirm password	<input type="text"/>	
* Hash function	Select	
* Integrate with SNOW?	<input checked="" type="radio"/> Yes <input type="radio"/> No	
* Time Zone	Select	
* Start Time	<input type="text"/>	
* End Time	<input type="text"/>	
<div>Create SNOW Ticket</div>		
* CChange ID	<input type="text"/>	
* AppViewX Username	<input type="text"/>	
* Password	<input type="text"/>	

21. Enter the challenge password and confirm password in the corresponding fields using which you can access the key.
22. From the **Hash function** dropdown list, select either **SHA256** or **SHA160**, depending on which hash algorithm you want to use.
23. Depending on whether or not you want to integrate the ITSM tool – ServiceNow, select the **Yes** or **No** radio button. To integrate the ITSM tool, enter the following details:
 - a. In the **Time Zone** dropdown list, click the  (**Retrieve field values**) button to retrieve the time zone. Select the time zone for the F5 LTM device that you are configuring.
 - b. Schedule the service window time and date using the **Start Date** and **End Date** fields. Click the  (**Calendar**) button to select the start and end date respectively. Configuration changes will be implemented during this service window.
24. Click the **Create SNOW Ticket** button to retrieve the ticket number. The ticket number automatically appears in the **Change ID** field.
25. Enter the AppViewX username and its associated password of the user who is trying to create the DigiCert Certificate.
26. Click **Submit**.
A new **Request ID** is created. To view all requests, refer to the [Request Inventory](#) section of this guide.

Work Order Flow

The following are the workorder tasks of DigiCert Certificate Creation 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. **Add DigiCert Connector** — The CA Connector is created for the certificate with a common name you mentioned in the form field.

3. **Get Request ID** — The CSR is created and submitted to the CA through the provisioning templates.
4. **Get WorkOrder Status** — The workorder status regarding implementation of the provisioning templates (for CSR creation) will be displayed.
5. **F5 Device Details** — Information such as the device name, SSL profile, certificate and its associated key file name, and whether the certificate is pushed manually or automatically to the f5 device are displayed.
6. **Apache Device Details** — Apache server information such as name, certificate and its associated key file name, FQDN, configuration file path and file name, and whether the certificate is pushed manually or automatically to the server.
7. **Add App Connectors** — The Application Connector is created for the certificate with a common name you mentioned in the form field.
8. **Push Certificate to Device** — A provisioning template is created to push the certificate to the corresponding device you selected.
9. **Get Request ID** — The request is created and submitted to push the certificates through the provisioning templates.
10. **Get WorkOrder Status** — The workorder status regarding implementation of the provisioning templates (to push the certificate) will be displayed.
11. **SSL Checker** — The SSL checker will validate the certificate that is created.


Request Inventory

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


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

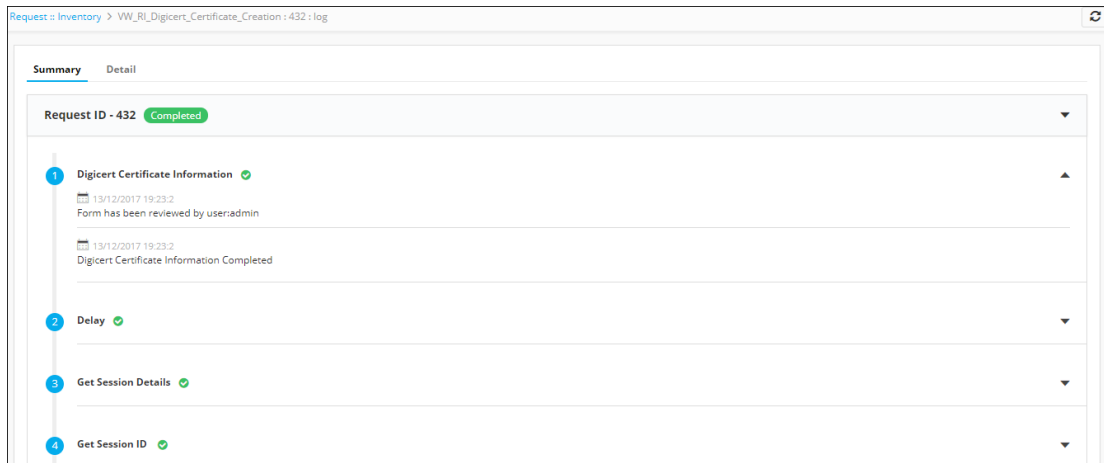
The *Request* screen opens with **My catalog** tab displayed by default.

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.



My catalog Request Inventory Scheduled workflows							
<input type="text" value="Search..."/> ▼							
Request ID	Workflow	Created by	Created time	Last updated	Status	Activity log	
432	VW_RI_Digicert_Certificate_Creati...	admin	13/12/2017 07:23 PM	13/12/2017 07:23 PM	Completed	View	
416	VW_RI_Digicert_Certificate_Creati...	admin	13/12/2017 04:38 PM	13/12/2017 04:38 PM	Failed	View	

4. Click the **Request ID** created for DigiCert Certificate Creation to view the tasks or phases of a request in a tree-view. For more details, refer to the [Work Order Flow](#) section of this guide.
5. You can also view the following details of the request that was created: request creator, request time, last updated time, status, and 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.






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 **My catalog** tab displayed by default.
3. Click the  (**Schedule workflow**) button on the DigiCert Certificate Creation workflow.
4. On the ASM Policy 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 the **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.

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.

Troubleshooting

I cannot find the DigiCert Certificate Creation 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 the DigiCert Certificate Creation Workflow](#) section of this guide.