Golden Configuration on F5 BIG-IP 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: 12.4.0

Document Version: 1.0

Last updated on: September 27, 2018

Contents

1 Description

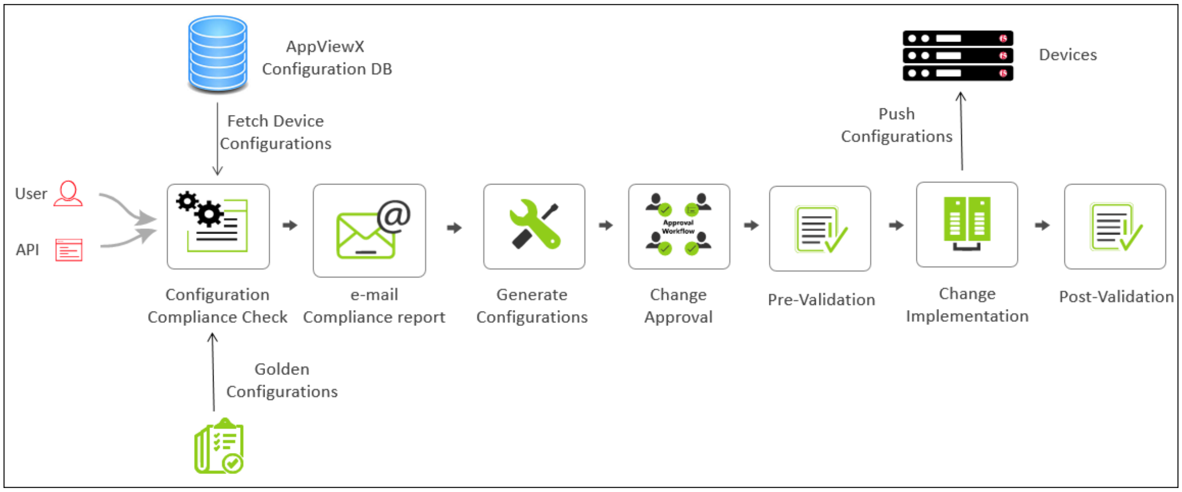
The Golden Configuration Compliance on F5 BIG-IP workflow is used to run a compliance check across all the managed F5 BIG-IP devices. The device configurations are checked against the pre-loaded golden configurations. The commands are executed to list out the information about the following objects:

- DNS Server
- NTP Server
- Banner
- SNMP Traps
- Syslog
- Timezone
- Management – Route IP
- Profile
- Persistence

For each of the objects in every device, the script will compare whether the expected parameters are compliant or not. Based on the final output, an Excel report will be generated along with color coded fields to highlight the results, which will be mailed to the user. For SNMP Traps, Syslog and Profile, the sheet will simply state Non-compliant. For the remaining objects, the user will get a list of objects already present. If the object for that particular device is compliant, the sheet will be updated as Compliant.

Following this, the commands generated will be implemented/rolled back after approval.

The flow diagram for the Enforce Golden Configuration workflow is shown in the image below:



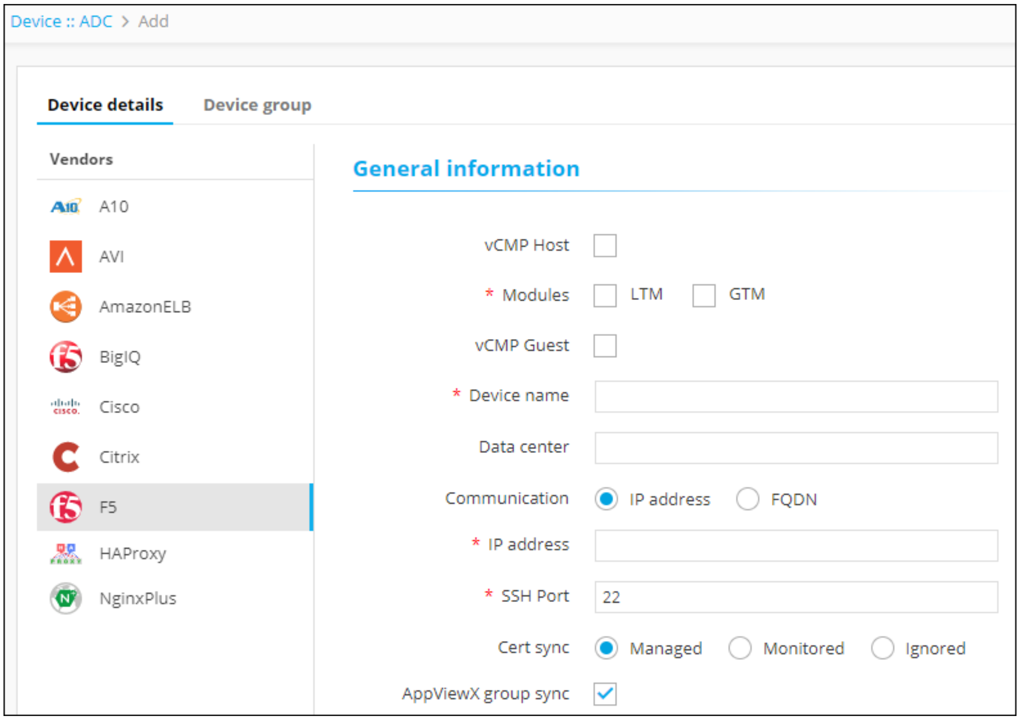
2 Prerequisites

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

- An F5 device (LTM/GTM) has been added to AppViewX as a managed device.
- The Excel sheet has been updated and uploaded in Provisioning > Collections.
- Each F5 device has been pre-configured with the given objects.

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.



vCMP Host □

* Modules □ LTM □ GTM

vCMP Guest □

* Device name

Data center

Communication ● IP address ○ FQDN

* IP address

* SSH Port 22

Cert sync ● Managed ○ Monitored ○ Ignored

AppViewX group sync ☑

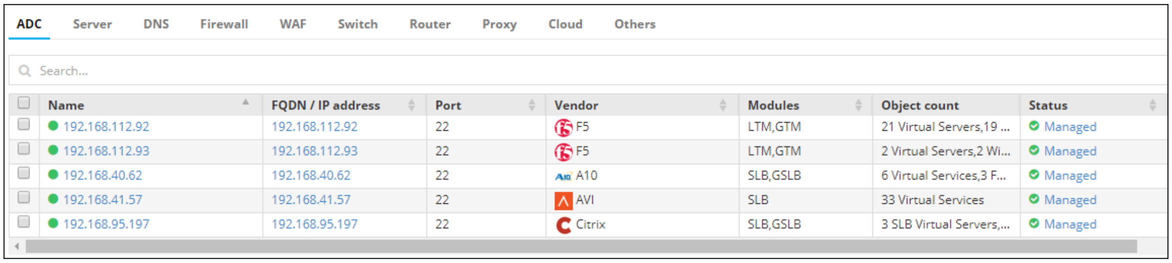
6. Click the **vCMP Host** check box, if you want to add and manage the vCMP host devices
7. Select the module to be managed on the ADC device.
8. Click the **vCMP Guest** check box, if you want to add and manage the vCMP guest devices.
9. Create a **Device name** that is specific to AppViewX and that 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.



□	Name	FQDN / IP address	Port	Vendor	Modules	Object count	Status
□	● 192.168.112.92	192.168.112.92	22	F5	LTM,GTM	21 Virtual Servers,19 ...	✓ Managed
□	● 192.168.112.93	192.168.112.93	22	F5	LTM,GTM	2 Virtual Servers,2 Wi...	✓ Managed
□	● 192.168.40.62	192.168.40.62	22	A10	SLB,GSLB	6 Virtual Services,3 F...	✓ Managed
□	● 192.168.41.57	192.168.41.57	22	AVI	SLB	33 Virtual Services	✓ Managed
□	● 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 Upload Golden Configuration

To upload the golden configuration file to Collection, complete the following steps:

1. Click the ☰ (**Menu**) button on the left-hand side of the AppViewX screen
2. Navigate to **Provisioning** > **Collection**.
3. Click the ⇩ (**Import**) button.
4. Click the **Browse** button and select the golden configuration file that you want to upload.
5. Click **Upload**.

3 Compatible Software Versions

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

- AppViewX –12.4.0
- F5 – V11.x, 12.x, and 13.x

4 Limitations

This workflow has the following limitations:

- Unmanaged devices will not be supported.
- Only the HTTP profile will be replaced during an execution.
- The fast L4 VIPs are not in scope.
- Before implementation, the existing profile and persistence must exist and be compatible. Else, an error will occur during a roll back.

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 Golden Configuration Compliance on F5 BIG-IP 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`.

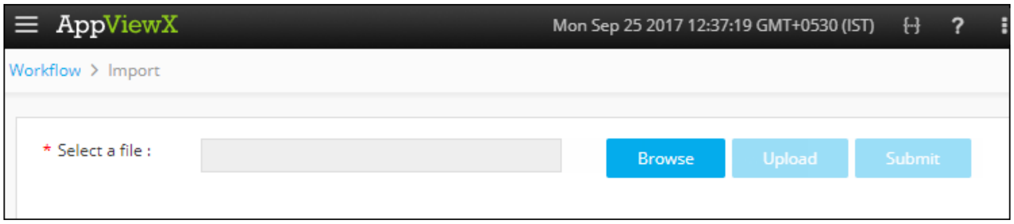
Note: It is recommended that you access AppViewX using the latest version of Internet Explorer, Firefox, or Google Chrome.

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**.

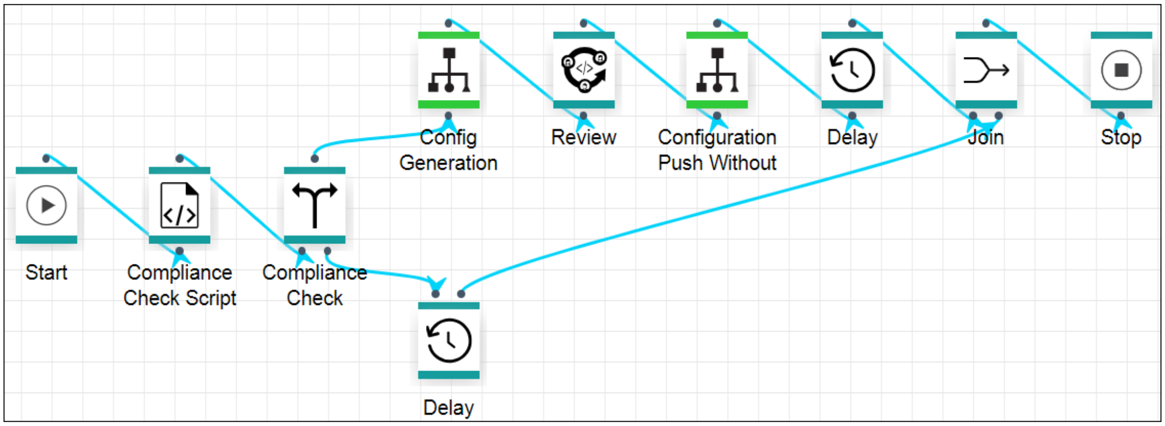
3. Click the (**Import**) button in the Command bar.
   The *Import* screen opens.



* Select a file :

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.

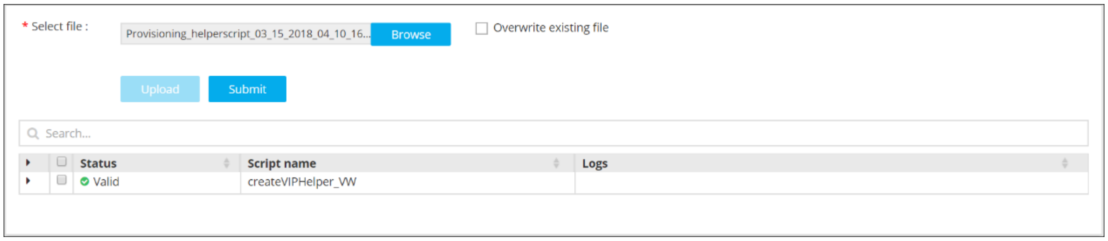
The DigiCert Certificate Creation workflow is shown in the image below:



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.



* Select file : Provisioning_helperscript_03_15_2018_04_10_16...

	□	Status	Script name	Logs
	□	✓ Valid	createVIPHelper_VW	

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

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

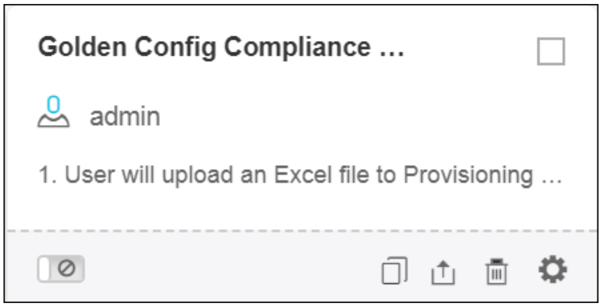
5.4 Enable the Golden Configuration Compliance on BIG-IP Workflow

To enable the Golden Configuration Compliance on F5 BIG-IP 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 **Golden Configuration Compliance on BIG-IP** 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.



Golden Config Compliance ... □

admin

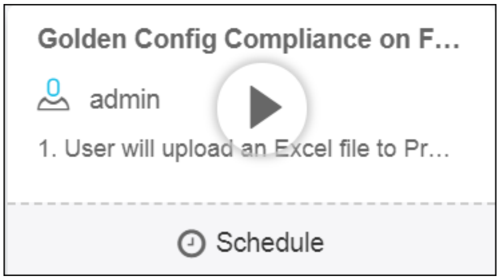
1. User will upload an Excel file to Provisioning ...

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

6 Golden Configuration Compliance on BIG-IP Workflow

To submit the Golden Configuration Compliance on BIG-IP 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 Golden Configuration Compliance on BIG-IP workflow to execute.



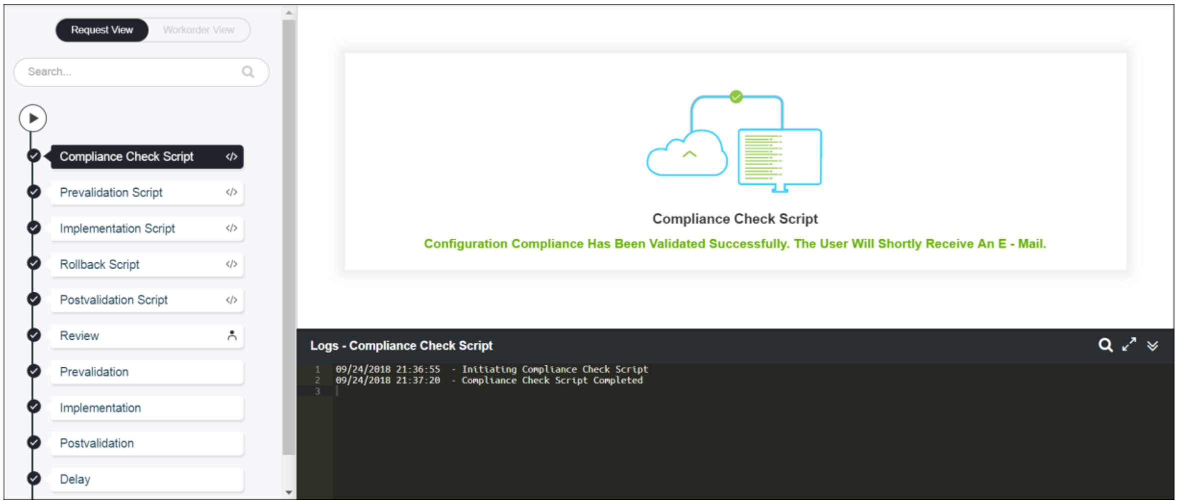
1. User will upload an Excel file to Pr…

The workflow execution begins.

6.1 Work Order Flow

The following are the workorder tasks of Golden Configuration Compliance on BIG-IP 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.



Configuration Compliance Has Been Validated Successfully. The User Will Shortly Receive An E - Mail.

```
09/24/2018 21:36:55  - Initiating Compliance Check Script
09/24/2018 21:37:20  - Compliance Check Script Completed
```

1. **Compliance Check Script —** The configuration compliance is validated and an email is sent to the user.
2. **Prevalidation Script —** The prevalidation configurations are generated.
3. **Implementation Script —** The implementation script is triggered to generate the configurations.
4. **Rollback Script —** The rollback configurations are generated.
5. **Postvalidation Script —** The postvalidation configurations are generated.
6. **Review —** The user can review the scripts that have been triggered.
7. **Prevalidation**, **Implementation**, **and Postvalidation —** These actions are completed based on the corresponding scripts that were triggered.
8. **Delay —** The next task is resumed after the delay time elapses.

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**.

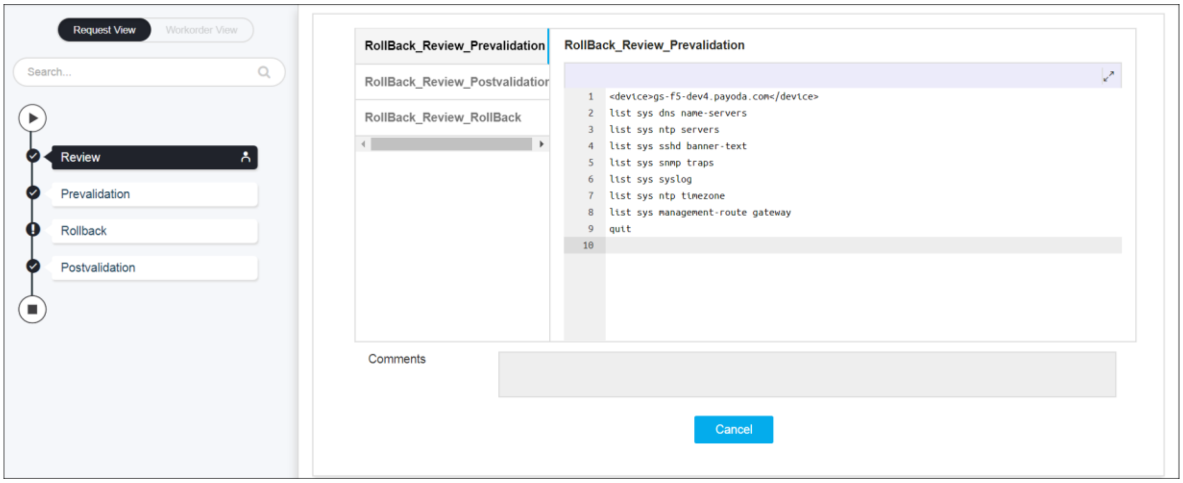
   The *Request* screen opens with **Workflow dashboard** displayed by default.
3. Click the **All** tab in **My requests** section.

   This displays all workflows that have been triggered. On the request inventory screen, you can search for a request created for Golden Configuration Compliance on BIG-IP 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 Rollback Flow

The following are the workorder tasks of Golden Configuration Compliance on BIG-IP 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.



```
<device>gs-f5-dev4.payoda.com</device>
list sys dns name-servers
list sys ntp servers
list sys sshd banner-text
list sys snmp traps
list sys syslog
list sys ntp timezone
list sys management-route gateway
quit

```

1. **Review —** The user can review the rollback scripts. The review of a work order is based on the role assigned to the user, who has access to approve and implement. After you submit the request form, the configuration changes are reviewed and approved at AppViewX. Configuration changes are implemented on the device only after approval is received.
2. **Prevalidation** – The prevalidation checks are executed.
3. **Rollback** – The configuration commands are rollbacked, resulting in the recreation of a objects deleted in the forward flow.
4. **Postvalidation —** The postvalidation checks are triggered.

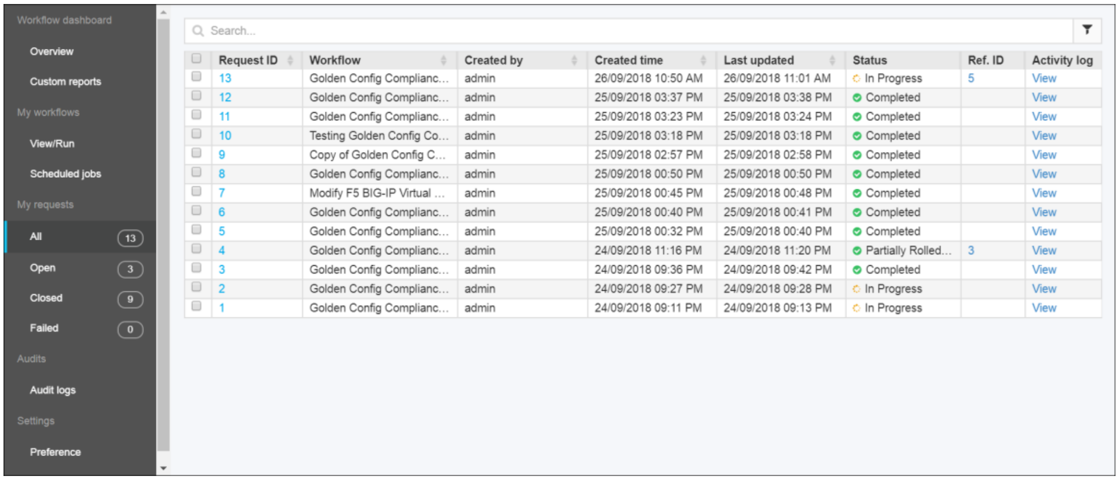
8 Request Inventory

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.

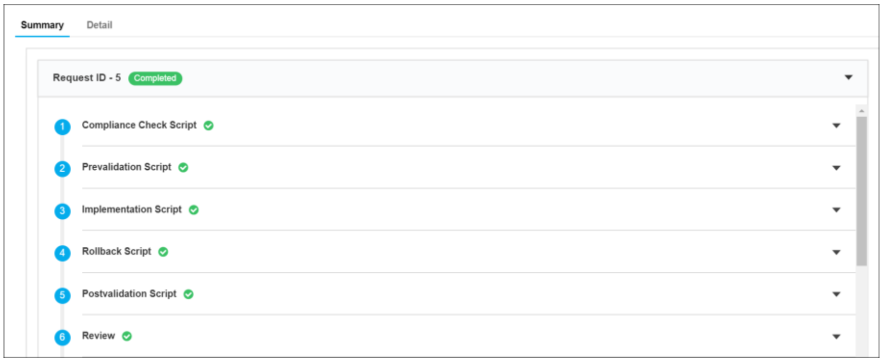
   This displays all workflows that have been triggered. On the **Request Inventory** screen, you can search for a request using the **Search** field and/or click the ▼ (**Filter**) button to select the options you want to use to sort the requests.



□	Request ID	Workflow	Created by	Created time	Last updated	Status	Ref. ID	Activity log
□	13	Golden Config Complianc...	admin	26/09/2018 10:50 AM	26/09/2018 11:01 AM	In Progress	5	View
□	12	Golden Config Complianc...	admin	25/09/2018 03:37 PM	25/09/2018 03:38 PM	✓ Completed		View
□	11	Golden Config Complianc...	admin	25/09/2018 03:23 PM	25/09/2018 03:24 PM	✓ Completed		View
□	10	Testing Golden Config Co...	admin	25/09/2018 03:18 PM	25/09/2018 03:18 PM	✓ Completed		View
□	9	Copy of Golden Config C...	admin	25/09/2018 02:57 PM	25/09/2018 02:58 PM	✓ Completed		View
□	8	Golden Config Complianc...	admin	25/09/2018 00:50 PM	25/09/2018 00:50 PM	✓ Completed		View
□	7	Modify F5 BIG-IP Virtual ...	admin	25/09/2018 00:45 PM	25/09/2018 00:48 PM	✓ Completed		View
□	6	Golden Config Complianc...	admin	25/09/2018 00:40 PM	25/09/2018 00:41 PM	✓ Completed		View
□	5	Golden Config Complianc...	admin	25/09/2018 00:32 PM	25/09/2018 00:40 PM	✓ Completed		View
□	4	Golden Config Complianc...	admin	24/09/2018 11:16 PM	24/09/2018 11:20 PM	✓ Partially Rolled...	3	View
□	3	Golden Config Complianc...	admin	24/09/2018 09:36 PM	24/09/2018 09:42 PM	✓ Completed		View
□	2	Golden Config Complianc...	admin	24/09/2018 09:27 PM	24/09/2018 09:28 PM	In Progress		View
□	1	Golden Config Complianc...	admin	24/09/2018 09:11 PM	24/09/2018 09:13 PM	In Progress		View

4. Click the **Request ID** created for **Golden Configuration Compliance on BIG-IP** to view its details.

   The screen opens with the **Request View** tab selected by default.
   a. After the workflow execution is complete, the **Request View** tab displays the tasks or phases of a request in a tree view. For more details, refer to the Work Order Flow section of this guide.
   b. Click the **Workorder View** tab to view the work order details such as work order ID, date and time when the work order was created and updated, status, RFC ID, and RFC status.
5. In the *Request Inventory* screen, you can also view the following details of the request: request creator, request time, last updated time, status, and activity log.
6. Click **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 ID - 5 Completed

1 Compliance Check Script ✓
2 Prevalidation Script ✓
3 Implementation Script ✓
4 Rollback Script ✓
5 Postvalidation Script ✓
6 Review ✓

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 **Golden Configuration Compliance** 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 Golden Configuration Compliance on F5 BIG-IP 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 Golden Configuration Compliance on BIG-IP Workflow section of this guide.