

# Generic Firewall Workflow Guide



Move Faster

Reduce Cost

Eliminate Errors

**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](http://www.centos.org)).

This product includes software developed by Red Hat, Inc. ([www.redhat.com](http://www.redhat.com)).

This product includes software developed by the VMware ([www.vmware.com](http://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](mailto:info@appviewx.com) Web:

<http://www.appviewx.com>

**Document Information**

Software Version: 12.2.0

Last updated on: April 10, 2018

Document version: WIP 2.1

## Contents

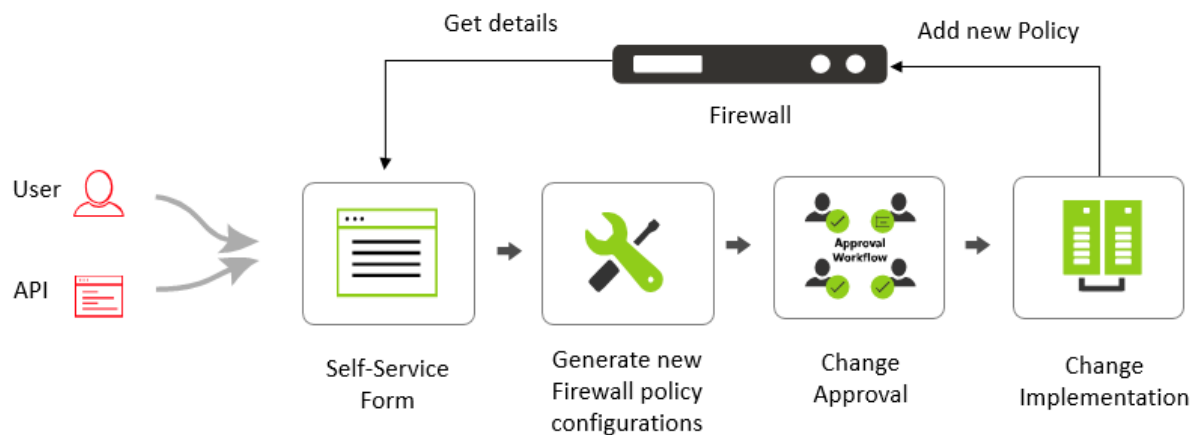
Description .....	1
Prerequisites .....	1
Compatible Software Versions .....	1
Limitations .....	2
Log In to AppViewX.....	2
Import Visual Workflows.....	2
Import Helper Scripts .....	3
Add an Firewall Device.....	3
Enable the Workflow .....	5
Generic Firewall Workflow.....	5
Work Order Flow .....	9
Request Inventory .....	9
Schedule a Workflow .....	10
View Scheduled Workflows .....	10
Add a Credential .....	11
Troubleshooting .....	11

## Description

The Generic Firewall workflow allows users to create firewall policies across multiple vendors such as Check Point, Cisco ASA, Fortinet, Juniper, and Palo Alto. This workflow is used to perform the following tasks:

- Create source objects and group them
- Create destination objects and group them
- Create service objects and group them
- Create a policy with the created objects

The flow diagram for the Generic Firewall workflow is shown in the image below:



## Prerequisites

To run this automation workflow in your environment, ensure that the following pre-requisites are met:

- Free AppViewX or AppViewX version 12.1.0 and 12.2.0 has been downloaded and installed.
- The Firewall devices have been added in the AppViewX inventory.
- Each Firewall device must be a managed entity in AppViewX inventory.

## Compatible Software Versions

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

- AppViewX – Free AppViewX, AVX 12.1.0, and AVX 12.2.0
- Check Point – version R80
- Cisco – version 8.x, or 9.x
- Fortinet – version 5.2.x
- Juniper – version 12.1.x
- Palo Alto – version 7.0.1

## Limitations

Not applicable.

## 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.`

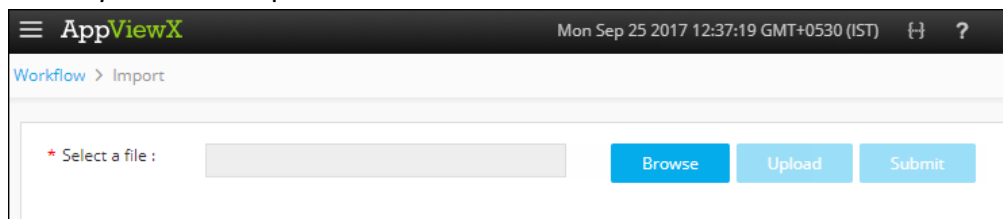
**Note:** It is recommended that you access AppViewX using Internet Explorer, Firefox, or Google Chrome.

## Import 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.

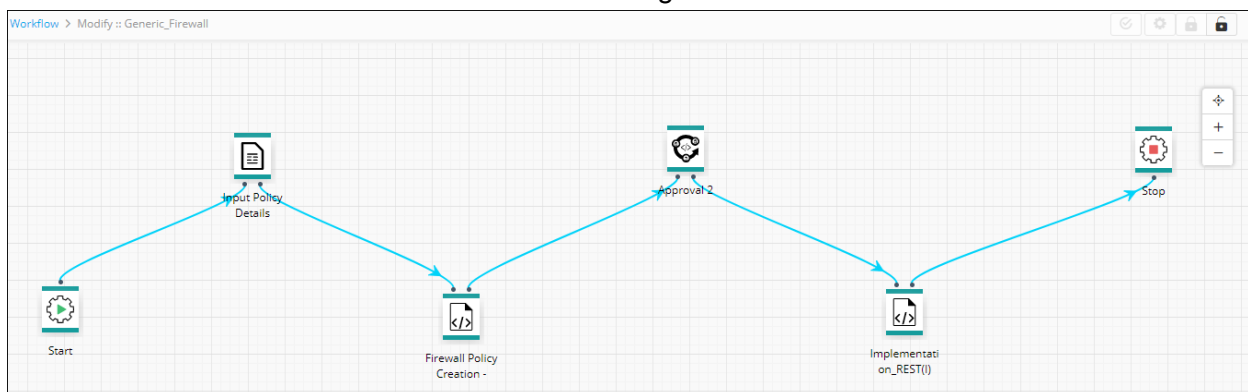
1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Configurator**.
3. Click the  (**Import**) button in the Command bar.

The *Import* screen opens.





4. On the *Import* screen that opens, complete the following steps:
  - a. Click the **Browse** button.
  - b. Select the zip file containing one or more workflows, then click **Upload**.
  - c. In the table at the bottom of the Import page, select the check box beside the unzipped workflow file.
  - d. Click **Submit** to deploy the workflow into your AppViewX environment.

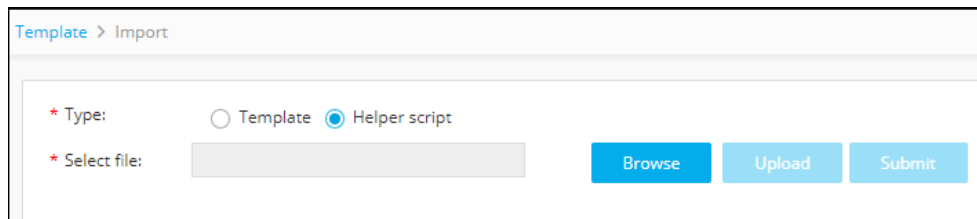
The Generic Firewall workflow is shown in the image below:



## Import Helper Scripts


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


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



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

## Add an Firewall Device

1. Click the  (**Menu**) button.
2. Navigate to **Inventory > Device**.

The *Device* screen opens with the **ADC** device inventory displayed by default.
3. Click the **Firewall** tab.
4. Click the  (**Add**) button in the Command bar.
5. On the *Add* screen opens, listing in the left-hand column each vendor supported by AppViewX.
6. Click the vendor name whose device you want to add.
7. In the **CI name** field, enter the asset number of the device used for provisioning.
8. Select the platform corresponding to the vendor from the dropdown list.
9. Enter a **device name** that is specific to AppViewX and that will identify the device in the AppViewX inventory.
10. Enter the **IP address** of 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. (Only applicable for Cisco, Fortinet, Juniper, and PaloAlto) Enter a name for the policy to which you want to associate the device.
13. 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.  
(Only applicable for Checkpoint) Enter a password used for accessing the expert mode.  
(Only applicable for Cisco) Enter a password used for accessing the privilege mode.
  - 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.
  - c. From the **Access type** dropdown list, select one of the following method: **API** or **SSH**  
This enables AppViewX communicate with the device and fetch its configuration details, after the device is in a manage state.
14. 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.
15. 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 device.

ADC   Server   DNS <u>Firewall</u> WAF   Switch   Router   Proxy   Cloud   Others								
Q Search...								
Name	FQDN / IP address	Vendor	Data center	Status	Rules count	Policy name	Version	
13.57.85.216	13.57.85.216	Fortinet		Unresolved	0	fortigate_policy1		
gs-f5-dev1b.payoda.com	172.16.24.54	F5		Available	0		11.5.4 build 0.0.256	
172.16.24.69	172.16.24.69	F5		Managed	4	/Common/afm_l(172.	11.5.4 build 0.0.256	
192.168.12.21	192.168.12.21	PaloAlto		Managed	1	test1	8.0.0	
192.168.12.249	192.168.12.249	CheckPoint		Failed	0			
192.168.12.250	192.168.12.250	CheckPoint		Failed	0		R77.30 - Build 009	
192.168.12.38	192.168.12.38	CheckPoint		Failed	0			
192.168.41.46	192.168.41.46	PaloAlto		Managed	2	PolicyPA	6.1.0	
PA	192.168.41.98	PaloAlto	dc	Managed	67	PA_policy	7.0.1	
PA_202	192.168.55.202	PaloAlto		Managed	19	pa_policy	8.0.0	
192.168.55.78	192.168.55.78	PaloAlto		Unresolved	0	test		
gs-f5-sme3b.payoda.com	192.168.99.35	F5		Unresolved	0			



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.

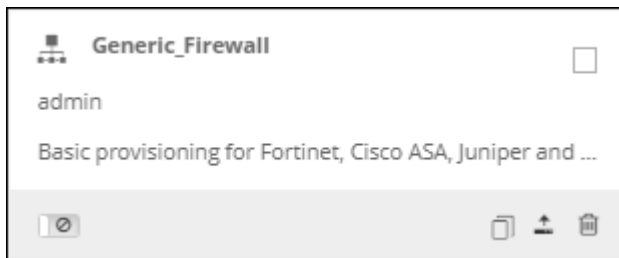
- **Failed** – Device configuration fetch failed due to unsupported version.

## Enable the Workflow

To enable the Generic Firewall 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 Generic Firewall 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 Generic Firewall workflow from the Card view by clicking the  (**Disable**) button.









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

## Generic Firewall Workflow

To submit the Generic Firewall 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. This screen displays all enabled workflows assigned to a specific user role.
3. Click the  (**Run workflow**) button for Generic Firewall.  
The *FormBuilder* screen opens.



4. Select the vendor name from the list of supported vendors.
5. In the **Device** field, click the  (**Retrieve field values**) button to fetch the list of devices from the database, based on the vendor you selected. Select the device in which the policy has to be created.
6. In the **Device IP** field, click the  (**Retrieve field values**) button to fetch the IP address of a device. Select the IP address of the device from the dropdown list.
7. *(Only for Cisco)* In the **Access List Name** field, enter the name of the rule that is available in Cisco
8. *(Only for Cisco)* In the **Interface** field, click the  (**Retrieve field values**) button to fetch the list of interfaces. Select the interface to which you want the policy to be applied.
9. *(Only for Cisco)* In the **Zone name** field, click the  (**Retrieve field values**) button to fetch the list of available zones. Select the zone in which you want the rule to be created.
10. *(Only for Cisco)* In the **Direction** field, click the  (**Retrieve field values**) button to fetch the list of available directions. Select the direction of the firewall policy.
11. *(Only for Juniper)* In the **Zone-Type** field, click the  (**Retrieve field values**) button to fetch the list of zones types available for the vendor you selected. Select the zone-type from the dropdown list.
12. *(Only for Juniper)* Select the **Zonal\_address book** or **Global\_address book** radio button based on how you want to acknowledge the address book.
13. *(Only for Palo Alto and Juniper)* Select the **From** and **To Zone** from their corresponding fields for the source and destination zone of the policy.
14. *(Only for Palo Alto, Juniper, and Fortinet)* Enter the name of the policy that you want to create in the device.
15. *(Only for Juniper)* Click the **Check if the policy name exists** button to ensure if the policy you want to create is not available in the selected device.
16. Enter the name of the group to which the source object is associated

17. Enter the name of source object from which you want allow or block the packets.
18. Select one of the following source object types from the dropdown list
19. Select the **IPv4** or **IPv6** radio button based on the type of IP you want to use for the source object.
20. Enter the IP address of the source object managed within the device.
21. *(Only for Fortinet)* Enter the comments relating to the source object from which you want to allow or block the packets.
22. *(Only for Fortinet)* Select the visibility to control features that you want to be visible in the GUI.
23. *(Only for Fortinet)* In the **Color** field, enter the color to control the GUI options.
24. Click the **(Add)** button.


If all the details are provided correctly, the source group member will appear in the table at the bottom.

**Note:** You can add more than one source group member.

25. Enter the name of the group to which the destination object is associated.
26. Enter the name of destination object to which you want to allow or block the packets.
27. Select one of the following destination object types from the dropdown list
28. Select the **IPv4** or **IPv6** radio button based on the type of IP you want to use for the destination object.
29. Enter the IP address of the destination object managed within the device.
30. *(Only for Fortinet)* Enter the comments relating to the destination object from which you want to allow or block the packets.
31. *(Only for Fortinet)* Select the visibility to control features that you want to be visible in the GUI.
32. *(Only for Fortinet)* In the **Color** field, enter the color to control the GUI options.
33. Click the **(Add)** button.

If all the details are provided correctly, the destination group member will appear in the table at the bottom.






**Note:** You can add more than one destination group member.

34. Enter the name of service object that you want to allow or block the packets from source to destination device.
35. *(Only for Fortinet)* In the **Service Category** field, click the  **(Retrieve field values)** button to fetch the list of available services categories. Select the service from the dropdown list.
36. *(Only for Fortinet)* Enter the **IP address** or the **FQDN** of the service object.
37. *(Only applicable for PaloAlto, Fortinet)* Select the **tcp** or **udp** radio button based on the type of protocol you want to use for the source object.
38. *(Only applicable for Cisco, Juniper, and Check Point)* Select the **protocol name** and **number** from the respective fields.
39. *(Only for Palo Alto, Fortinet, and Check Point)* Enter the port number for the source and destination object in their respective fields.

40. *(Only for Palo Alto, Cisco, Juniper, and Check Point)* Enter the name of the group to which the service object is associated.
41. Click the **(Add)** button.

If all the details are provided correctly, the service group member will appear in the table at the bottom.

**Note:** You can add more than one service group member.
42. *(Only for Cisco, Juniper, and Fortinet)* Enter the name of the group to which the source user is associated.
43. *(Only for Cisco, Juniper, and Fortinet)* Enter the user name corresponding to the group you selected.
44. Click the **(Add)** button.

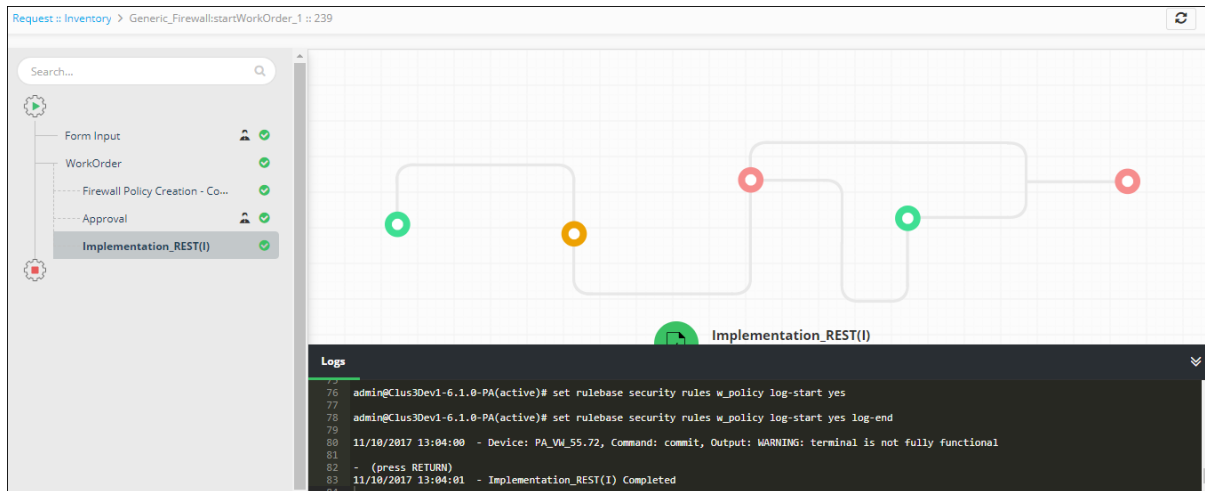
If all the details are provided correctly, the source user group member will appear in the table at the bottom.
45. From the **Action** dropdown list, select whether you want the policy to **permit** or **deny** the packets from source to destination device.
46. From the respective dropdown fields, select the type of service member, source member, user member, destination member you want to use.
47. *(Only for Palo Alto, Cisco, and Juniper)* In the **Service Object Members List** field, click the  **(Retrieve field values)** button to fetch the list of members you added. Select the service object that you want to allow or block the packets from source to destination device.
48. *(Only for Palo Alto, and Juniper)* In the **Source Object List** field, click the  **(Retrieve field values)** button to fetch the list of members you added. Select the source object from which you want allow or block the packets.
49. *(Only for Cisco, and Juniper)* In the **Network/User Object List** field, click the  **(Retrieve field values)** button to fetch the list of members you added. Select the user object to which you want allow or block the packets.
50. *(Only for Palo Alto, Cisco, and Juniper)* In the **Destination Member List** field, click the **(Retrieve field values)** button to fetch the list of members you added. Select the source object to which you want to allow or block the packets.
51. *(Only for Fortinet)* In the **Source Interface** field, click the  **(Retrieve field values)** button to fetch the list of interfaces you added. Select the source interface from which you want to allow or block the packets.
52. *(Only for Fortinet)* In the **Destination Interface** field, click the  **(Retrieve field values)** button to fetch the list of interfaces you added. Select the destination interface to which you want to allow or block the packets.
53. *(Only for Palo Alto and Cisco)* Select the **start** or **end** or **both** radio button depending on whether or not you want to store the firewall policy logs.
54. *(Only for Juniper and Fortinet)* Select the **Yes** or **No** radio button depending on whether or not you want to store the firewall policy logs.

55. (Only applicable for CheckPoint) Select the **enabled** or **disabled** radio button depending on how you want set the mode of policy.
56. Click **Submit** to the template.

## Work Order Flow

The tasks are included in the Generic L4 Firewall Policy Creation workflow.

**Note:** You can click each task to view its details. Where applicable, the logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.




**Firewall Policy Creation - Config Generation** — Configuration commands are generated to create and add a policy to the firewall device you selected.


**Approval** — Approval of a work order is based on the role assigned to the user, who has approval and implementation permissions. After you submit the request form, the configuration changes are reviewed and approved at AppViewX. The configuration changes are implemented on the device only after the approval is received.

**Implementation** — A new policy is created to permit or deny the packets or services from the source object to the destination object based on the inputs provided in the form fields.

## 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

1 to 2 of 2

My catalog **Request inventory** Scheduled workflows

Search...

Request ID	Workflow	Created by	Created time	Last updated	Status	Activity log
1239	Copy of TCP Wave Resource Rec...	admin	01/02/2018 06:18 PM	01/02/2018 06:18 PM	Completed	<a href="#">View</a>
239	Generic_Firewall	admin	10/11/2017 01:00 PM	10/11/2017 01:00 PM	Completed	<a href="#">View</a>

- Click the **Request ID** created for **Generic L4 Firewall Policy 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
- You can also view the following details of the request that are created: request creator, request time, last updated time, status, and activity log.
- Click the **View** link in the **Activity log** column to display the request in a stage view. In the **Summary** tab, click the  (**Expand**) icon to view the details of each task. Click the **Details** tab to view log messages and other particulars of a request.

Request > Inventory > Generic\_Firewall : 239 : log



Summary **Detail**

Request ID - 239 **Completed**

- Form Input**
  - 10/11/2017 13:0:59  
Form has been reviewed by user:admin
  - 10/11/2017 13:0:59  
Form Input Completed
- WorkOrder**
  - 10/11/2017 13:1:6  
Child WorkOrder ID: 1, has been created for the Child workflow: WorkOrder
  - 10/11/2017 13:4:10  
WorkOrder Completed

## Schedule a Workflow



To schedule a workflow, complete the following steps:

- Click the  (**Menu**) button.
- Navigate to **Workflow > Request**.  
The *Request* screen opens with **My catalog** tab displayed by default.
- Click the  (**Schedule workflow**) button on the Generic L4 Firewall Policy creation workflow.
- On the Generic Firewall window that opens, select the frequency of the policy creation process: once, hourly, daily, weekly, monthly, or yearly. The remaining fields in the Scheduler region update depending on what you select.
- Click **Save**.

## View Scheduled Workflows


To go to the scheduled workflow screen, complete the following steps:


- Click the  (**Menu**) button.
- 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.

## 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 **Firewall** 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  (**Credential**) or  (**Delete**) button in the Command bar.

## Troubleshooting

### I cannot find the Generic Firewall 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 Workflow](#) section of this guide.