AlgoSec FireFlow

Software Version: A30.10

Configuration Guide

View our most recent updates in our online ASMS Tech Docs.

Document Release Date: 26 November, 2020 | **Software Release Date**: April 2020

Legal Notices

AlgoSec, FireFlow, AppViz and AppChange are registered trademarks of AlgoSec Systems Ltd. and/or its affiliates in the U.S. and certain other countries.

Check Point, the Check Point logo, ClusterXL, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, INSPECT, INSPECT XL, OPSEC, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, UserAuthority, VPN-1, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, VPN-1 XL, are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates.

Cisco, the Cisco Logo, Cisco IOS, IOS, PIX, and ACI are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

Specifications subject to change without notice.

Proprietary & Confidential Information

This document contains proprietary information. Neither this document nor said proprietary information shall be published, reproduced, copied, disclosed, or used for any purpose other than the review and consideration of this material without written approval from AlgoSec, 65 Challenger Rd., Suite 310, Ridgefield Park, NJ 07660 USA.

The software contains proprietary information of AlgoSec; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between AlgoSec and the client and remains the exclusive property of AlgoSec If you find any problems in the documentation, please report them to us in writing. AlgoSec does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of AlgoSec Systems Ltd.

Contents

FireFlow administration

This section describes how FireFlow users can customize their own settings, and FireFlow administrators can configure workflows, templates, and other settings for all users.

This section also describes periodic maintenance performed by FireFlow administrators.

Note: To configure FireFlow and perform maintenance procedures, you must log in for configuration purposes. Additionally, some configuration procedures require a FireFlow restart when complete.

For more details, see Log in for configuration purposes and Restart FireFlow.

For more details, see:

User configurations	The following procedures are available for each user: • Configure user preferences
Administrator configuration	The following procedures are used by FireFlow to configure workflows, templates, and more: • Customize the FireFlow Home page • Configure global settings • Manage FireFlow users and roles • Manage workflow options • Manage request templates • Manage FireFlow emails and notifications • FireFlow hooks
Periodic maintenance	The following procedures are used from time to time to maintain FireFlow: • FireFlow troubleshooting

Logins and other basics

This topic describes the very basics of working with ASMS, such as logging in and out and supported browsers.

Supported browsers

View ASMS in one the following web browsers, at screen resolution of **1920x1080** or above.

- **Mozilla Firefox**
- **Google Chrome**
- **Microsoft Edge**
- **Internet Explorer 11** and higher. Internet Explorer 8.0 is supported for FireFlow requestors only.

Log in to ASMS

Log in to ASMS from any desktop computer using the credentials provided by an AFA administrator.

Do the following:

1. In your browser, navigate to **https://<algosec_server>** where **<algosec_server>** is the ASMS server IP address or DNS name.

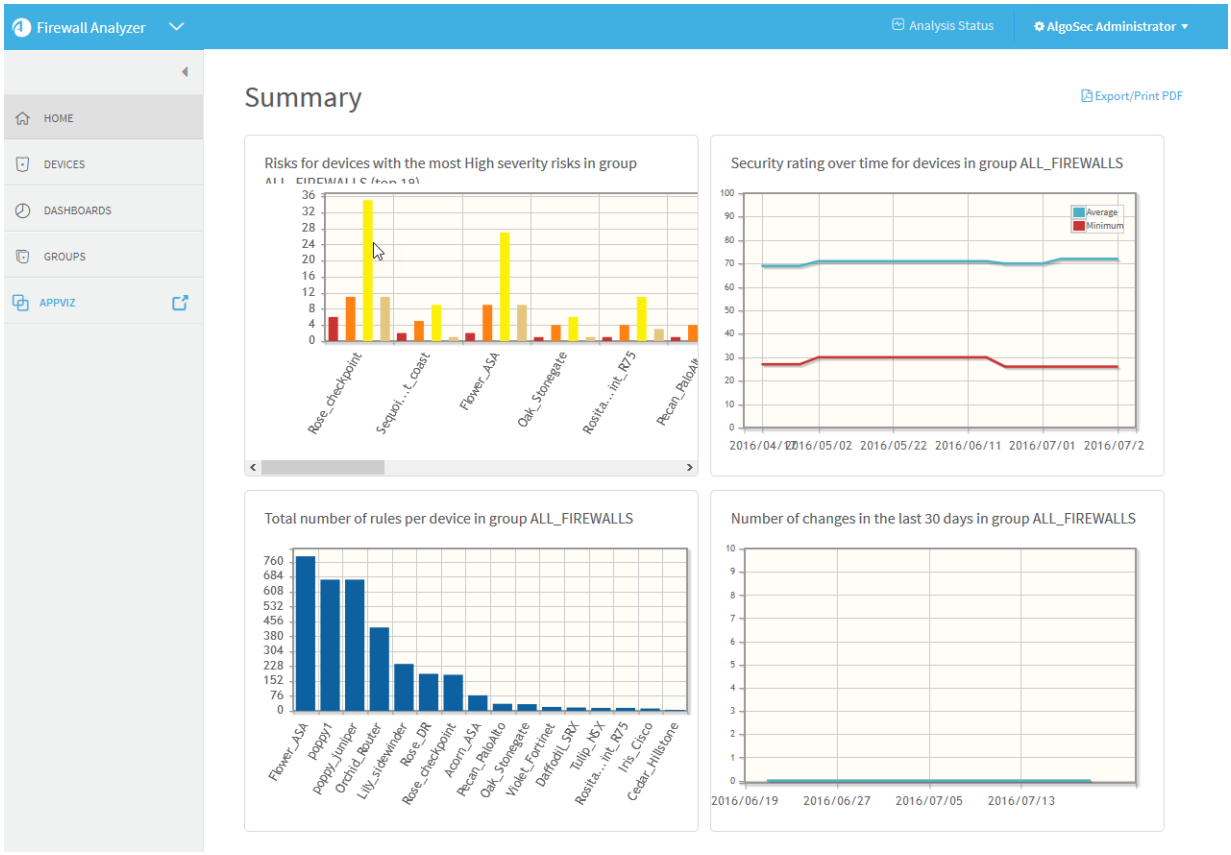
   If a warning message about the web server's certificate appears, click **Accept** or **OK**. For more details, contact your network administrator.

   The **Security Management Suite** login page appears.

2. In the **Username** and **Password** fields, enter your username and password, and click **Login**.

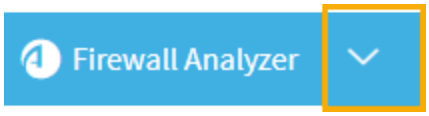
You are logged in, and ASMS displays AFA by default.

For example:

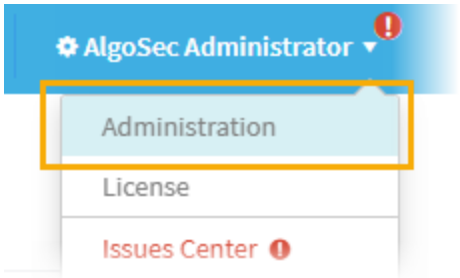


Switch ASMS products

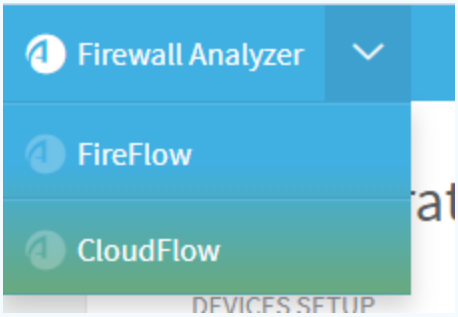
If you are a user in multiple ASMS products, such as AFA, FireFlow, and AppViz, switch between products using the dropdown at the top-left, above the main menu.



If you are an administrator for any of these products, the relevant administration menu is available from your user dropdown at the top-right:



Note: CloudFlow is now accessible from inside ASMS. Click the dropdown at the top-left and select **CloudFlow**.



For more details, see our CloudFlow Help Center.

Adjust your screen space

To adjust the screen space available for your main workspace, hide, display, or change the size of the main menu on the left.

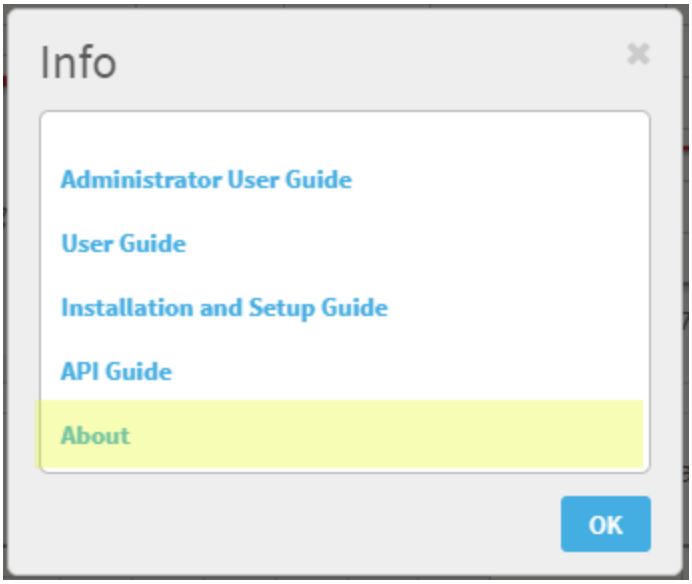
- **To adjust the size of the main menu**, hover between the menu and the workspace and drag the border left or right.
- **To collapse the menu entirely**, click at the top. When collapsed, click to expand it again.

View ASMS product details

This procedure describes how you can identify your AFA, FireFlow, or AppViz installation version and build number.

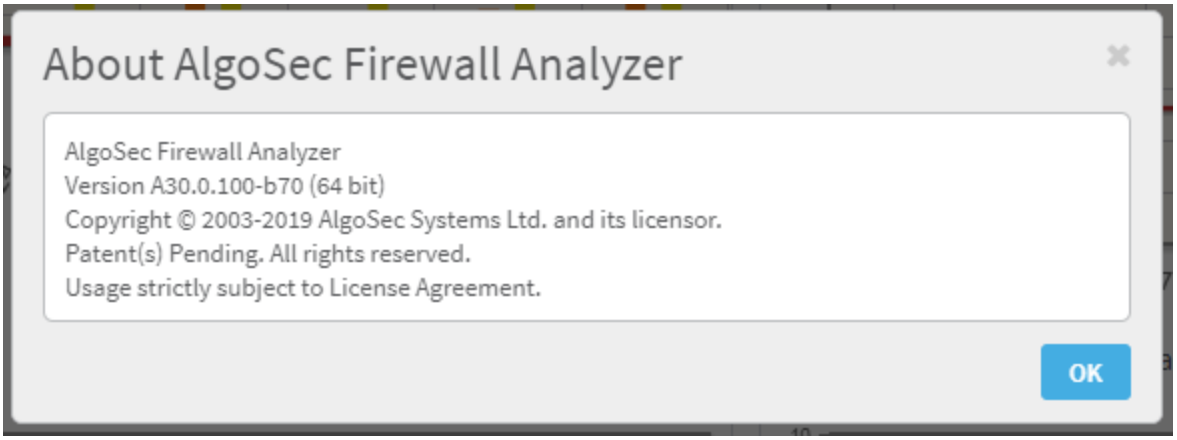
Do the following:

1. In the toolbar, click your username and then select **About** or **Info**.
2. For example, if you're in AFA, in the **Info** dialog, click **About**.



The **About** dialog appears, showing details about the product you have installed.

For example:



Note: If you are running the FIPS 140-2 compliant version of AFA, this information is indicated in the window.

Log out of ASMS

Log out of ASMS by clicking your username at the top right, and selecting **Logout**.

You are logged out of all ASMS products available to you.

Note: If Single Sign On is configured, you must browse to the **Logout** page hosted on your IdP to log out.

For more details, see the *AlgoSec Firewall Analyzer Administrator Guide*.

Configure user preferences

This topic describes how to configure your own FireFlow user preferences.

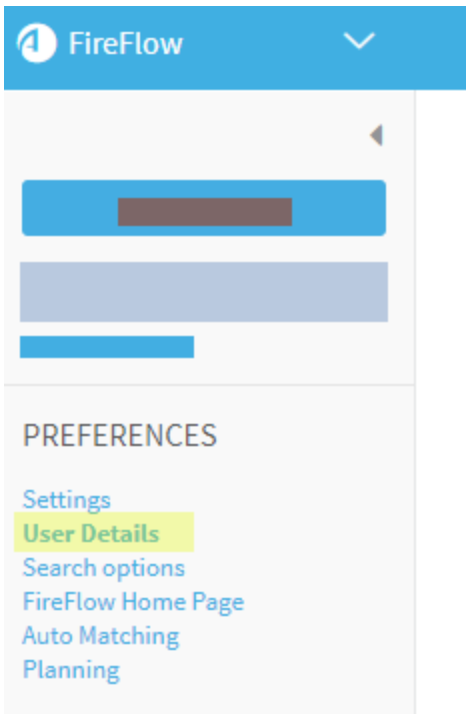
Access the Preferences page

To access your user preferences page, do the following:

1. In the main menu on the left, click **PREFERENCES**.

   If you are a **requestor**, FireFlow will take you directly to the **Preferences** fields.

   If you are a **privileged user**, you may need to click **User Details** on the left. For example:



> **Note:** If the system is configured to import user information from an LDAP server upon each login, FireFlow reminds you that changes to these settings may be overridden then next time you log in.
>
> In such cases, you must make these changes in the LDAP server instead of FireFlow.

2. Modify the fields as needed. For details, see User preferences fields.
3. Click **Save Preferences**.

User preferences fields

Enter details in the following fields as needed.

Identity fields

Email	Your email address. This field is read-only.
Full Name	Your full name. This field is read-only.
Nickname	Type your nickname.
Language	Select the desired FireFlow interface language. All fields will be displayed in the selected language.
Timezone	Select the time zone in which you are located. To use the default time zone defined in FireFlow, select **System Default**.

Location fields

Organization	Type the name of your organization.
Address 1	Type your primary mailing address.
Address 2	Type your secondary mailing address.
City	Type your city.
State	Type your state.
Zip	Type your zip code.
Country	Type your country.

Phone number fields

Home	Type your home telephone number.
Work	Type your work telephone number.
Mobile	Type your mobile telephone number.
Pager	Type your pager number.

Additional information

This area displays any custom fields defined for your system.

Signature

Enter a string that you'd like appended to all your comments and replies in FireFlow.

Log in for configuration purposes

You can perform configurations via the FireFlow user interface, when logged in as a *FireFlow configuration administrator*. A FireFlow configuration administrator is a privileged user with **FireFlow Administrator - Allow FireFlow Configuration** permissions.

Note: After completing initial configuration, it is recommended to revoke **FireFlow Administrator - Allow FireFlow Configuration** permissions for all users, in order to avoid accidental changes to the configuration.

Do the following:

1. In your browser's **Address** field, type `https://<algosec_server>/algosec/` where `<algosec_server>` is the AlgoSec server URL.

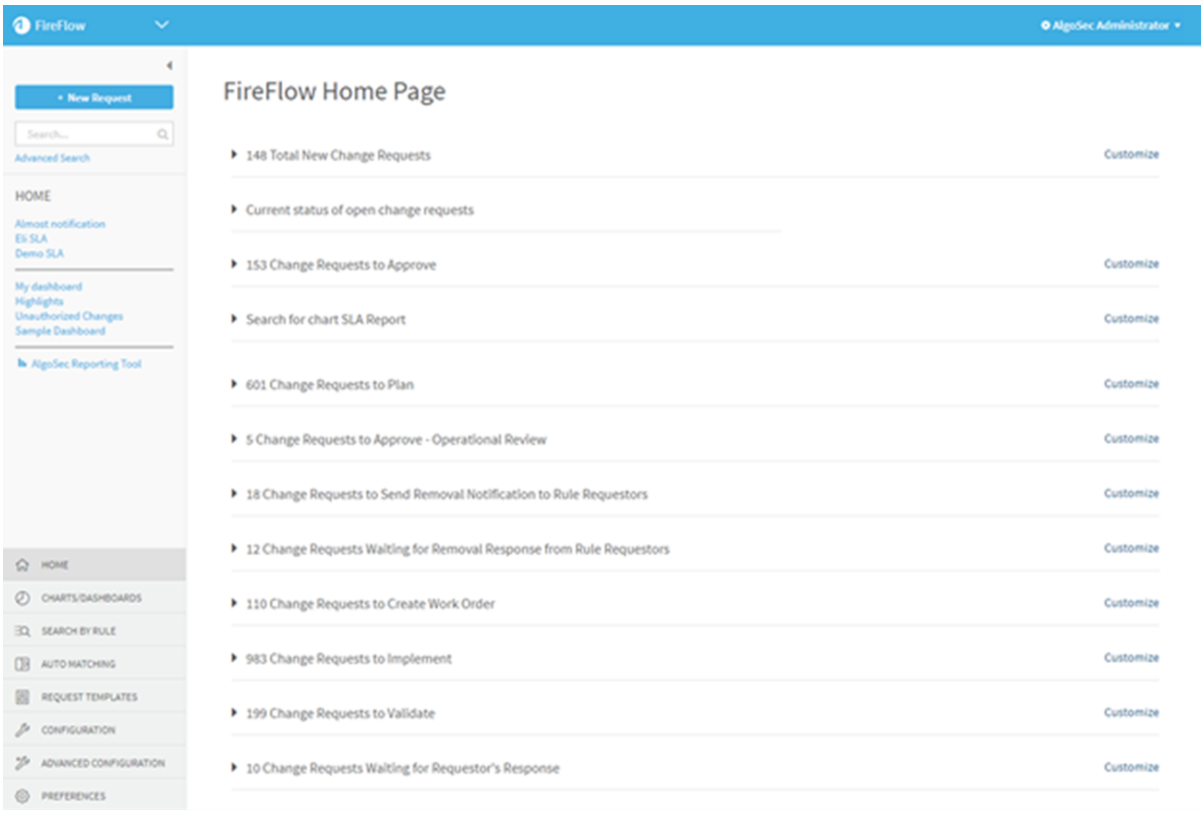
   The **Security Management Suite** Login page appears.

2. In the **Username** and **Password** fields, type your username and password.
3. Click **Login**.

   One of the *AlgoSec Security Management Suite* products will appear.
4. If FireFlow does not appear, switch to FireFlow.

The **FireFlow Home Page** appears.



Configuration settings can be accessed by clicking the **Configuration** and **Advanced Configuration** main menu items.

Configure global settings

Relevant for: Network operations, information security, and administrative users

This section describes how to configure global settings across all FireFlow workflows and templates.

For details, see:

- FireFlow display settings
- Search result settings
- Customize the FireFlow Home page
- Customize the Auto Matching Page
- Customize initial planning
- Override FireFlow system defaults

FireFlow display settings

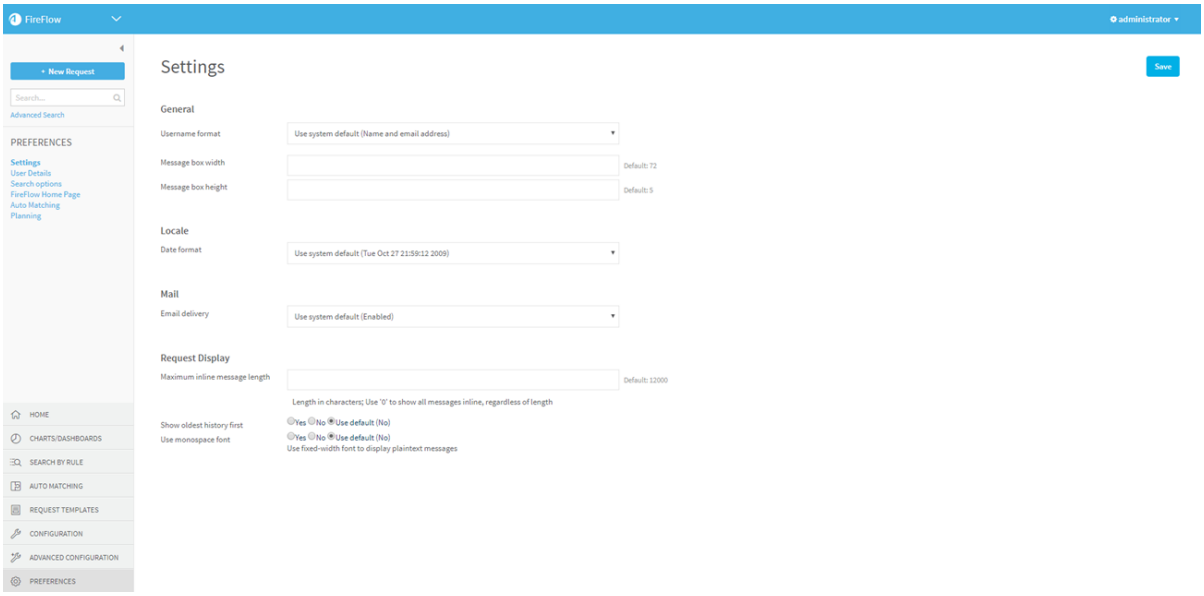
You can customize the following general settings:

- How user names are displayed
- The dimensions of message boxes
- How dates are displayed
- The number of results to display in each Home page list
- How change request histories are displayed

Do the following:

1. In the main menu, click **Preferences**.

   The **Settings** page is displayed.



2. Configure the fields using the information in the following table.
3. Click **Save**.

Settings Fields

In this field...	Do this...
Change Request display	
Maximum inline message length	Type the maximum length (in characters) of messages that should be displayed in change request history items. Messages longer than the specified length will not be displayed, and you must download the message to view it. To display all messages in the change request histories, regardless of their length, type 0. The default value is 12,000.
General	

In this field...	Do this...
Username format	Select the format in which to display user names in FireFlow: • Use system default (Name and email address): Use the system default username format, which is to display both the username and email address. • Short usernames: Display the username only. • Name and email address: Display both the username and email address.
Message box width	Type the width (in characters) of message boxes, in which you type comments and replies. The default value is 72 characters.
Message box height	Type the height (in characters) of message boxes, in which you type comments and replies. The default value is 5 characters.
Locale	
Date format	Select the format in which to display the date in FireFlow.
Mail	
Email delivery	Specify whether to enable delivery of FireFlow notifications via email, by selecting one of the following: • Use system default (Enabled): Use the system default, which is to enable delivery of send notifications via email. • Enabled: Enable delivery of notifications via email. • Suspended: Suspend delivery of notifications via email. Users will not receive notifications from FireFlow.
Request display	

In this field...	Do this...
Show oldest history first	Specify whether to show the oldest change request history item first in the change request history, by choosing one of the following: Yes: Show the oldest change request history item first. No: Show the oldest change request history last. Use default (No): Use the system default, which is to show the oldest change request history last.
Use monospace font	Specify whether to display messages appearing in change request history items in monospace font, by choosing one of the following: Yes: Use monospace to display messages. No: Use a fixed-width plaintext font to display messages. Use default (No): Use the system default, which is to use a fixed-width plaintext font to display messages.

Search result settings

You can specify which columns FireFlow displays in search results by default.

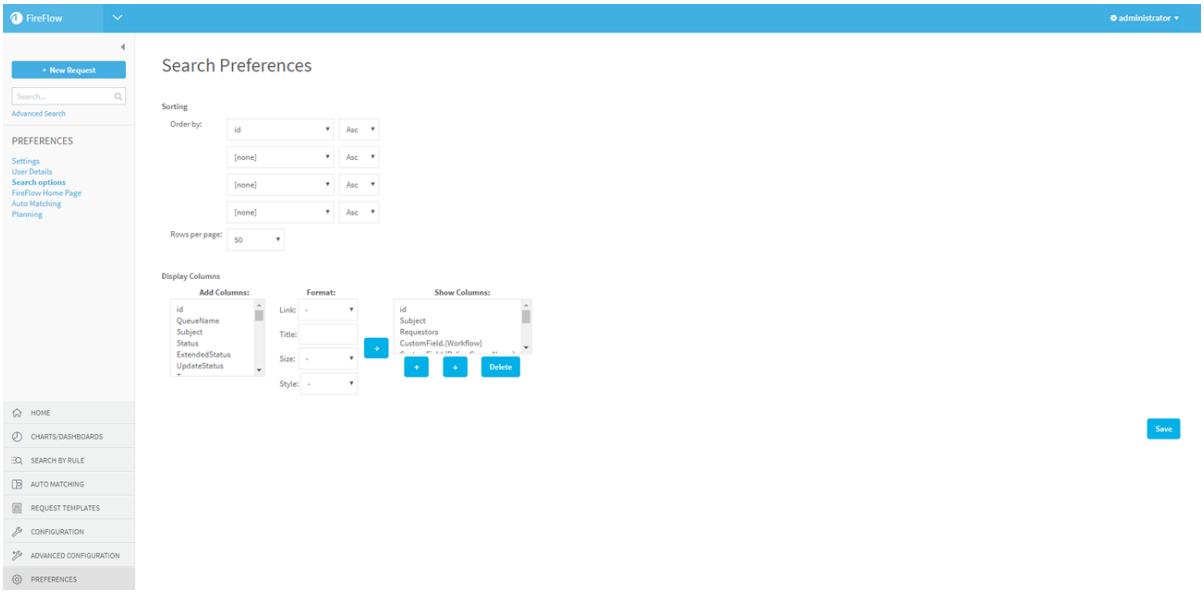
Do the following:

1. In the main menu, click **Preferences**.

   The **Settings** page is displayed.

2. In the main menu, click **Search options**.

   The **Search Preferences** page is displayed.



In the **Sorting** area, do the following:

Order by	In the **Order by** area, specify the default sort order of the search results as follows: a. In the left-side fields, select one or more columns according to which the search results should be sorted. b. In the right-side fields, select the sort order to use for each specified column: ascending (**Asc**) or descending (**Desc**).
Rows per page	In the **Rows per page** field, select the number of search result rows that should appear in each page.
Display Columns	In the **Display Columns** area, do the following for each column you want to appear in the search results:

Add Columns	Do the following: a. In the **Add Columns** box, select a column you want to appear. b. Complete the fields in the **Format** area using the information in Column Format Fields. (see Column Format Fields) c. Click  . The column appears in the **Show Columns** box. The order that the columns appear in the box (top to bottom) represents the order in which they will appear in the search results (left to right). To move the column up or down in the box, select the column and click the  or  buttons. To delete the column, select it and click **Delete**.

3. Click **Save**.

Column Format Fields

In this field...	Do this...
Link	Specify whether items in the column should be linked, by selecting one of the following: • **-**. Items in the column are not linked. • **Take:** Clicking on an item in the column assigns you the relevant change request. • **Display:** Clicking on an item in the column displays the relevant change request.
Title	Type the name of the column.
Size	Specify the text size of items in the column, by selecting one of the following: • **-**. Items in the column appear in medium-sized text. • **Small:** Items in the column appear in small-sized text. • **Large:** Items in the column appear in large-sized text.

In this field...	Do this...
Style	Specify the font style of items in the column, by selecting one of the following: • **-**. Items in the column appear in normal font. • **Bold:** Items in the column appear in bold font. • **Italic:** Items in the column appear in italicized font.

Customize the FireFlow Home page

Relevant for: FireFlow administrators

This topic describes how FireFlow administrators can customize the FireFlow home page for all users or per role, adding search results and charts as needed.

Customize Homepage Views: Watch to learn how to customize the homepage view for each user role.

Customize the Home page globally

By default, the **Home** page is globally configured to include the **Change Request I own** pre-defined search results and a **Refresh** field. If desired, you can add or remove elements.

Global customization affects the **Home** page of all users. It enables adding or removing any screen element.

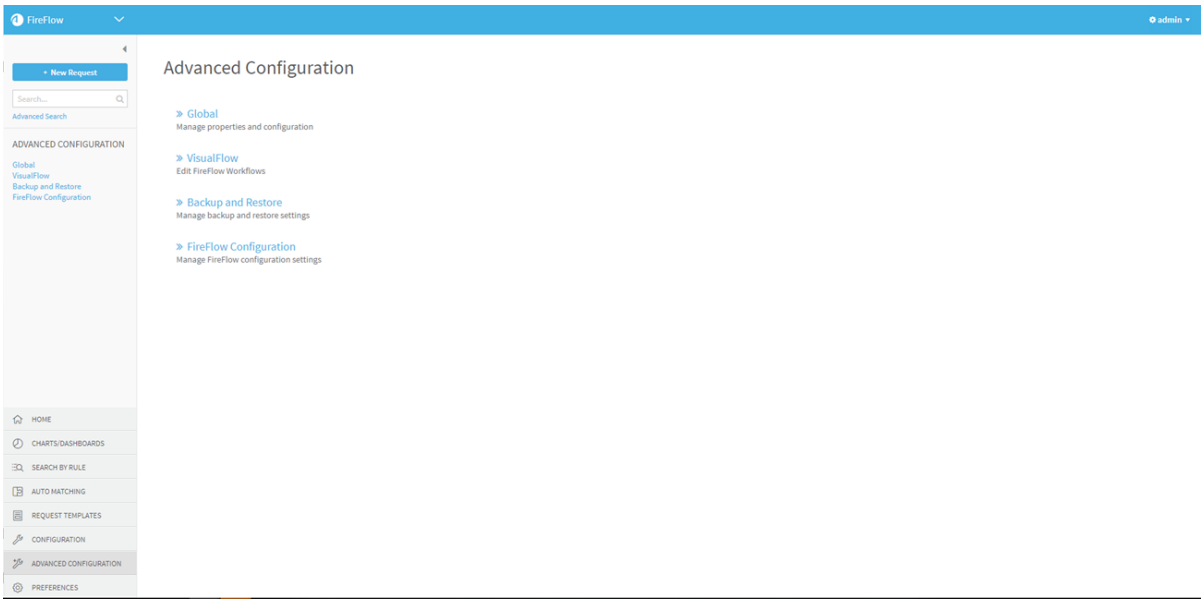
Note: Elements that are added to the **Home** page via global customization cannot be removed via per-role or per-user customization.

Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.

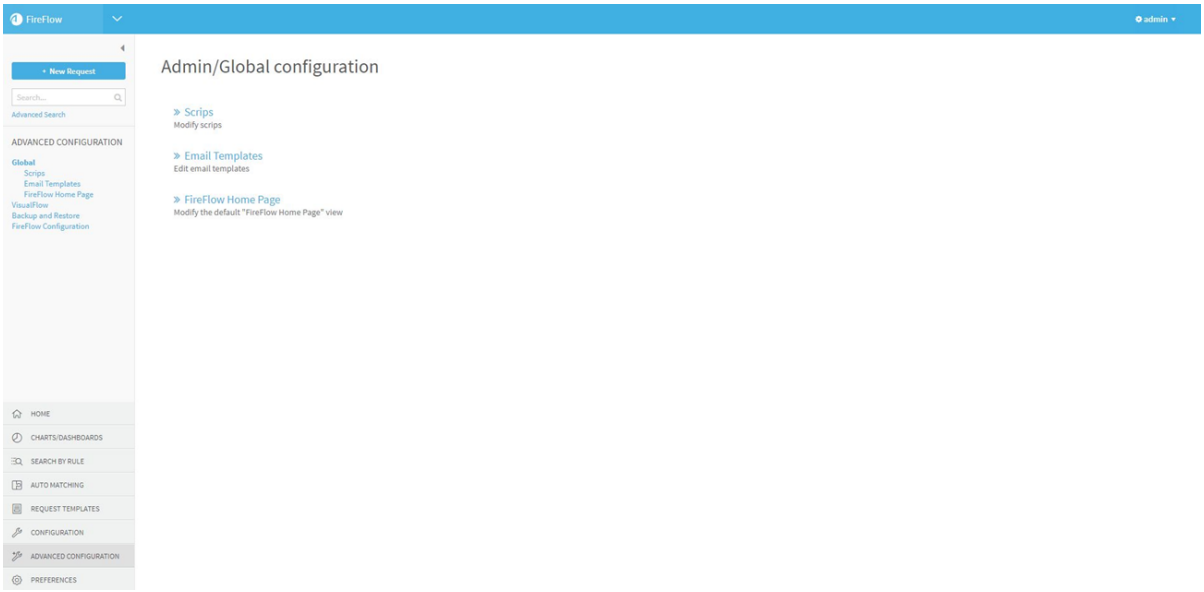
2. In the main menu, click **Advanced Configuration**.

   The **Advanced Configuration** page appears.



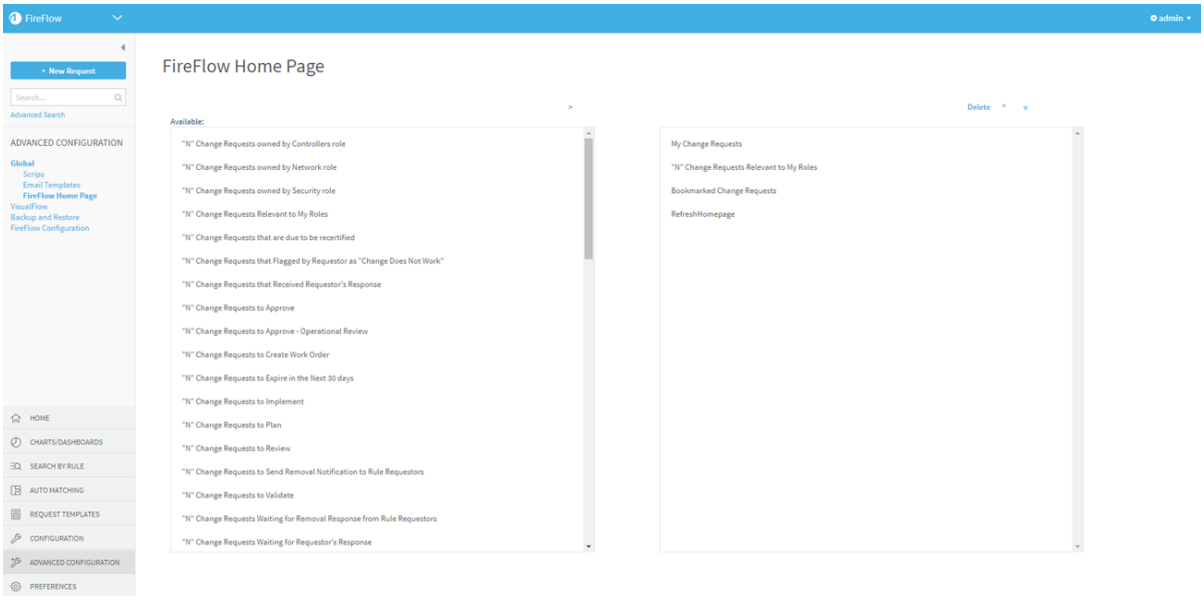
3. Click **Global**.

   The **Admin/Global configuration** page appears.



4. Click **FireFlow Home Page**.

   The **FireFlow Home Page** configuration page appears.



5. For each element you want to add to the **Home** page, do the following:

    a. In the **Available** list box, select the element you want to add. For details, see Home page elements.

    b. Click + Add to Dashboard .

    The selected element moves to the right list box. The order that the elements appear in the box represents the order in which they will appear in the **Home** page.

    c. To move the element up or down in the box, select the element and click the ↓ Move down or ↑ Move up buttons.

    d. To delete the element, select it and click **Delete**.

Your changes are saved.

Home page elements

Add or remove any of the following elements from the FireFlow home page.

Select this element...	To add this to the Home page...
"N" Soon to be due change requests	Pre-defined search results consisting of a list of open change requests in the system that have a due date that has passed, that is the current date, or that is the day after the current date.
"N" Change Requests owned by Controllers group	Pre-defined search results consisting of a list of change requests in the system that are owned by the Controllers role.
"N" Change Requests owned by Network group	Pre-defined search results consisting of a list of change requests in the system that are owned by the Network role.
"N" Change Requests owned by Security group	Pre-defined search results consisting of a list of change requests in the system that are owned by the Security role.
"N" Change Requests Relevant to My Groups	Pre-defined search results consisting of a list of change requests in the system that are relevant to the user roles to which you belong.
"N" Change Requests that are due to be recertified	Pre-defined search results consisting of a list of traffic change requests in the system that expired, and which should be recertified.
"N" Change Requests Flagged by Requestor as "Change Does Not Work"	Pre-defined search results consisting of a list of change requests in the system that have been flagged by the requestor as "Change Does Not Work".
"N" Change Requests that Received Requestor's Response	Pre-defined search results consisting of a list of change requests in the system that are currently in the Validate stage and received the requestor's confirmation that the requested change was implemented successfully.
"N" Change Requests to Approve	Pre-defined search results consisting of a list of change requests in the system that are currently in the Approve stage.

Select this element...	To add this to the Home page...
"N" Change Requests to Create Work Order	Pre-defined search results consisting of a list of change requests in the system which are currently in the Implement stage and awaiting a work order to be created.
"N" Change Requests to Expire in the Next 30 days	Pre-defined search results consisting of a list of change requests in the system that will expire within the next 30 days.
"N" Change Requests to Implement	Pre-defined search results consisting of a list of change requests in the system that are currently in the Implement stage and awaiting implementation.
"N" Change Requests to Plan	Pre-defined search results consisting of all change requests in the system that are currently in the Plan stage.
"N" Change Requests to Review	Pre-defined search results consisting of a list of change requests in the system that are currently in the Review stage and awaiting a controller's review.
"N" Change Requests to Send Removal Notification to Rule Requestors	Pre-defined search results consisting of a list of change requests in the system that are currently in the Approve stage, and for which a rule removal notification will be sent to the rule's traffic requestors.
"N" Change Requests to Validate	Pre-defined search results consisting of a list of change requests in the system that are currently in the Validate stage.
"N" Change Requests Waiting for Removal Response from Rule Requestors	Pre-defined search results consisting of a list of change requests in the system that are currently in the Approve stage and awaiting confirmation from the rule’s traffic requestors that the requested rule removal is approved.
"N" Change Requests Waiting for Requestor's Response	Pre-defined search results consisting of a list of change requests in the system that are currently in the Validate stage and awaiting the requestor's confirmation that the requested change was implemented successfully.

Select this element...	To add this to the Home page...
"N" New Change Requests	Pre-defined search results consisting of a list of change requests in the system that are new and still in the Request stage, and whose traffic has already been checked against devices.
"N" New Recertification Requests	Pre-defined search results consisting of a list of recertification requests in the system that are new and still in the Request stage.
"N" Open Change Requests	Pre-defined search results consisting of a list of change requests in the system that are currently open.
"N" Parent Recertification Requests Pending Sub Requests Implementation	Pre-defined search results consisting of a list of parent recertification requests in the system that are currently in the Implement stage and awaiting implementation of the relevant sub-requests.
"N" Parent Requests Pending Sub Request Implementation	Pre-defined search results consisting of a list of parent requests in the system that are currently in the Implement stage and awaiting implementation of the relevant sub-requests.
"N" Recertification Requests to Create Work Order	Pre-defined search results consisting of a list of recertification requests in the system which are currently in the Implement stage and awaiting a work order to be created.
"N" Recertification Requests to Implement	Pre-defined search results consisting of a list of recertification requests in the system that are currently in the Implement stage and awaiting implementation.
"N" Recertification Requests to Plan	Pre-defined search results consisting of all recertification requests in the system that are currently in the Plan stage.
"N" Recertification Requests to Send Recertify Notification to Traffic Requestors	Pre-defined search results consisting of a list of recertification requests in the system that are currently in the Approve stage, and for which a recertification notification will be sent to the traffic requestors.

Select this element...	To add this to the Home page...
"N" Recertification Requests to Validate	Pre-defined search results consisting of a list of recertification requests in the system that are currently in the Validate stage.
"N" Recertification Requests Waiting for Recertify Response from Traffic Requestors	Pre-defined search results consisting of a list of recertification requests in the system that are currently in the Approve stage and awaiting confirmation from the traffic requestors that the requested recertification is approved.
"N" Rejected Change Requests	Pre-defined search results consisting of a list of change requests in the system that were rejected.
"N" Resolved Change Requests	Pre-defined search results consisting of a list of change requests in the system that have been resolved.
"N" Total New Change Requests	Pre-defined search results consisting of a list of all change requests in the system that are new and still in the Request stage, including change requests whose traffic has not yet been checked against devices.
Bookmarked Change Requests	A list of change requests that the user bookmarked.
My Change Requests	Pre-defined search results consisting of a list of change requests in the system that are owned by you.
RefreshHomepage	Controls for refreshing the page.
Unowned Change Requests	Pre-defined search results consisting of a list of change requests in the system that currently have no owner.
Saved Search Name	A custom search that was saved under "FireFlow's saved searches", and which is available to your user role.
Chart Name	A chart that was saved under "FireFlow's saved searches", and which is available to your user role.
Search for chart *Chart Name*	A custom search on which a certain chart is based.

Customize the Home page per role

By default, the **Home** page for a user role is configured to include certain pre-defined search results, as well as the globally configured elements. If desired, you can add or remove elements.

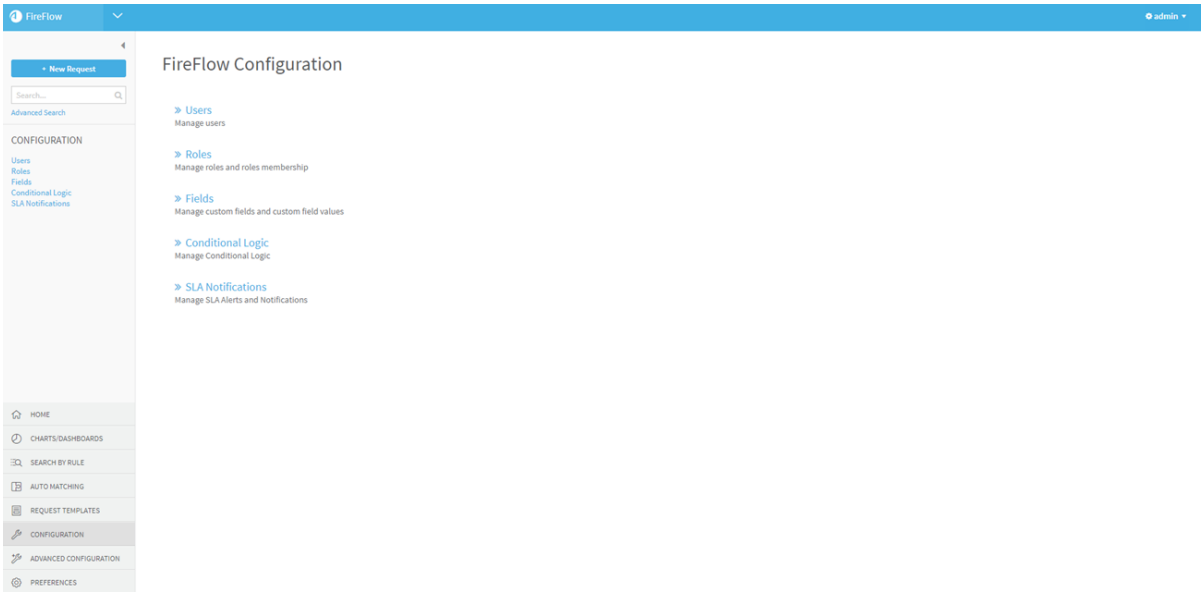
Per-role customization affects the **Home** page of all users belonging to a specific user role. It enables adding screen elements to the **Home** page, but not removing those that were added via global customization.

> **Note:** Elements that were added to the **Home** page via global customization cannot be removed via per-role customization. Likewise, elements that are added to the **Home** page via per-role customization cannot be removed via per-user customization.

Do the following:

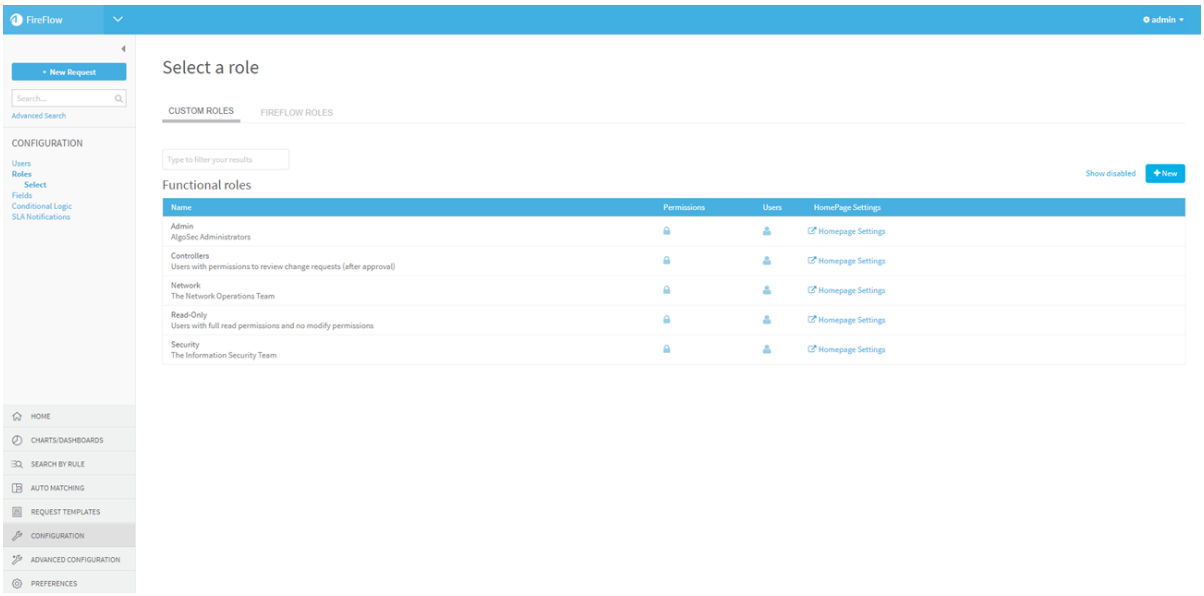
1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page appears.



3. Click **Roles**.

   The **Select a role** page appears.



4. (Optional) To display disabled roles, click the **Show disabled** link.

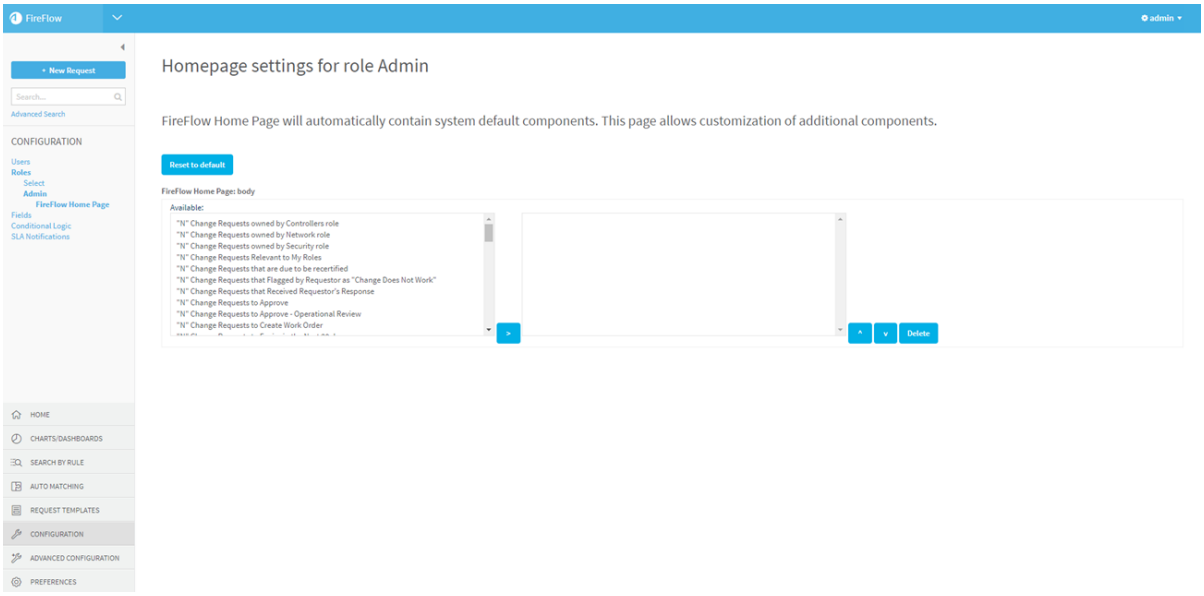
   To revert to a list which only displays enabled roles, click the **Hide disabled** link.

5. (Optional) To search for the desired role, type your search in the **Type to filter your results** field.

   The roles which match your search appear in the **Functional roles** area.

6. In the row of the relevant role, click **Homepage settings**.

   The **HomePage settings for role** page appears.



7. For each element you want to add to the **Home** page, do the following:

   a. In the **Available** list box, select the element you want to add. For details, see Home page elements.

   b. Click + Add to Dashboard .

      The selected element moves to the right list box. The order that the elements appear in the box represents the order in which they will appear in the **Home** page.

      Note: All custom elements will appear *above* the globally added pre-defined search results in the **Home** page.

   c. To move the element up or down in the box, select the element and click the ↓ Move down or ↑ Move up buttons.

   d. To delete the element, select it and click **Delete**.

   Your changes are saved.

8. To reset the page's fields to their default values, click **Reset to default**.

Customize pre-defined search results

The pre-defined search results represent specific saved searches.

For example, **"N" New Change Requests** represents an advanced search for all change requests with the status "New", and it displays search results in descending order sorted according to the **LastUpdated** column.

Do either of the following, as needed:

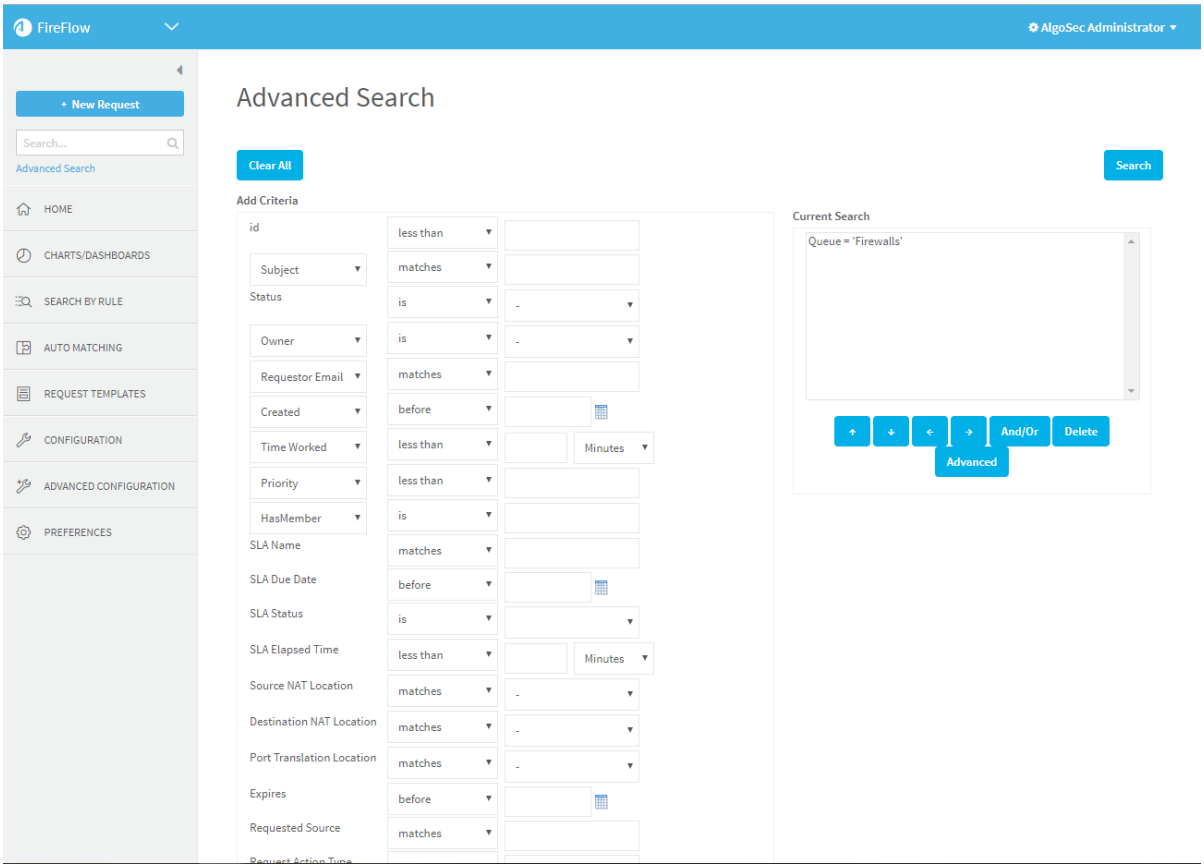
Customize the appearance of pre-defined search results

Customize the pre-defined search results' appearance, so as to include different columns, sort order, number of results rows, and so on.

Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Advanced Search** link.

   The **Advanced Search** page appears.



3. Scroll to the bottom of the page.
4. In the **Saved Searches** area, in the **Load saved search** drop-down menu, select the relevant pre-defined search.
5. Click **Load**.

   The search is loaded.
6. In the **Display Columns** area, modify the search results' appearance as desired.
7. Click **Save**.

The pre-defined search's definition is modified.

Adding the "Certify Change Requests" Button to Pre-Defined Search Results

Add the **Certify Change Requests** button to pre-defined search results that consist of resolved traffic change requests, in order to enable users to create recertification

requests.

Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Advanced Search**.

   The **Advanced Search** page appears.
3. Scroll to the bottom of the page.
4. In the **Saved Searches** area, in the **Load saved search** drop-down menu, select the relevant pre-defined search.
5. Click **Load**.

   The search is loaded.
6. In the **Current Search** area, click **Advanced**.

   The **Edit Query** page is displayed.
7. In the **Format** field, add:

   ```
   /ALLOW_RECERTIFICATION
   ```
8. Click **Apply**.

   The **Advanced Search** page reappears with your changes.
9. Click **Save**.

The pre-defined search's definition is modified.

Customize the Auto Matching Page

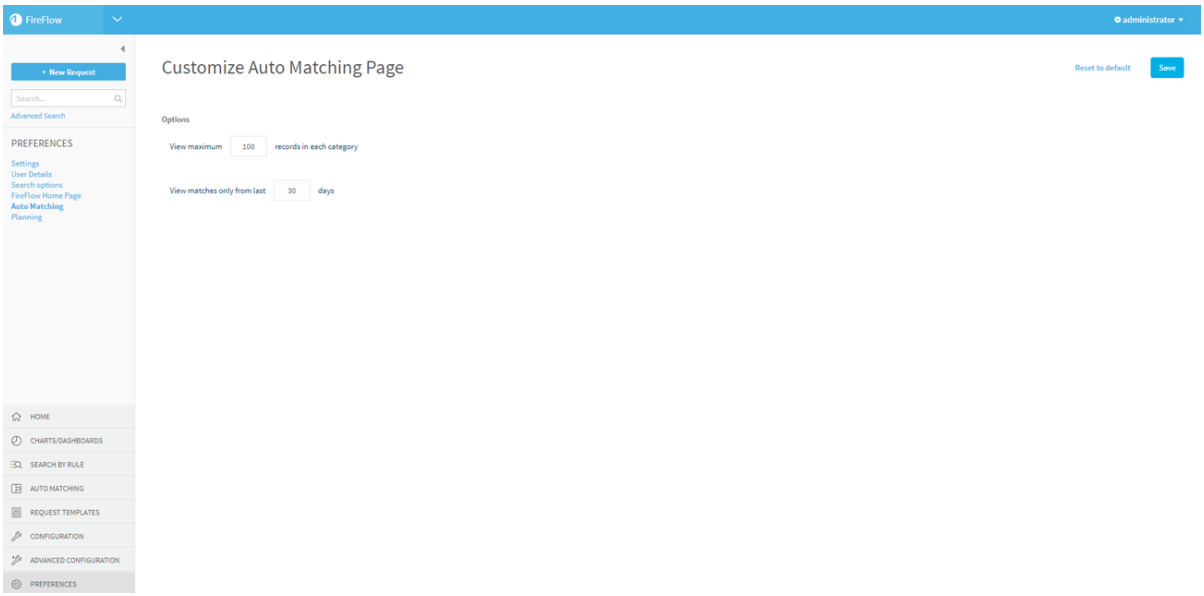
You can customize the following elements of the **Auto Matching** page:

- The number of changes displayed in relevant sub-lists.
- The number of days for which change requests are displayed in relevant sub-lists.

Do the following:

1. Do one of the following:
   - In the main menu, click **Preferences**, then click **Auto Matching**.
   - In the **Auto Matching** page, click **Customize** next to any list heading.

   The **Customize Auto Matching Page** is displayed.



2. In the **View maximum records in each category** field, type the maximum number of records to display in each of the **Auto Matching** page's sub-lists and in the **Auto Matching > Changes** page.
3. In the **View matches only from last** field, type the number of days for which the **Matched** list's **Perfect Auto Match**, **Last X Days** and **Manual Match, Last X Days** sub-lists should display change requests.
4. To reset the page's fields to their default values, click **Reset to default**.
5. Click **Save**.

Customize initial planning

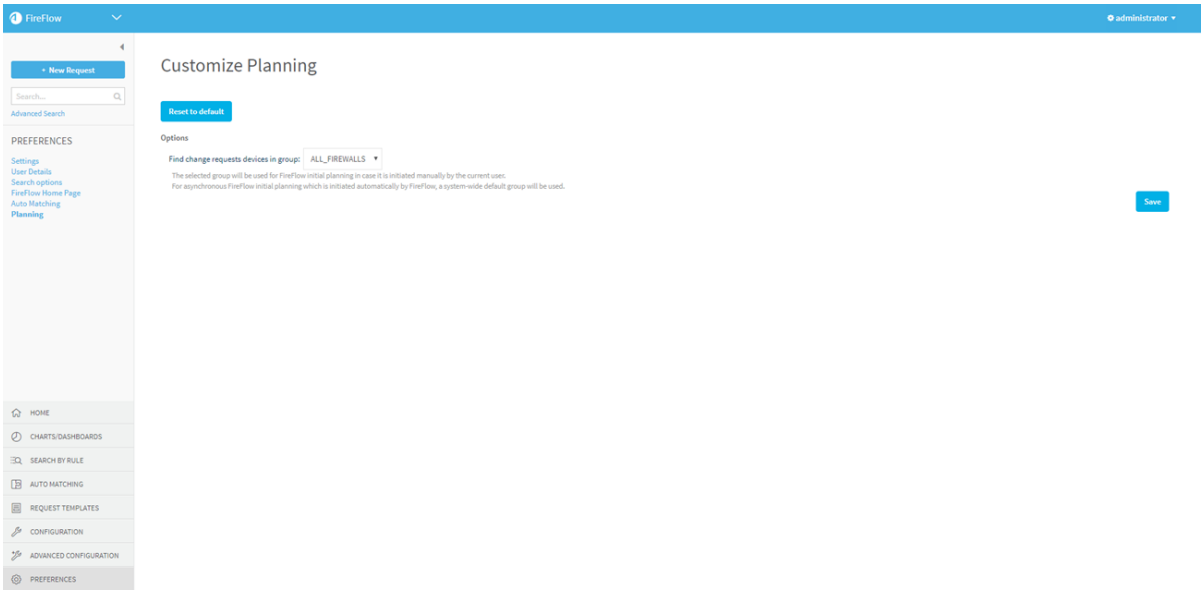
By default, when planning a change request in the **Initial Planning** page, FireFlow checks the traffic specified by the change request against all device groups in the

system. If desired, you can customize FireFlow to check traffic against a specific device group only. The **Find change requests devices in group** drop-down list will display the specified device group by default.

Do the following:

1. In the main menu, click **Preferences**, then click **Planning**.

   The **Customize Planning** page is displayed.



2. In the **Find change requests devices in group** drop-down list, select the device group against which FireFlow should check traffic by default.
3. To reset the page's fields to their default values, click **Reset to default**.
4. Click **Save.**

Override FireFlow system defaults

This section explains how to configure FireFlow parameters to override the FireFlow system defaults.

Note: You can find all configuration parameters and their descriptions in the FireFlow user interface. Additionally, the `FireFlow_Config.json` file located under

`/usr/share/fireflow/local/etc/` contains detailed information about each parameter.

For more details, see FireFlow configuration parameter reference or contact AlgoSec.

Configure FireFlow parameters (UI)

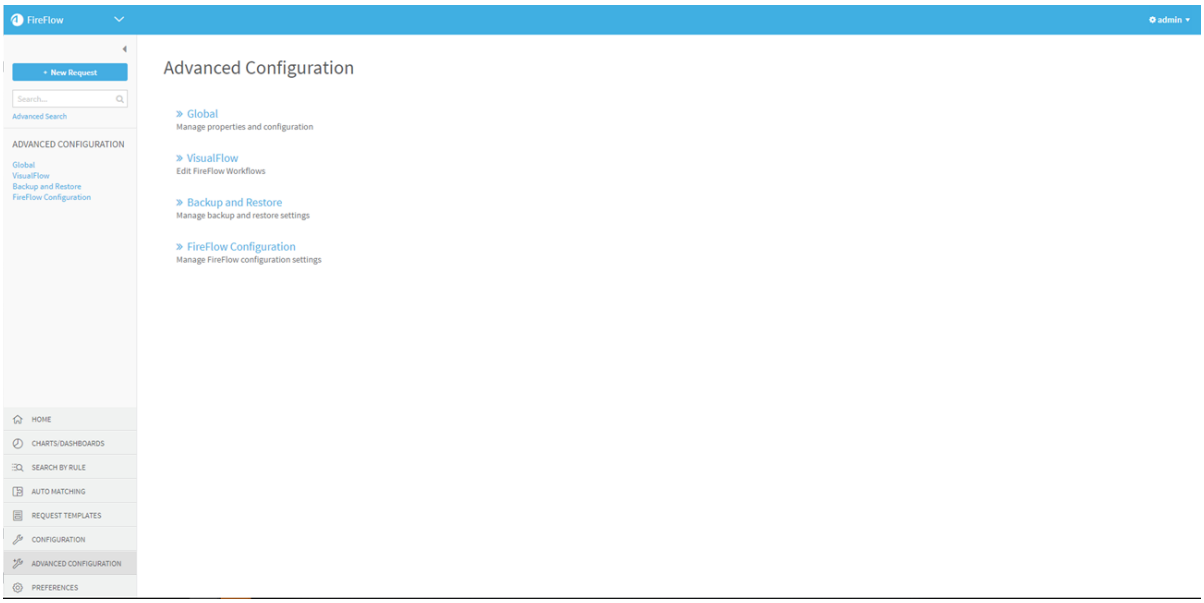
You can override default system settings, including timeout settings, log file settings, the default columns displayed in search results, and more.

Note: Optionally, you can customize system default settings using the CLI. For details, see Configure FireFlow parameters (CLI).

Do the following:

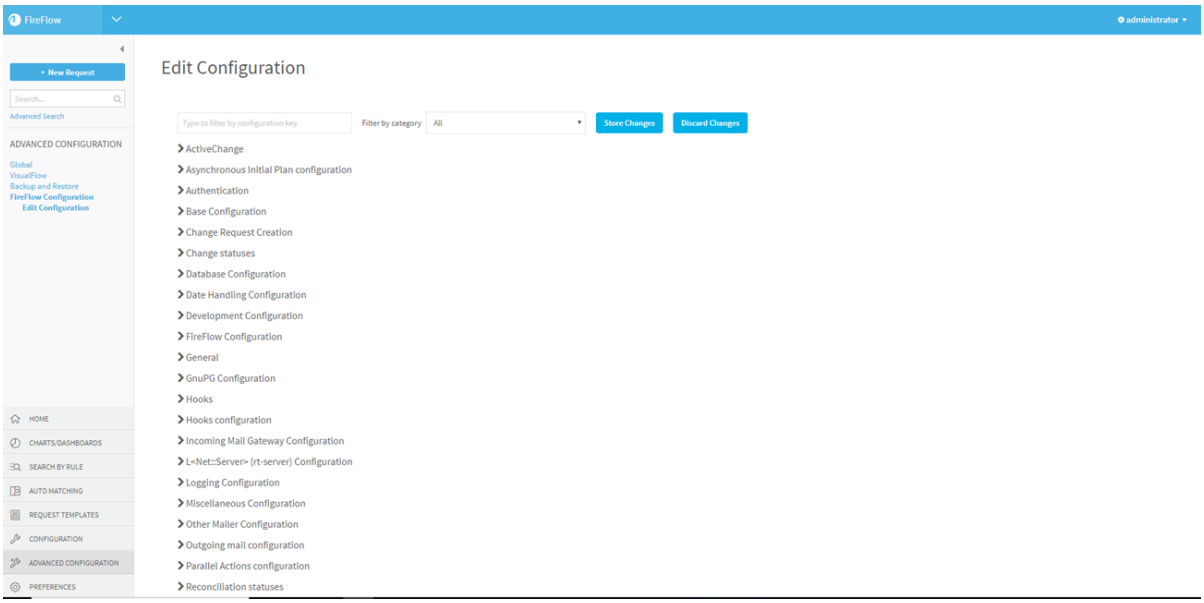
1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Advanced Configuration**.

   The **Advanced Configuration** page appears.



3. Click **FireFlow Configuration**.

   The **Edit Configuration** page appears.



4. Type the configuration parameter you want to set into the **Type to filter by configuration key** field.

   The configuration parameter appears.

5. Do one of the following:

   - To enable the configuration parameter's function, check the check box.
   - To disable the configuration parameter's function, uncheck the check box. Disabling the parameter reverts it to its default configuration.
   - To set a value for the parameter, click .

     The **Insert JSON value** field appears. Type the desired value into the field, and click **Done**.

6. Click **Save**.

   The configuration file `FireFlow_Config.json` is updated.

When the value of a parameter is not the default setting, Edited appears next the the parameter's name.

7. If necessary, restart FireFlow. For details, see Restart FireFlow.

Note: Whether restarting FireFlow is necessary is specified below each parameter in the Web Interface.

Configure FireFlow parameters (CLI)

You can optionally override system default settings using the CLI.

Do the following:

1. Log in to the FireFlow server using the username "root" and the related password.
2. Under the directory `/usr/share/fireflow/local/sbin/`, locate `FireFlow_edit_config.pl`.
3. If you do not know whether the configuration parameter has been previously configured, determine this by running the following:

   perl FireFlow_edit_config.pl -list -changed

   All parameters with a value different than the default value are printed.

   If the parameter you want to configure was printed, the parameter has been previously configured.

4. For each setting you want to override, do one of the following:

New configuration	To customize a system setting that has not been previously configured, run the following: **perl FireFlow_edit_config.pl -n** *<parameter_name>* **-add** *<parameter_value>* where, *<parameter_name>* is the name of the parameter and *<parameter_value>* is the desired parameter value.

Update configuration	To customize a system setting that has been previously configured, run the following: **perl FireFlow_edit_config.pl -n** *<parameter_name>* **-e** *<parameter_value>* where, *<parameter_name>* is the name of the parameter and *<parameter_value>* is the desired parameter value.

The configuration file `FireFlow_Config.json` is updated with the parameter's new setting.

5. If necessary, restart FireFlow. For details, see Restart FireFlow.

Note: Whether restarting FireFlow is necessary is specified below each parameter in the Web Interface.

Revert to FireFlow defaults

Depending on your system configuration, you may want to periodically revert to FireFlow system defaults.

Do the following:

1. Log in to the FireFlow server using the username "root" and the related password.
2. (Recommended) In the directory `/usr/share/fireflow/local/etc/site/`, backup the file `FireFlow_Config.json`.
3. Remove `FireFlow_Config.json` from the directory.
4. In the directory `/usr/share/fireflow/local/etc/site/po/`, remove any *.po files.
5. Run the FireFlow setup tool `fireflow_setup_config.sh`.

Restart FireFlow

FireFlow configuration parameter reference

This section describes specific system settings that can be customized, most via setting their configuration parameter(s).

For more details, see Override FireFlow system defaults.

Note: You can find all configuration parameters and their descriptions in the FireFlow user interface.

Additionally, the `FireFlow_Config.json` file located under `/usr/share/fireflow/local/etc/` contains detailed information about each parameter.

For more details, contact AlgoSec.

FireFlow includes the following types of configuration parameters:

- Display option parameters
- Requestor option parameters
- Traffic field parameters
- Network Address Translation (NAT) parameters
- Email parameters
- Asynchronous task parameters
- SLA parameters
- Recertification parameters
- Change request parameters for policy-based devices
- Initial planning parameters
- Sub-request parameters
- Finding affected rules parameters
- Work order parameters

- ActiveChange parameters
- Change validation parameters
- FireFlow logging parameters
- Additional FireFlow parameters

Display option parameters

Configuring the Maximum Rows Displayed in Home Page Lists

By default, FireFlow shows a maximum of 10 rows in each change request list in the **Home** page. You can modify this system default using the following configuration parameter.

Note: This system default can also be overridden by individual users via the page **Preferences > FireFlow Home Page**.

Configuration Parameter Name	Value
`DefaultSummaryRows`	The desired number of rows in each change request list in the **Home** page. To specify an unlimited number of rows, set the value as an empty string (**" "**). The default setting is 10 rows.

Configuring Whether to Draw Charts on Bigger Canvas

If desired, you can specify that charts be drawn on bigger canvases.

Configuration Parameter Name	Value
`BigCharts`	**0**. To specify that charts be drawn on the standard canvas size. (Default) **1**. To specify that charts be drawn on a bigger canvas.

Configuring the Change Request History Order

By default, FireFlow displays the change request history with the newest item appearing at the top, and change request creation appearing at the bottom. You can reverse the order using the following procedure.

Note: This system default can also be overridden by individual users via the page **Preferences > Settings**.

Configuration Parameter Name	Value
`OldestTransactionsFirst`	**0**. To display change request histories with the newest items appearing at the top. (Default) **1**. To display change request histories with the newest items appearing at the bottom.

Including/Excluding a Change Request's History in the Change Request's Display Page

By default, FireFlow displays a change request's history on the change request's display page. If desired, you can exclude this information.

Configuration Parameter Name	Value
`ShowTicketHistory`	**0**. To exclude the change request's history. **1**. To include the change request's history. (Default)

Configuring the Maximum Rows Displayed in Auto Matching Page Sub-Lists

By default, FireFlow shows a maximum of 100 rows in each sub-list in the **Auto Matching** page. You can modify this system default using the following procedure.

Note: This system default can also be overridden by individual users via the page **Preferences > Auto Matching**.

Configuration Parameter Name	Value
`ChangesMaxRows`	The desired number of rows in each sub-list in the **Auto Matching** page. To specify an unlimited number of rows, set the value as an empty string (**" "**). The default setting is 100 rows.

Configuring the Time Frame for Items Displayed in Auto Matching Page Lists

By default, FireFlow shows matches made in the last 30 days in each sub-list in the **Auto Matching** page. If desired, you can modify this.

Note: This system default can also be overridden by individual users via the page **Preferences > Auto Matching**.

Configuration Parameter Name	Value
`ReconciliationLastDays`	The desired number of days for which to display matches in each sub-list in the **Auto Matching** page. To specify an unlimited number of days, set the value as an empty string (**" "**). The default setting is 30 days.

Hiding Change Request Fields

If desired, you can hide the following change request fields:

- `Priority`
- `Due`
- `Describe the issue`
- `Cc`
- `Refers To` and `Referred to by`, together

Hidden fields will not be displayed in the FireFlow Web interface.

Note: Hidden fields are not *removed* from change requests; they are just not *displayed*. A hidden field can still be assigned a value via the request template, and workflow conditions that rely upon a hidden field will still work.

Configuration Parameter Name	Value
`HideFieldsFromTicket`	A bracket enclosed, comma seperated list, including each field you want to hide. Each field must be enclosed in quotation marks. The fields to hide: • **Priority** • **Due** • **Describe the issue** • **Cc** • **RefersTo** (which will hide "Refers To" and "Referred to by"). For example, the following value hides the Priority, Describe the issue, and Cc fields: **["Priority", "Describe the issue", "Cc"]** The default value is an empty list (**[]**), meaning that none of the fields are hidden.

Configuring the Date Format

When filling in a change request's due date or expiration date, and when searching for change requests according to these date fields, users can specify the desired date in a variety of formats (for example, "20 Oct 09", "Oct 20 2009", "2009-10-20", and more). By default, FireFlow interprets inputted dates in the format ##/##/## as "dd/mm/yy" (for example, 10/11/09 is interpreted as the 10th of November, 2009). This system default can be changed to "mm/dd/yy" (for example, 10/11/09 is interpreted as the 11th of October, 2009).

Configuration Parameter Name	Value
DateDayBeforeMonth	0. To interpret inputted dates in the format ##/##/## as "mm/dd/yy". 1. To interpret inputted dates in the format ##/##/## as "dd/mm/yy". (Default)

Adding a Custom Logo

You can add a custom logo to the top right corner of every page in ASMS. This option is configurable in the AFA Web Interface.

Note: Additionally, the logo will appear on all new AFA reports. Existing reports will not change.

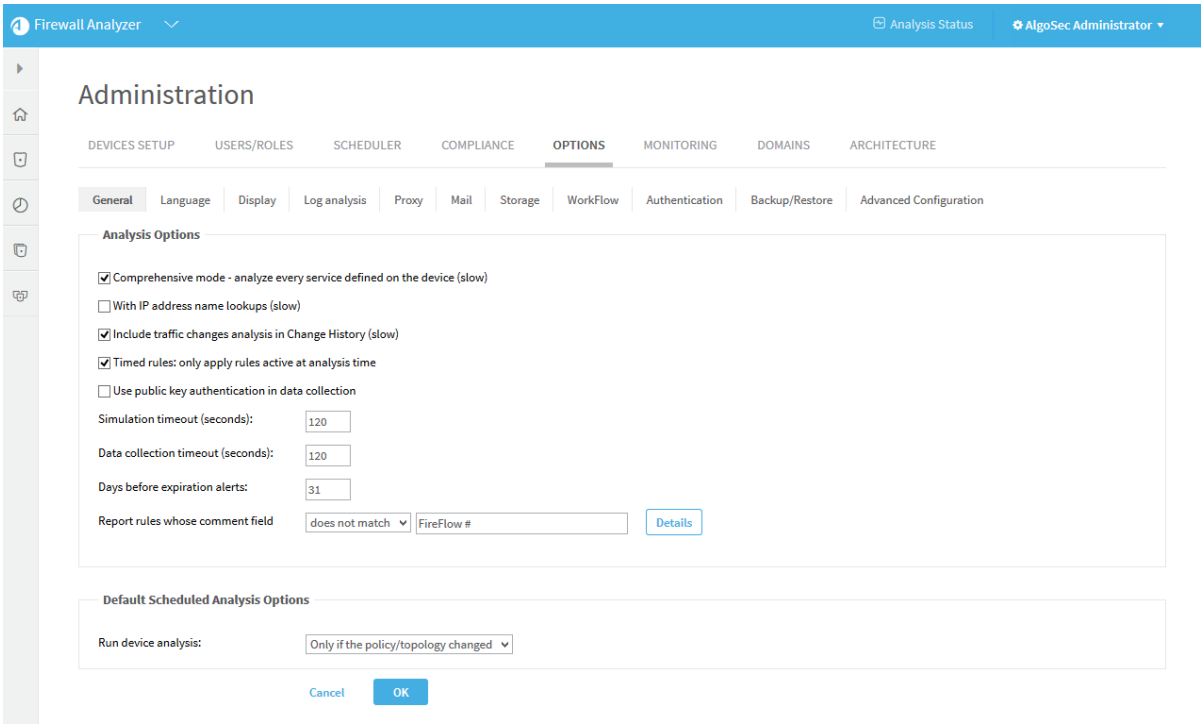
To add a custom logo

1. Create a logo file.

   The logo file must be in GIF, JPG, or PNG format, and it must be 115 pixels in width and 50 pixels in height. It is important to use these exact dimensions, so that the logo image is not distorted.
2. Switch to AFA.
3. In the toolbar, click your username.

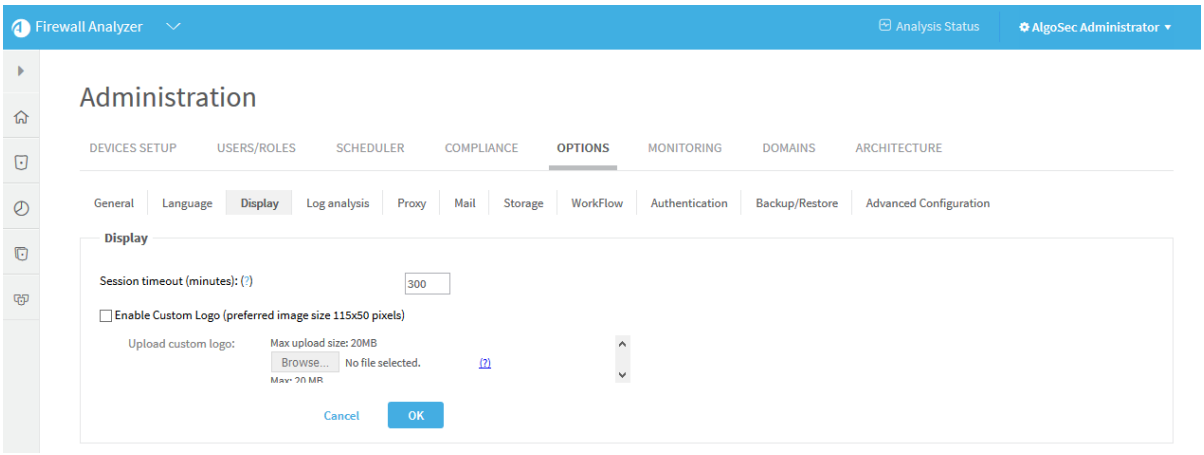
   A drop-down menu appears.
4. Select **Administration**.

   The **Administration** page appears, displaying the **Options** tab.



5. Click the **Display** tab.

   The **Display** page appears.



6. Select the **Enable Custom Logo** check box.
7. Click **Browse** and navigate to the custom logo file.
8. Click **Open**.
9. Click **OK**.

The custom logo is uploaded.

A success message appears.

10. Click **OK**.

To remove a custom logo

1. Switch to AFA.
2. In the toolbar, click your username.

   A drop-down menu appears.
3. Select **Administration**.

   The **Administration** page is displayed with the **Options** tab selected.
4. Click the **Display** tab.

   The **Display** page appears.
5. Clear the **Enable Custom Logo** check box.
6. Click **OK**.

The custom logo is removed.

Configuring FireFlow's Default Interface Language

FireFlow's default interface language is English. If desired, you can change the language.

Configuration Parameter Name	Value
`DefaultLang`	**zh_CN** – Chinese (PRC) **zh_TW** – Chinese (Taiwan) **hr** – Croatian **cs** – Czech **da** – Danish **nl** – Dutch **en** – English **fi** – Finnish **fr** - French **de** – German **he** - Hebrew **hu** – Hungarian **id** – Indonesian **it** – Italian **ja** – Japanese **nb** – Norwegian Bokmal **pl** – Polish **pt** – Portuguese **pt_BR** – Portuguese (Brazillian) **ru** – Russian **es** – Spanish **sv** – Swedish **tr** – Turkish

Modifying FireFlow Interface Text

You can modify the text appearing in the FireFlow interface in the following ways:

- **Change the language**

  For example, you can change the interface language to French, Spanish, or any other language.

- **Change the wording**

  For example, you can change the name of the "Change Requests Waiting for User Accept" list to "Change Requests Waiting to be Accepted".

Do the following:

1. Under `/usr/share/fireflow/local/po` or `/usr/share/fireflow/lib/RT/I18N`, open the *.po file of the language whose texts you want to translate or change.
2. In any text editor, create a language file encoded in UTF-8.
3. Add the following lines at the start of the new language file you created:

   ```
   msgid ""
   msgstr ""
   "Content-Type: text/plain; charset=UTF-8\n"
   ```

   Note: These must be the first three lines of the file.

4. For each string you want to translate or change, copy the relevant `msgid` lines from the *.po file you opened into the language file you created.

   The `msgid` lines represent the original text.

5. In the language file you created, after each `msgid` line, add a `msgstr` line specifying the desired text.

   For example, to translate the text on the **No Change Record** button into French, the file should include the following lines:

   ```
   msgid "No Change Record"
   msgstr "Aucun enregistrement de modification"
   ```

To translate the **Add More Files** link to French, the file should include the following lines:

```
msgid "Add More Files"    msgstr "Ajouter d'autres fichiers"
```

Tip: You can also translate text that includes placeholders (in the format `%x`), by including the same placeholders in the translation.

For example:

```
msgid "Owner changed from %1 to %2"    msgstr "Propriétaire changé de %1 en %2"
```

6. Close the original *.po file without saving changes.
7. Save the new file as `XX.po`, where `XX` is a two-letter abbreviation of the language used in the file or some other indication of the file's use.
8. Log in to the FireFlow server using the username "root" and the related password.
9. Place the language file on the FireFlow server, under the directory `/usr/share/fireflow/local/etc/site/po/`.

   Note: You can use `scp` to copy the file from your own computer to the FireFlow server.

10. Restart FireFlow.

FireFlow will refer to the new *.po file for strings. If a string does not appear in the file, FireFlow will refer to the original English-language *.po file for the missing string.

Modifying Workflow Stage Names

You can modify the names of stages in every workflow in FireFlow, or in specific workflows.

Configuration Parameter Name	Value
`WorkflowStagesNamesTranslation`	A copy of the default or current configuration, with the stage names on the right side of the colon modified as desired. You can specify different stage names for different workflows by adding multiple comma separated configurations. See the examples below for details. The default configuration for all workflows is as follows: `{ "default": { "certify": "Certify", "check": "Approve", "implement": "Implement", "open": "Plan", "reconcile": "Match", "rejected": "Rejected", "review": "Review", "validate": "Validate" } }` The left side of each colon is the internal name for each workflow stage, and the right side of each colon is the name that appears in the Web Interface for each stage.

Example 1:

The following value renames the **Implement** stage for all workflows the **Commit** stage.

The change appears in bold.

```
{   "default": {
"certify": "Certify",
"check": "Approve",
"implement": "Commit",
"open": "Plan",
"reconcile": "Match",
```

```
"rejected": "Rejected",
"review": "Review",
"validate": "Validate" } }
```

Example 2:

The following value renames the **Implement** stage of the Web Filter workflow the **Commit** stage. All other workflows keep the default stage names. The change appears in bold.

```
{   "default": {
"certify": "Certify",
"check": "Approve",
"implement": "Implement",
"open": "Plan",
"reconcile": "Match",
"rejected": "Rejected",
"review": "Review",
"validate": "Validate" }
,
"Web-filter": {
"certify": "Certify",
"check": "Approve",
"implement": "Commit",
"open": "Plan",
"reconcile": "Match",
"rejected": "Rejected",
"review": "Review",
"validate": "Validate" } }
```

Configuring Whether the Standard Template Appears in the Request Templates Page

By default, FireFlow displays the Standard template as an option in the **Request Templates** page. The standard template is a "default" traffic template which includes all

built-in fields (FireFlow fields) and uses the standard workflow. If desired, you can specify that the Standard template should not appear in this page.

Note: By default, FireFlow includes a single queue called “Firewalls”. When there are multiple queues, and a user is allowed to create change requests in more than one queue, the Standard template does not appear. (This is because a change request's template must specify the queue in which the change request is created, and the Standard template does not include pre-filled fields.)

Configuration Parameter Name	Value
`ShowStandardTemplate`	**0**. To specify that the Standard template should not appear in the **Request Templates** page. **1**. To specify that the Standard template should appear in the **Request Templates** page. (Default)

Requestor option parameters

Enabling/Disabling the No-Login Web Form

FireFlow includes a No-Login Web form that allows users to submit requests without logging in to the system. If desired, you can disable this, requiring authentication for change request creation.

Configuration Parameter Name	Value
`AllowNoAuthTicketCreation`	**0**. To disable the No-Login Web form. **1**. To enable the No-Login Web form. (Default)

Configuring Requestor User Properties

When using the `GetRequestorSearches` hook to display searches in the Requestor Web Interface, the hook retrieves a list of the requestor's user properties as a hash. By default, the following properties are included:

- `City`
- `Country`
- `EmailAddress`
- `HomePhone`
- `Id`
- `Organization`
- `RealName`
- Custom user fields. These fields will appear without spaces as hash keys. For example, a custom field named "Custom Field" will appear as: "`CustomField`".

For example, the user properties hash in XML format may appear as follows:

```
<User>
<City></City>
<Country></Country>
<EmailAddress>requestor1@mycompany.com</EmailAddress>
<HomePhone></HomePhone>
<Id>6894</Id>
<Organization></Organization>
<RealName>Rachel Requestor</RealName>
<CustomField></CustomField>
</User>
```

If desired, you can modify the included user properties.

Configuration Parameter Name	Value

`UserFieldsForHooksSearch`	The default or current value, with the desired modifications. To add items to the user properties list, add the desired user properties in single quotation marks, separated by commas.
	You can add any of the properties listed in the following table.
	The default value is as follows:
	`[`
	`"Id",`
	`"RealName",`
	`"HomePhone",`
	`"Organization",`
	`"EmailAddress",`
	`"City",`
	`"Country"`
	`]`

Supported User Properties

Property	Description
`Address1`	The requestor's primary mailing address.
`Address2`	The requestor's secondary mailing address.
`AuthSystem`	The type of authentication to use for the requestor.
`City`	The requestor's city.
`Comments`	Comments about the requestor.
`Country`	The requestor's country.
`Created`	The date on which the requestor was added to FireFlow.
`Creator`	The user who added the requestor to FireFlow.

Property	Description
`EmailAddress`	The requestor's email address.
`HomePhone`	The requestor's home telephone number.
`Id`	The requestor's ID number.
`Lang`	The requestor's desired FireFlow interface language.
`LastUpdated`	The date on which the requestor's properties were last updated in FireFlow.
`LastUpdatedBy`	The user who last updated the requestor's properties in FireFlow.
`MobilePhone`	The requestor's mobile telephone number.
`Name`	The requestor's username.
`Nickname`	The requestor's nickname.
`Organization`	The requestor's organization.
`PagerPhone`	The requestor's pager number.
`Password`	The requestor's password.
`RealName`	The requestor's full name.
`Signature`	The requestor's signature.
`State`	The requestor's state.
`TimeZone`	The requestor's time zone.
`WorkPhone`	The requestor's work telephone number.
`Zip`	The requestor's zip code.

Configuring a Help Link for the Requestor Interface

If desired, you can configure the FireFlow Requestor Interface to display a link to a custom Help. The link can vary depending on whether the user is an authenticated requestor, or is using the No-Login Web Form. Clicking the link will open a new tab, and link to a customized page. The link will always appear at the top of the **Home** page and at the top of the **Create a New Change Request** page.

Note: The customized page can be on an external server or on the AlgoSec server. An external server is preferred. If you require the page be installed on the AlgoSec server, contact AlgoSec support for further information.

Configuration Parameter Name	Value

ChangeRequestCreationInstructions	A copy of the default or current configuration, with the **Label** (text of the link)and **URL** properties modified as desired. You can specify different properties for Requestors (authenticated users) and unauthenticated users (users of the no-login web form). See the example below for details.
	The default configuration is as follows:
	`{ "Requestor": { "Label": "How to submit a FireFlow change request as a requestor?", "URL": http://www.example.com/NewCRInstructions_Requestors.html" }, "Unauthenticated": { "Label": "How to submit a FireFlow change request?", "URL": "http://www.example.com/NewCRInstructions_Unauth.html" } }`
	Example: The following value configures a link for unauthenticated users with the name **Access Help** which sends you to **http://www.MyRequestorHelp.com**. The changes appear in bold.
	`{ "Requestor": { "Label": "How to submit a FireFlow change request as a requestor?", "URL": http://www.example.com/NewCRInstructions_Requestors.html" }, "Unauthenticated": { "Label": "Access Help", "URL": "http://www.MyRequestorHelp.com" } }`

Traffic field parameters

Enable / disable multiple traffic rows in change requests

By default, FireFlow allows users to add more traffic rows to a change request, by clicking **Add More Traffic**. If desired, you can disable this option and remove the **Add More Traffic** button.

Configuration Parameter Name	Value
`EnableMultipleTraffic`	**0**. To disable multiple traffic rows. **1**. To enable multiple traffic rows. (Default)

Determine whether traffic fields are mandatory

By default, the source, destination, service, and action fields are mandatory for traffic change requests, and FireFlow automatically validates these fields to ensure they are filled in. If desired, you can specify that traffic fields are optional.

Note: You can also disable automatic traffic field validation for the value of traffic fields. See Enabling/Disabling Traffic Field Validation (see Enable / disable traffic field validation).

Configuration Parameter Name	Value
`AllTrafficFieldsMandatory`	**0**. To specify that traffic fields are optional. **1**. To specify that traffic fields are mandatory. (Default)

Enable / disable traffic field validation

By default, FireFlow automatically validates traffic fields in change requests, to determine whether all mandatory fields are filled in with appropriate values. If desired, you can disable validation of traffic fields.

Configuration Parameter Name	Value
`ValidateTrafficFields`	**0**. To disable traffic field validation. **1**. To enable traffic field validation. (Default)

Enable / disable application or service translation for Palo Alto devices

When a change request is submitted for a Palo Alto device, the requestor may define the traffic using a service, even when it would be better to define the traffic with an application.

If desired, you can enable automatic translation of services to their relevant applications. After initial planning, the sub-requests will be created with the service "application-default" and the relevant application. Services will only be translated into an application if they match an application's default service exactly and uniquely.

Note: AppViz users should not enable this configuration option as it will cause flows to fail validation.

Note: This configuration option is only relevant when application awareness is enabled. See Enabling/Disabling User and Network Application Awareness (see Enable / disable user and network application awareness).

Note: The maximum number of services translated per traffic line is three. If more than three services appear in a single traffic line, the services in that line will not be translated into applications.

Configuration Parameter Name	Value
`PanoramaServicesTranslation`	**0**. To disable application/service translation. (Default) **1**. To enable application/service translation.

Enable / disable user and network application awareness

ASMS supports the **User** traffic field for Check Point devices and the **User** and **Application** traffic fields for Palo Alto devices. Network application awareness parameters must be manually enabled.

Awareness means that these fields will appear wherever traffic fields appear and will be considered in all traffic simulation queries such as initial planing, risk checks, and connectivity checks.

If desired, you can manually enable or disable user and network application awareness in FireFlow and AppViz.

Note: After changing either of these parameters, you must restart AppViz in addition to restarting FireFlow.

Note: Disabling this support discards all user and/or network application data in FireFlow and AppViz.

Configuration Parameter Name	Value
`ShowApplicationFieldInCreateForm`	**0**. To disable network application awareness in FireFlow and AppViz. (default) **1**. To enable network application awareness in FireFlow and AppViz.
`ShowUserFieldInCreateForm`	**0**. To disable user awareness in in FireFlow and AppViz. (default) **1**. To enable user awareness in in FireFlow and AppViz.

Enable / disable inclusion of user-defined custom traffic fields in flat tickets

By default, FireFlow automatically includes all user-defined custom traffic fields (traffic fields, source fields, user fields, destination fields, service fields, and application fields)

in the XML of a change request (a *flat ticket*). If desired, you can disable inclusion of such fields in flat tickets.

Configuration Parameter Name	Value
`IncludeUserDefinedTrafficCustomFieldsInXML`	**0**. To disable inclusion of user-defined custom traffic fields in flat tickets. **1**. To enable inclusion of user-defined custom traffic fields in flat tickets. (Default)

Network Address Translation (NAT) parameters

Adding/Removing Standard NAT Fields in Change Requests

You can remove all standard NAT fields from change requests. The standard NAT fields include:

- **Source NAT**
- **Destination NAT**
- **NAT Type**
- **Port Translation**

Note: The following procedure will remove the standard NAT fields for all users except FireFlow configuration administrators. If it is necessary to remove these fields for FireFlow configuration administrators as well, contact AlgoSec Professional Services.

To add/remove standard NAT fields in change requests

1. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page is displayed.

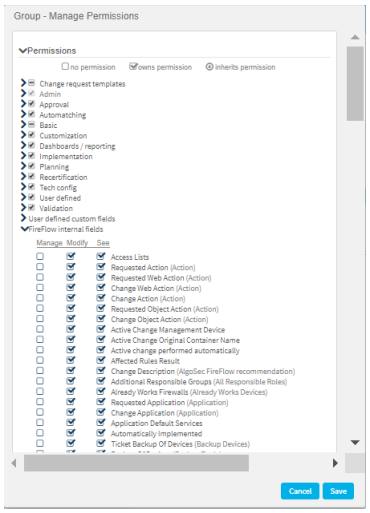
2. Click **Roles**.

The **Select a role** page is displayed.

3. For each role, do the following:

   a. In the row of the role, click .

      The **Manage Permissions** window for the role appears.



   b. Click › next to **FireFlow internal fields**.

      The **FireFlow internal fields** are displayed.

   c. Do one of the following:

      Note: These check boxes might not appear for all user roles.

      - To add the standard NAT fields, check the **See** and **Modify** check boxes for all FireFlow fields listed in the table below.
      - To remove the standard NAT fields, clear the **See** and **Modify** check boxes for all FireFlow fields listed in the table below.

   d. Click **Save**.

NAT-related FireFlow Fields

FireFlow Field	Description
Change Destination NAT	Displays the destination NAT value to which the connection's destination should be translated, as planned during the Plan stage.
Change NAT Type	Displays the type of NAT (Static or Dynamic), as planned during the Plan stage.
Change Port Translation	Displays the port value to which the connection's port should be translated, as planned during the Plan stage.
Change Source NAT	Displays the source NAT value to which the connection's source should be translated, as planned during the Plan stage.
Requested Destination NAT	Displays the destination NAT value to which the connection's destination should be translated, as specified in the original request.
Requested NAT Type	Displays the type of NAT (Static or Dynamic), as specified in the original request.
Requested Port Translation	Displays the port value to which the connection's port should be translated, as specified in the original request.
Requested Source NAT	Displays the source NAT value to which the connection's source should be translated, as specified in the original request.

Adding/Removing Optional NAT Fields in Change Requests

You can configure FireFlow to display separate fields for source NAT, destination NAT, and port translation before and after translation. In this case, the existing **Source NAT**, **Destination NAT**, and **Port Translation** fields will display the values before translation, and the following new fields will display the values after translation:

- **Source after NAT**
- **Destination after NAT**
- **Port after Translation**

The new NAT fields will appear below the standard NAT fields throughout the FireFlow Web interface, for example in work orders or when editing a change request.

To add optional NAT fields

1. On the original site, open a terminal and log in using the username "root" and the related password.
2. Enter the following command:

   /usr/share/fireflow/local/sbin/additional_NAT_fields.pl -e

   The optional NAT fields are added to the FireFlow Web interface.

To remove optional NAT fields

1. On the original site, open a terminal and log in using the username "root" and the related password.
2. Enter the following command:

   /usr/share/fireflow/local/sbin/additional_NAT_fields.pl -d

   The optional NAT fields are removed from the FireFlow Web interface.

Configuring NAT Enhancements in Traffic Change Requests

By default, FireFlow provides the following NAT features:

- A traffic change request which includes NAT fields will stay open, even if the requested traffic is already allowed.
- The initial planning analysis uses NAT addresses.
- During initial planning, you can specify a NAT location in the NAT settings window.
- Risk checks use NAT information.
- Only relevant addresses appear on sub-requests.

If desired, you can disable the above features. You can disable all of the features, or only disable using NAT information in risk checks.

Configuration Parameter Name	Value
`handleNATChanges`	**0**. To disable NAT enhancements in traffic change requests. **1**. To enable NAT enhancements in traffic change requests. (Default)

If you enabled NAT enhancements in traffic change requests, configure whether FireFlow should use NAT information in risk checks.

Note: When this feature is enabled, the **Source NAT** and **Destination NAT** fields will be used in risk checks. However, if the optional **Source after NAT** field is enabled, it will be used instead of the **Source NAT** field. Likewise, if the optional **Destination after NAT** field is enabled, it will be used instead of the **Destination NAT** field. For information on these optional fields, see Adding/Removing Optional NAT Fields in Change Requests (see Adding/Removing Optional NAT Fields in Change Requests).

Configuration Parameter Name	Value
`sendNATinformationInRiskCheck`	**0**. To disable using NAT information in risk checks. **1**. To enable using NAT information in risk checks. (Default)

Email parameters

Configuring the "From" Address in Dashboard Emails

Users who are subscribed to dashboards periodically receive the dashboard's content via email. By default, the email's "From" field displays the FireFlow server's email

address. If desired, you can change the email address displayed in the "From" field of dashboard emails.

Configuration Parameter Name	Value
`DashboardAddress`	The email address that you want to appear as the "From" address in dashboard emails. Example: The following value sets the address to "admin@mycompany.com" **admin@mycompany.com**

Enabling/Disabling Email Notifications for Requestors

By default, FireFlow will send email notifications to requestors. These notifcations occur when their request is approved, denied, additional information is required, etc. If desired, you can configure FireFlow to never send email notifications to requestors.

Note: In the log, skipped requestors are identified as follows: `<addr> belongs to the requestor [<name>]. Skipping`

Configuration Parameter Name	Value
`SendEmailsToRequestors`	**0**. To disable email notifications for requestors. **1**. To enable email notifications for requestors. (Default)

Enabling/Disabling Inclusion of the Rule to be Removed in Email Notifcations for Related Change Requests

In the Approve stage of the Rule Removal request's lifecycle, FireFlow sends an email to the requestors of change requests with traffic intersecting that of the rule slated for removal, informing them that the rule will be removed by a certain date. By default, the email includes a table displaying the rule in question. If desired, you can specify that this table should not be included in the email.

Configuration Parameter Name	Value
`ShowRuleInfoWhenNotifyRuleToRemove`	**0**. To disable including a table with the rule to be removed in email notifications. **1**. To enable including a table with the rule to be removed in email notifications. (Default)

Enabling/Disabling Opening of Change Requests Via Email

By default, FireFlow allows opening change requests via email. If desired, you can disable this feature.

Note: When opening change request via email is disabled, commenting on change requests via email is still allowed.

Configuration Parameter Name	Value
`AllowCreateTicketFromEmails`	**0**. To disable opening change request via email. **1.** To enable opening change request via email. (Default)

Configuring Link URLs to FireFlow pages

By default, links to FireFlow pages use the URL used by the client incoming request. These links include:

- Links to FireFlow pages in emails sent by FireFlow.
- Links in the "reffered to" field of a change requests to another change request.

If desired, you can configure FireFlow to use a specific URL you configure: the IP Address or hostname for your FireFlow server. This configuration is recommended when using FireFlow behind a reverse proxy.

Configuration Parameter Name	Value
`WebBaseURL`	The base URL of the FireFlow server. When the value is set as an empty string (" "), the server will determine its own IP address. (Default) **Example** `https://fireflow.company.com` **Note:** The URL does not require a trailing "/".
`WebURL`	The FireFlow application URL. When the value is set as an empty string (" "), the server will determine its own IP address. (Default) **Example** `https://fireflow.company.com/FireFlow/`
`CanonicalizeRedirectURLs`	**0**. To configure FireFlow to use URLs used by the client incoming request. (Default) **1**. To configure FireFlow to use URLs configured with the `WebBaseURL` and `WebURL` parameters. This is typically relevant when using FireFlow behind a reverse proxy.

Customizing the incoming email parsing format

In organizations where submitting requests to FireFlow via email is supported, all request emails must confirm to the following format by default:

```
Source: <source>Destination: <destination>Service: <service>Action: <action>
```

where:

`<source>` is the IP address, IP range, network, or device object.

`<destination>` is the IP address, IP range, network, or device object.

`<service>` is the device service or port for the connection.

`<action>` is the device action to perform for the connection. This can be either of the following:

- `allow` - Allow the connection.
- `drop` - Block the connection.

If desired, you can change the required format for request emails. For further information, contact AlgoSec.

Asynchronous task parameters

Configuring Change Request Creation

By default, FireFlow creates change requests asynchronously. This enables you to complete other tasks while FireFlow creates the change request. If desired, you can disable this. When asynchronous change request creation is enabled, you can configure the length of time FireFlow has to create the change request before the action will timeout. The default timeout value is 600 seconds (10 minutes).

Configuration Parameter Name	Value
`CallTicketCreationAsync`	**0**. To disable asynchronous change request creation. **1**. To enable asynchronous change request creation. (Default)
`AsyncTicketCreationTimeout`	The desired timeout value, in seconds. The default value is **600** (10 minutes).

Enabling/Disabling Asynchronous Initial Plan

To control the initial planning phase, see Configuring Initial Planning (see Configuring Initial Planning).

Enabling/Disabling Asynchronous Sub-Request Creation

At the end of the Initial Planning stage in the change request lifecycle, FireFlow creates a sub-request for each affected device. By default, FireFlow creates sub-requests synchronously.

If desired, you can enable asynchronous sub-request creation. This enables you to complete other tasks while FireFlow creates the sub-requests. When asynchronous sub-request creation is enabled, after initial planning, the **Home** page appears with a

link to the parent request and sub-requests displayed in a message at the top of the page.

Configuration Parameter Name	Value
`CallSubTicketCreationAsync`	**0**. To disable asynchronous sub-request creation. (Default) **1**. To enable asynchronous sub-request creation.

Enabling/Disabling Asynchronous Risk Checks

At the beginning of the Approve stage in the change request lifecycle, FireFlow performs a risk check. By default, FireFlow performs this risk check asynchronously. This enables you to view and handle the change request while FireFlow performs the risk check. If desired, you can disable this.

Configuration Parameter Name	Value
`CallRiskCheckAsync`	**0**. To disable asynchronous risk checks. **1**. To enable asynchronous risk checks. (Default)

Enabling/Disabling Asynchronous Work Order Creation

At the beginning of the Implement stage in the change request lifecycle, FireFlow creates a work order for each change request (in case of sub-requests, FireFlow creates a work order for each sub-request). By default, FireFlow creates the work order asynchronously. This enables you to view and handle the change request while FireFlow creates the work order. If desired, you can disable this.

Configuration Parameter Name	Value
`CallWorkOrderAsync`	**0**. To disable asynchronous work order creation. **1**. To enable asynchronous work order creation. (Default)

Configuring Background Task Prioritization

FireFlow performs the following background tasks:

Task Worker	Task Description
`CreateTicketWorker`	Creating Change Requests **Note:** This includes creating sub-requests when asynchronous sub-request creation is enabled.
`InitialPlanWorker`	Performing Initial Planning
`RiskCheckWorker`	Performing Risk Checks
`WorkOrderWorker`	Creating Work Orders
`SendEmailWorker`	Sending Emails

Each of these tasks are performed by general workers. By default, creating change requests is executed by the higher priority general worker, and performing initial planning, performing risk checks, creating work orders, and sending emails are executed by the lower priority general worker. If desired, you can change this behavior in the following ways:

- Change which task workers are executed by which general worker.
- Create a custom general worker (which you can assign the task workers you desire).

Each general worker has the following elements:

Element	Description
`niceLevel`	The priority of the worker. A higher number means the worker is a lower priority. Valid values are between 8 and 19.
`numOfWorkers`	The number of tasks that this general worker can execute in parallel.
`workers`	A list of the task workers performed by the general worker.

Note: When configuring general workers, there is a risk of overloading the machine. When in doubt, please contact AlgoSec support.

Parameter name: GeneralWorkers

Value: A copy of the default or current configuration, with the desired changes.

See the examples below for details.

The default value is as follows:

```
{"HighPriority": {
"niceLevel": 8,
"numOfWorkers": 3,
"workers": [ "CreateTicketWorker" ] },
"RegularPriority": {
"niceLevel": 10,
"numOfWorkers": 3,
"workers": [
"InitialPlanWorker", "SendEmailWorker", "WorkOrderWorker",
"RiskCheckWorker", "ValidationWorker" ] } }
```

Example 1: The following value configures initial planning to be executed by the higher priority general worker. The change appears in bold.

```
{"HighPriority": {
"niceLevel": 8,
"numOfWorkers": 3,
"workers": [ "CreateTicketWorker", "InitialPlanWorker" ] },
"RegularPriority": {
"niceLevel": 10,
"numOfWorkers": 3,
"workers": [
"SendEmailWorker", "WorkOrderWorker", "RiskCheckWorker",
"ValidationWorker" ] } }
```

Example 2: The following value configures a lower priority custom general worker **LowPriority**, and the task workers for performing risk checks and change validation were moved to this general worker (and will therefore be performed at a lower priority). The change appears in bold.

```
{"HighPriority": {
"niceLevel": 8,
"numOfWorkers": 3,
"workers": [ "CreateTicketWorker" ] },
"RegularPriority": {
"niceLevel": 10,
"numOfWorkers": 3,
"workers": [
"InitialPlanWorker", "SendEmailWorker", "WorkOrderWorker" ] },
"LowPriority": {
"niceLevel": 12,
"numOfWorkers": 3,
"workers": [
"RiskCheckWorker", "ValidationWorker" ] } }
```

Configuration Parameter Name	Value
`GeneralWorkers`	A copy of the default or current configuration, with the desired changes.

Note: There is no prioritizing workers within the same general worker.

Note: If a specific task worker is not defined in any of the general workers, and it is enabled, a new general worker named "default" will be created to perform this task.

SLA parameters

Configuring FireFlow to Measure SLO Time in Business Hours

By default, the time spent in each SLO is measured absolutely. If desired, you can configure the time spent in each SLO to be measured in business hours.

Configuration Parameter Name	Value
`UseBusinessHoursInSLA`	**0**. To measure the time spent in each SLO absolutely. (Default) **1**. To measure the time spent in each SLO in business hours.

Configuration Parameter Name	Value
BusinessHours	A copy of the default or current configuration, modified to represent your company's business hours and holidays. See the desciption of the default configuration (below) for details. The default configuration is as follows: { "0": { "End": "18:00", "Name": "Sunday", "Start": "09:00" }, "1": { "End": "18:00", "Name": "Monday", "Start": "09:00" }, "2": { "End": "18:00", "Name": "Tuesday", "Start": "09:00" }, "3": { "End": "18:00", "Name": "Wednesday", "Start": "09:00" }, "4": { "End": "18:00", "Name": "Thursday", "Start": "09:00" }, "5": { "End": null, "Name": "Friday", "Start": null }, "6": { "End": null, "Name": "Saturday", "Start": null }, "holidays": ["01-01", "12-25"] } **Work hours per week:** Each day of the week is represented by the following elements: • **Start**. The time the workday starts (in 24 hour format) • **End**. The time the workday ends (in 24 hour format) • **Name**. The name of the day of the week. Set the value for **Start** and **End** to `null` for days of the week that are not work days. By default, work hours are set as Sunday through Thursday from 9:00 am to 6:00pm. **Holidays:** The **holidays** element includes the dates of the year that are not workdays (in MM-DD format). By default, the holidays are set as January 1 and Decemeber 25.

Configuration Parameter Name	Value
`BusinessDayLength`	The average number of hours per working day. **Note:** Set this value only if your SLO timer is set not to clear on revisit (the default setting).

Configuring the Default Due Date for Rule Removal Requests

For Rule Removal requests, the **Due Date** field specifies the date by which requestors of related change requests must respond regarding the rule's impending deletion. This field's default value is 14 days from the change request's creation. If desired, you can change the default value.

Configuration Parameter Name	Value
`DefaultRuleRemovalDue`	The desired default value for the due date of rule removal requests, expressed in number of days after change request creation. The default value is 14. (The due date is 14 days after the change request is created).

Recertification parameters

In this topic:

Configuring the Workflow Used for Recertification Requests

When traffic requests are resolved, you can request recertification by clicking the **Recertify** button. The default workflow for recertification requests is **Request-Recertification**. If desired, you can change the default workflow for recertification.

Configuration Parameter Name	Value
`RecertificationDefaultWorkflow`	The desired default recertification workflow. Valid values are workflows defined in VisualFlow and installed in FireFlow as **Request Recertification** type.

Configuring the Default Due Date for Change Requests Marked for Future Recertification

When marking change requests for future recertification, the due date for the change request(s) is, by default, deferred to 365 days from the original due date. If desired, you can change this default value.

Configuration Parameter Name	Value
`DefaultExpirationPeriod`	The desired default value for the due date of change requests marked for future recertification, expressed in number of days after the change request's original dute date. The default value is 365. (The due date of change requests marked for recertification is 365 days after the change request's original due date).

Configuring the Default Due Date for Recertification Requests

When recertifying a change request, the due date for the recertification change request, by default, is 14 days from the date the change request is created. If desired, you can change this default value.

Configuration Parameter Name	Value
`RecertificationDaysToWaitForResponses`	The desired default value for the due date of recertification requests, expressed in number of days after change request creation. The default value is 14. (The due date is 14 days after the change request is created).

Change request parameters for policy-based devices

In this topic:

Configuring Device-Based Change Requests for Policy-Based Devices

By default, FireFlow uses policy-based change requests for Palo Alto Networks Panorama, Check Point,and Fortinet FortiManager. The change requests will suggest modifying the policies installed on the devices that are relevant to the change from the perspective of the policy (not the individual devices).

If desired, you can configure FireFlow to create device-based change requests for these devices. The change request will modify the policy from the perspective of each relevant device, where each rule added to the policy will only be installed on a single device. Note that this behavior may cause the same rule to be added to a policy multiple times (once per relevant device).

Note: Policy-based change requests are not supported for Palo Alto Firewalls or Fortinet FortiGate devices defined in AFA directly (not via Panorama or FortiManager).

Note: When using policy-based change requests, you do have the option to specify that the change should only be installed on the specific devices relevant to the change (and not every device with the policy). See Configuring Policy-Based Work Orders to Recommend Installing Rules Only on Relevant Devices (see Configuring Policy-Based Work Orders to Recommend Installing Rules Only on Relevant Devices).

Configuration Parameter Name	Value
`PolicyBasedRequestFMGR`	**Policy**. All change requests will be policy-based. (Default) **None**. All change requests will be device-based.

Configuration Parameter Name	Value
`PolicyBasedRequestForCheckPoint`	**Policy**. All change requests will be policy-based. (Default) **None**. All change requests will be device-based.
`PolicyBasedRequestForPanorama`	**DeviceGroup**. All change requests will be policy-based. (Default) **None**. All change requests will be device-based.

Configuring Policy-Based Work Orders to Recommend Installing Rules Only on Relevant Devices

By default, FireFlow policy-based change requests will always recommend installing new rules for a policy on every device with the policy. FireFlow identifies the devices relevant to the requested change in **Initial Planning**, and the work order will suggest installing the new rules on every device with the same policy as the devices that were identified as relevant. This behavior is true for all policy-based change requests.

If desired, you can configure FireFlow to suggest changing only the devices relevant to the change request. When a policy-based change request work order suggests adding a new rule to a policy, the suggested rule's "install on" field will include only the devices **Initial Planning** identified as relevant to the change request. This will be the behavior for all policy-based devices.

By default, if more than 5 specific devices are identified as relevant, FireFlow will suggest installing the rule on every device with the policy. If desired, you can customize this threshold.

Note: This configuration option is only relevant when FireFlow manages Palo Alto Networks Panorama, Check Point, and Fortinet Fortimanager devices with policy-based changes requests (this is the default behavior). This is not relevant if FireFlow is configured to manage policy-based devices with device-based change requests.

For more information, see Configuring Device-Based Change Requests for Policy-Based Devices (see Configuring Device-Based Change Requests for Policy-Based Devices).

Configuration Parameter Name	Value
`ApplyPolicyOnSuggestedDevices`	**1**. To configure FireFlow to suggest new rules be installed on only the relevant devices. **0**. To configure FireFlow to suggest new rules be installed on all devices with the policy. (Default)
`MaxTargetThreshold`	The maximum number of specific devices to install a rule on without installing the rule on every device with the policy. (Only relevant when `ApplyPolicyOnSuggestedDevices` is set to **1**.) The default value is **5**.

➔ **See also**:

- AlgoSec & Palo Alto Networks

Initial planning parameters

Configuring Initial Planning

By default, FireFlow performs initial planning in the following manner:

Immediately upon creation of a change request, FireFlow performs initial planning by comparing the traffic specified in the change requests to the policies of relevant devices, using the most recent device configuration available on the AlgoSec server (made available via the real-time monitoring mechanism). If the traffic already works (meaning traffic is allowed for all routing devices in case of an 'allow' request, and possibly is not routed at all), then FireFlow automatically closes the change request and sends the requestor an email indicating that the change request was closed.

If desired, you can change this behavior in the following ways:

- Configure FireFlow to perform initial planning at the end of the Plan stage, instead of at the end of the Request stage.
- Configure FireFlow to use the periodic AFA device reports when performing initial planning, instead of using the real-time monitoring data.
- Disable automatic closing of change requests whose traffic already works.

Note: New change requests appear in the **Home** page's **New Change Requests** list once initial planning is complete or when ten minutes have elapsed since the change request's creation, whichever occurs first. Therefore, when initial planning occurs at the end of the Request stage, new change requests appear in the **Home** page as soon as traffic checking is done; however, when traffic checking occurs at the end of the Plan stage, ten minutes will pass before new change requests appear in the **Home** page.

Note: In order to cause new change requests to appear in the **Home** page immediately, regardless of when traffic checking occurs, customize the Network Operations role's **Home** page as follows: Remove the **"N" New Change Requests** element, and add the **"N" Total New Change Requests** element. New change requests will appear in the **Home** page's **Total New Change Requests** list immediately upon change request creation.

Note: For more details, see Customize the FireFlow Home page.

Configuration Parameter Name	Value
`CallInitialPlanAsync`	**0**. To configure FireFlow to perform initial planning at the end of the Plan stage. **1**. To configure FireFlow to perform initial planning at the end of the Request stage. (Default)

Configuration Parameter Name	Value
`UseMonitorDataForFirewallQuery`	**0**. To configure FireFlow to perform initial planning using AFA reports. **1**. To configure FireFlow to perform initial planning using real-time monitoring data. (Default)
`AutomaticCheckAlreadyWorks`	**0**. To disable automatic closing of change requests that already work. **1**. To enable automatic closing of change requests that already work. (Default)

Enabling/Disabling Displaying the Policy Name in Initial Planning

By default, the policy name is displayed in the initial planning results table and in the initial planning table of all devices (for manually adding additional relevant devices). If desired, you can disable this.

Configuration Parameter Name	Value
`DisplayFirewallPolicyInInitialPlan`	**0**. To disable displaying the policy name in initial planning. **1**. To enable displaying the policy name in initial planning. (Default)

Configuring the Initial Plan Expiration Period

By default, an initial plan will expire 2 days after it was calculated. If desired, you can change the expiration period. If you increase the expiration period, you additionally need to increase the expiration period for the data.

Configuration Parameter Name	Value
`InitialPlanResultValidityPeriod`	The desired expiration period for initial plan results, in seconds. The default value is 172800 (2 days).

Configuration Parameter Name	Value
`Work_Expiration_Hours_Time`	The same time period as the value for `InitialPlanResultValidityPeriod` , but set in hours. For example, if you set `InitialPlanResultValidityPeriod` to 259200 (3 days in seconds), set `Work_Expiration_Hours_Time` to 72 (3 days in hours). Ony set this parameter if you configured the expiration period (`InitialPlanResultValidityPeriod`) to a value greater than 172800 seconds.

Enabling/Disabling the Initial Plan PDF

By default, FireFlow creates a PDF with initial plan results that is accessible from the Web Interface. If desired, you can disable this.

Configuration Parameter Name	Value
`CreateInitialPlanPDF`	**0**. To disable creation of the initial plan PDF. **1**. To enable creation of the initial plan PDF. (Default)

Enabling/Disabling Inclusion of Initial Plan Information in Flat Tickets

By default, FireFlow does not include initial plan information in the XML of a change request (a *flat ticket*). If desired, you can change this.

Configuration Parameter Name	Value
`IncludeInitialPlanResultInXML`	**0**. To disable inclusion of initial plan information in flat tickets. (Default) **1**. To enable inclusion of initial plan information in flat tickets.

Enabling/Disabling Storing Allowing Rules from the Initial Plan Query

By default, FireFlow does not store the allowing rules that AFA finds in the initial plan query. If desired, you can change this. FireFlow will store the allowing rules in the **Initial Plan Results** custom field.

Configuration Parameter Name	Value
`ReturnAllowingRulesInQuery`	**0**. To disable storing allowing rules from the initial plan query. (Default) **1**. To enable storing allowing rules from the initial plan query.

Configuring Automatic Device Selection for Initial Plan Results

During initial planning, FireFlow automatically selects devices that are relevant to the request. By default, FireFlow will only automatically select Analysis and Monitoring supported devices. If desired, you can configure FireFlow to also select monitoring only devices. Optionally, you can disable automatic device selection completely.

Configuration Parameter Name	Value
`AutoCheckAEFInInitialPlan`	**0.** To allow automatic selection of only Analysis and Monitoring supported devices, during initial planning. (Default) **1**. To allow automatic selection of Monitoring only devices during initial planning.
`UncheckDevicesAfterInitialPlanning`	**0**. To enable automatic device selection during initial planning. (Default) **1**. To disable automatic device selection during initial planning..

Configuring Initial Plan Results for F5 BIG-IP

Note: This parameter is only relevant for F5 Big-IP devices defined in AFA as "F5 Big-IP LTM only" devices. This certainly includes all Analysis and Monitoring

supported F5 devices which were defined in AFA before version 2018.2. This parameter is irrelevant to F5 Big-IP devices defined in AFA from version 2018.2 as "F5 Big-IP LTM and AFM".

For F5 BIG-IP devices that were defined in AFA as "F5 Big-IP LTM only", you must set the following configuration parameter if these devices are in fact using AFM. If these devices are in fact using AFM, AFA traffic simulation query results are inconclusive because AFM may either allow or block the traffic. This affects Initial Plan, Work Order, and Change Validation results because they are all based on the AFA traffic simulation query.

When this parameter indicates that the devices are using AFM, this tells FireFlow that the AFA traffic simulation results may not be accurate. Consequently, FireFlow will provide relevant notifications and recommendations.

Configuration Parameter Name	Value
`IsF5AfmExist`	**0**. If using F5 BIG-IP LTM Only (Default) **1**. If using F5 BIG-IP LTM with AFM

Sub-request parameters

Configuring Sub-Request Ownership

By default, when the status of a change request changes, the owner of the parent request is not automatically assigned to the sub-requests. Configure this behavior as needed, for all or specific status changes.

Tip: This parameter is particularly relevant when using the **GetRealGroupName** hook. For details, see GetRealGroupName .

Configuration Parameter Name	Value
DoNotCopyOwnerToSubTicketsStatuses	**{"All":1}**. (Default) Determines that sub-requests never inherit the **owner** value from their parent request. **{"None":1}**. Determines that sub-requests always inherit the **owner** value from their parent request.

Configuring Sub-requests to Include Traffic for the Whole Change Request

By default, if a whole traffic line in a change request is not in a network map path that passes through the device, that traffic line will not be included in that device's sub-request. Furthermore, if NAT is taking place in some devices in the path, the IP addresses of the sub-request will change accordingly. If desired, you can configure FireFlow to include all traffic lines in all sub-requests.

Note: If the network map is inaccurate (paths are missing in), it is advised to disable the FIP algorithm in AFA. In this case, this feature will automatically be disabled and sub-requests will consequently include all traffic.

Configuration Parameter Name	Value
PerSubRequestTrafficDifferentiation	**0**. To configure sub-requests to include all traffic lines as is. **1**. To configure sub-requests to include only traffic lines in path and to modify their values according to NAT taking place in devices in the path. (Default)

Enabling/Disabling Sub-Request Traffic Modification

By default, FireFlow does not allow users to modify traffic specified in sub-requests. If desired, you can enable sub-request traffic modification.

Note: When traffic modification in sub-requests is enabled you may edit existing traffic lines in sub-requests. Addition and removal of traffic lines is never allowed.

Configuration Parameter Name	Value
`ModifySubTicketChangeTraffic`	**0**. To disable sub-request traffic modification. (Default) **1**. To enable sub-request traffic modification.

Configuring the Risk Check Method for Change Requests with Multiple Devices

In the Approve stage of a traffic change request's lifecycle, FireFlow performs a risk check, to determine whether implementing the change specified in the change request will introduce risks. The risk check is run on the device(s) specified in the change request, using the Risk Profile that the device was assigned when generating the last successful report in AFA.

When performing a risk check for a parent request with sub-requests, there are multiple devices and potentially multiple Risk Profiles involved. You can configure FireFlow to use any of the following risk check methods:

One

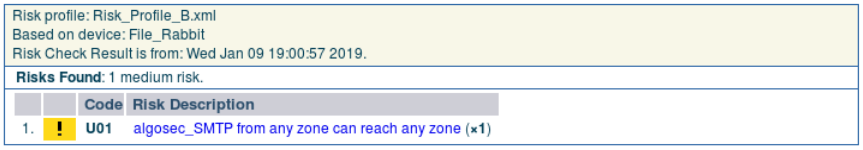
FireFlow runs the risk check on one random device out of all the sub-request devices.

For example, let us assume that there are three sub-requests, as follows:

Sub-request	Device	Risk Profile
500	Check Point A	r1
501	Check Point B	r2
502	Cisco C	r1

FireFlow will select a device at random (such as Cisco C) and run the risk check on it (using Risk Profile r1).

Only risk check results for the selected device will be displayed.

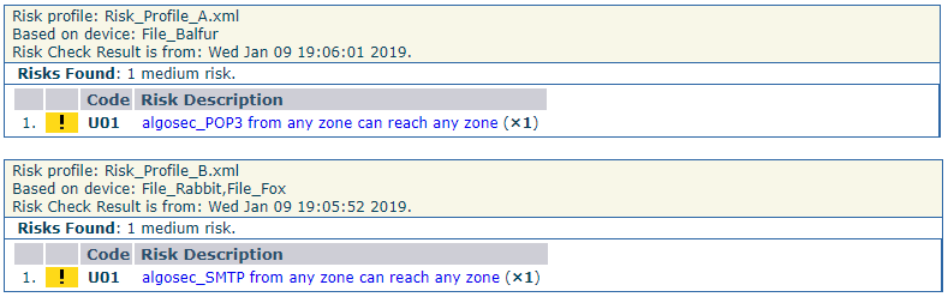


Profile

FireFlow runs the risk check on one random device per Risk Profile used by the sub-request devices.

In our example, there are two Risk Profiles, r1 and r2. FireFlow will select a device at random (either Check Point A or Cisco C) to run the risk check on using Risk Profile r1, and it will also run a risk check on Check Point B using Risk Profile r2.

Risk check results will be displayed per risk profile.



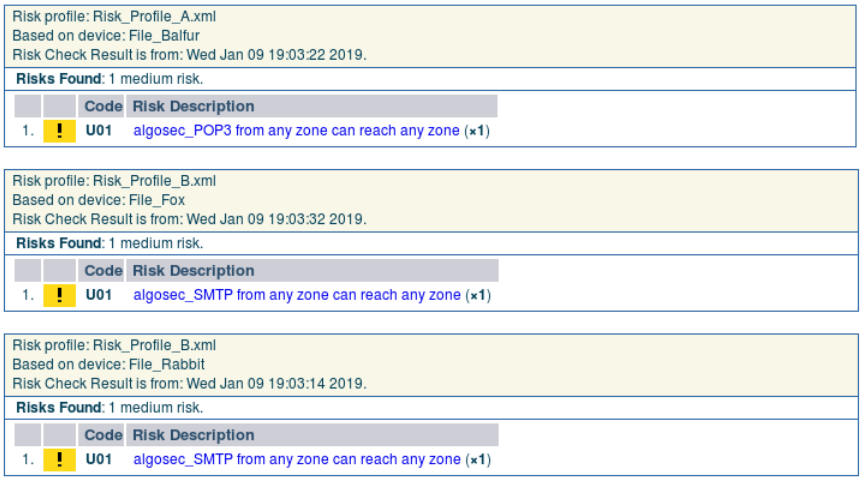
All

FireFlow runs the risk check on each of the sub-request devices.

In our example, FireFlow will run a risk check on Check Point A, Check Point B, and Check Point C, using their respective Risk Profiles.

Note that the risk check may take a while, and the results for each device may be similar.

Risk check results will be displayed for each device.



Configuration Parameter Name	Value
`RiskCheckOnParentTicket`	**one**. To use the One method. **profile**. To use the Profile method. (Default) **all**. To use the All method.

Finding affected rules parameters

Enabling/Disabling Cyan Highlighting in Finding Affected Rules Results

When deleting an object from a rule on a Check Point device, the object will be replaced with "any" if it was the only object for source, destination, or service for that rule. By default, cyan highlighting in the finding affected rules results indicates where an object slated to be deleted will be replaced by "any". If desired, you can disable this.

Configuration Parameter Name	Value
`HighlightRulesForDeletedObject`	**0**. To disable cyan highlighting in finding affected rules results. **1**. To enable cyan highlighting in finding affected rules results. (Default)

Enabling/Disabling Locating Objects by Scope When Finding Affected Rules

For Check Point devices, objects can be defined on the MDSM or on the CMA, so deleting an object may affect rules on devices other than the device in the current change request. By default, all devices that may have the object are analyzed when finding affected rules. If desired, you can disable this. When this feature is disabled, only the device specified in the object change request will be analyzed for affected rules.

Configuration Parameter Name	Value
`FindRulesByScope`	**0**. To disable locating objects by scope when finding affected rules. **1**. To enable locating objects by scope when finding affected rules. (Default)

Work order parameters

This section provides a reference of the work order configuration parameters available from the FireFlow ADVANCED CONFIGURATION area.

Configure work order creation for "No Action Required" change requests

In the Implement stage of a traffic change request lifecycle, FireFlow creates a work order consisting of a list of recommendations for implementing the requested change. If FireFlow detects that traffic is not routed through the device, then the work order states that no action is required.

In some cases involving Layer-2 devices, routing information may be missing, causing FireFlow to erroneously state that no action is required. You may therefore prefer to force FireFlow to create work orders suggesting a rule to add to the device policy, even when it has determined that no action is required.

Note: Such work orders will include a disclaimer stating the following: "Routing information might be missing. Recommendation could be incomplete."

Name	Value
ForceCreateWorkOrderForNA	0. To specify that work orders should state "No Action Required" when FireFlow detects that traffic is not routed through the device. (Default) 1. To force FireFlow to create work orders suggesting a rule to add to the device policy, even when FireFlow has determined that no action is required.

Configure work orders to include partially allowed and/or non-routed traffic

By default, if a traffic line in a change request to allow traffic is already partially allowed, or part of the traffic is not routed through the device, the work order will not include the allowed or not routed traffic because nothing needs to be implemented on the device for the sake of this traffic. In version 6.4 and below, the allowed and not routed traffic in a traffic line along with blocked traffic is included in the work order. If desired, you can configure FireFlow to include the not routed traffic or to include the not routed traffic and the partially allowed traffic in work orders.

Name	Value
ForceCreateWorkOrderForNAR	0. To configure work orders to include neither partially allowed traffic nor not routed traffic. (Default) 1. To configure work orders to include not routed traffic but not include partially allowed traffic. 2. To configure work orders to include not routed traffic and include partially allowed traffic. (Default for version 6.4 and earlier)

Configure work orders to include already allowed or blocked traffic

If a traffic line in a change request to allow traffic has already been allowed or blocked, the work order will not include the allowed or blocked traffic because nothing remains to be implemented on the device for this traffic. If desired, you can configure FireFlow to include the allowed traffic in work orders.

Name	Value
ForceCreateWorkOrderForAlreadyAllowed	**0**. To configure work orders not to include already allowed/blocked traffic (the work order will state: "no action required". (Default) **1**. To configure work orders to include already allowed/blocked traffic

Configure the network object translation method for work order creation

FireFlow provides two methods to perform network object translation: standard algorithms and a grep algorithm. When a large number of network objects are being used, translation is much faster when using the grep algorithm. The default threshold for using the grep algorithm is 500 network objects. If desired, you can change this threshold. In addition, you can disable the grep algorithm.

Name	Value
Min_Host_Groups_ Grep_Threshold	The desired threshold for number of network objects before using the grep algorithm. The default value is 500.
Min_Host_Groups_ Grep_Threshold	**0**. To enable the grep algorithm. (Default) **1**. To disable the grep algorithm

Configure work orders to include partially not-in-path traffic

By default, if part of a traffic line in a change request is not in a network map path that passes through the device, the work order will not include the not-in-path traffic because

nothng needs to be implemented on the device for the sake of this traffic. In version 6.7 and below, the not-in-path traffic in a traffic line along with blocked traffic is included in the work order. If desired, you can configure FireFlow to include the not-in-path traffic in work orders.

Note: If the network map is inaccurate (paths are missing), it is advised to disable the FIP algorithm in AFA. In this case, this feature will automatically be disabled, and work orders will include all traffic.

Name	Value
RemoveNotInPathAdressesInWorkOrder	**0**. To configure work orders to *not* remove not-in-path traffic. **1**. To configure work orders to remove not-in-path traffic. (Default)

Configure edit work orders to allow wider objects

By default, FireFlow allows editing a work order with objects that may contain more IP addresses than the original request, by using the **Wider Object** tab in the Advanced Editing Wizard. This allows you to add a subnet without having to re-plan the change request. Optionally, you can specify how wide of an object can be suggested.

If desired, you can disable this feautre, removing the **Wider Object** tab from the Advanced Editing Wizard.

Note: Allowing wider objects to be added to a work order may introduce risks, since the risk check will not be re-performed.

Name	Value
ShowWiderOption	**1**. To enable the **Wider Object** tab in the Advanced Editing Wizard. (Default) **0**. To disable the **Wider Object** tab in the Advanced Editing Wizard.

Name	Value

WiderObjectsSizeToSuggest	A copy of the default or current configuration, with the relevant modifications.
	Each element includes the following properties:
	• **requestedObjectSize**. The number of IP addresses in the originally requested object.
	• **maxWiderObjectSize**. The maximum number of IP addresses for any object that the Advanced Editing Wizard will suggest as a replacement for an object of the size specified in the **requestedObjectSize** property.
	Example:
	The following example does the following:
	• Changes the maximum allowed width of suggested objects for objects containing 100 IP addresses to 512 IP addresses (from 256)
	• Includes a new item that specifies that the maximum allowed width of suggested objects for objects containing 512 IP addresses is 1024 IP addresses.
	The change is highlighted.
	`[`
	` { "maxWiderObjectSize": 512,`
	`"requestedObjectSize": 100 },`
	`{ "maxWiderObjectSize": 1024,`
	`"requestedObjectSize": 512 },`
	`{ "maxWiderObjectSize": 65536,`
	`"requestedObjectSize": 256 },`
	`{ "maxWiderObjectSize": 16777216,`
	`"requestedObjectSize": 65536 }`
	`]`

Configure edit work orders to include object naming at external sites

If desired, you can configure FireFlow to support object naming at an external site as a part of editing a work order. When this feature is enabled, a "**...**" button will appear next to every editable object in the edit work order dialog box. Clicking this button will instigate the following sequence:

1. A new window opens, displaying the specified site and FireFlow sends the site a field ID.
2. The user generates the new object name at the external site.
3. The external site sends the object name and field ID back to FireFlow.
4. FireFlow updates the field with the generated object name.
5. When the user saves the work order, FireFlow saves the generated object name as a part of the work order.

Note: To enable this feature, aside from completing the following procedure, you must configure the external site to behave in the above specified manner.

Name	Value
UseExternalSiteToGenerateHostNames	**1**. To enable configuring FireFlow to support object creation at an external site as a part of editing a work order. **0**. To disable configuring FireFlow to support object creation at an external site as a part of editing a work order. (Default)
EditWorkOrderExternalSiteURL	The external site's URL. For example, **https://192.168.3.184/AFA/php/test/test.php**.

Configure edit work orders to allow empty fields

By default, empty fields are considered valid when editing a work order (partial Edit Work Orders can be saved). If desired, you can require that all fields are completed.

Name	Value
AllowEmptyFieldsInEditWorkOrder	**0**. To disable allowing empty fields when editing a work order. **1**. To enable allowing empty fields when editing a work order. (Default)

Automatically send work orders to implementation team

Sometimes, changes to devices are implemented by a group of people who have no access to the FireFlow system. In this case, you can configure FireFlow to automatically generate a work order in PDF format and send it to the implementation team via email, each time a work order is created.

To automatically send work orders to an implementation team

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. Enable generating work orders in PDF format, by doing the following:
    a. In the main menu, click **Advanced Configuration**.
    b. Click **Global**.
    c. Click **Scrips**.
    d. Click the **Show Disabled** link at the top right.
    e. Click **550 On completion of Create Work Order Create Summary PDF**.
    f. In the **Stage** field, select **TransactionCreate**.
    g. Click **Update**.
3. Enable automatic sending of emails with work orders in PDF format attached, by doing the following:

a. In the main menu, click **Advanced Configuration**.
b. Click **Global**.
c. Click **Scrips**.
d. Click the **Show Disabled** link at the top right.
e. Click **560 On completion of Create Work Order Notify Work Order Recipient**.
f. In the **Stage** field, select **TransactionCreate**.
g. Click **Update**.

4. To customize the email template used for sending work orders, do the following:
   a. In the main menu, click **Advanced Configuration**.
   b. Click **Global**.
   c. Click **Email Templates**.
   d. Click **Notify Work Order Summary**.
   e. Edit the email content as desired.
   f. Click **Update**.
5. Configure the email recipient, by doing one of the following:
   - When customizing the email template as described in the previous step, type the desired address in the **To** field.
   - Configure the following parameter:

Name	Value
WorkOrderRecipientEmail	The email address to which to send the work order.

Note: If you configure the recipient email address using both methods, the email template overrides the configuration parameter.

Configure inclusion of work details in flat tickets

By default, FireFlow does not include work order information in the XML of a change request (a *flat ticket*). If desired, you can change this.

Name	Value
IncludeWorkOrderInXML	**0**. To disable inclusion of work order information in flat tickets. (Default) **1**. To enable inclusion of work order information in flat tickets.

Configure work order suggestions for drop traffic change requests

For traffic change requests which include a "Drop" action, the default work order suggestion is to add a drop rule to the policy. If desired, you can configure FireFlow to instead suggest removing a rule in the policy which allows the traffic.

Name	Value
DropTrafficUsingDropRule	**0**. To configure work orders for drop traffic change requests to suggest removing an allow rule. **1**. To configure work orders for drop traffic change requests to suggest adding a drop rule. (Default).

Configure ACL exclusion for Cisco work orders

When calculating a work order for Cisco devices, FireFlow determines which ACLs should be updated. It is possible to configure FireFlow to exclude some ACLs based on regular expression matching of the ACL name. If an ACL is excluded, the check box next to it will appear unchecked when the user views the work order.

Note: ACLs can be excluded using more complex logic using the **ExcludeAcl** hook. See Using Hooks (see FireFlow hooks).

Name	Value
ExcludeACLsInWorkOrderByName	A regular expression matching the names (or part of the names) of the ACLS to exclude. ' '(empty string). To configure work orders to not exclude any ACLs. (Default) For example, to configure excluding all ACLs starting with 'mgmt' or 'global', case insensitive, set the configuration parameter to the following value: **gr!^\s*(mgmt|global)!i**

Configure work order results for F5 BIG-IP

For details, see Configuring Initial Plan Results for F5 BIG-IP.

Configure rule position control for Check Point devices

When adding a new rule to a Check Point device, FireFlow determines where the rule can be placed in the policy. In the work order, the **Before Rule** field indicates that the new rule must appear before a specific rule so that, for example, the traffic is not dropped before it reaches the relevant allowing rule.

By default, you cannot edit the value of the **Before Rule** field to a value below a blocking rule. This prevents you from compromising the security policy. If desired, you can enable this ability, allowing you to add a rule to the policy wherever you want. This control may be desirable when you want to add a rule under a specific section header.

Note: When this feature is enabled, it is possible to "break" the policy. For example, if you are adding a rule to allow traffic and you add it below a rule which drops the traffic, the traffic will still be dropped. FireFlow will not prevent you from adding the rule as you specify, and a warning appears indicating the issue.

Name	Value
SetBelowBlockingRule	**0**. To disable rule position control for Check Point devices. (Default) **1**. To enable rule position control for Check Point devices.

Configure rule position control for Palo Alto Panorama devices

When adding a new rule to a Palo Alto Panorama device, FireFlow determines whether the rule should be placed in the "pre" section or "post" section of the device group policy, so that policy is optimized. If desired, you can specify that every rule should always be placed in the "pre" section or "post" section.

Note: When FireFlow is configured to always place rules in the "post" section, it is possible that traffic could be dropped by the "pre" section or by the local rule base. If this is the case, the work order page will display the following warning: "Rules from higher level policies might override the requested traffic."

Name	Value
PanoramaDefaultPolicySection	**Pre**. To specify all rules should be added to the "pre" section of the device group policy. **Post**. To specify all rules should be added to the "post" section of the device group policy. **Calculated**. To specify FireFlow should determine the most efficient place for each rule. (Default)

Configure Check Point work orders to suggest rules only below a specified section

If desired, you can configure FireFlow work orders for Checkpoint devices to recommend new rules only below a certain section (for example, below stealth rules). FireFlow will search the section headers for the string, and only recommend new rules below the specified section.

Name	Value
EditRuleSectionHeader	A part of the section header text. For example, setting the value to **stealth** configures work orders to only recommend new rules below the section **stealth**.

Configure security and log forwarding profiles for panorama devices

FireFlow provides the ability to configure a default value for the following fields in all Panorama work orders:

- Security Profile
- Log Forwarding Profile

By default, these fields are empty.

Note: Regardless of whether you set default values for these fields, you can modify them by editing individual work orders.

Name	Value
PanoramaSecurityProfile	The desired default value for the security profile in all Panorama work orders. The default value is **none**.
PanoramaLogForwardingProfile	The desired default value for the log forwarding profile in all Panorama work orders. The default value is **none**.

Configure shared level object creation for panorama devices

By default, FireFlow will always recommend creating new objects for Panorama devices at the Device Group level. If desired, you can configure FireFlow to always recommend creating new objects at the Shared level.

Name	Value
PanoramaObjectsCreation	Where the work order should recommend creating new objects. One of the following: **Shared** • **Device Group** (Default)

Configure zone recommendations for Palo Alto and Fortinet devices

FireFlow determines the source and destination zones from the source and destination IP addresses in the change request. By default, FireFlow will not recommend a rule with multiple zones in the **source zone** or **destination zone** fields. If the change request requires a rule which includes sources from multiple zones (or destinations from multiple zones), the recommended rule will always specify "any" zone for the **source zone** and/or **destination zone** fields.

If desired, you can configure FireFlow to support accurate zone spanning recommendations for Palo Alto and Fortinet devices. The recommendation for the **source zone** and **destination zone** fields will always include only the specific relevant zone(s), and you will be able to remove recommended zones while editing the work order. You can optionally enable the ability to select additional zones (from the device's available zones) when editing a work order, even if they were not detected as relevant.

Alternatively, you can configure FireFlow to always recommend the "Global" zone for Fortinet Devices.

Note: Fortinet devices version 4.x and below do not support multiple values in the **source zone** and **destination zone** fields.

Name	Value
MultipleZonesRecommendation	**1**. To enable the ability to detect and recommend multiple, specific zones for Palo Alto and Fortinet devices. **0**. To disable the ability to detect multiple, specific zones. (Default)

Name	Value
SelectUndetectedZones	**1**. To enable the ability to select additional zones while editing work orders for Palo Alto and Fortinet Devices. (Only relevant when **MultipleZonesRecommendation** is enabled.) **0**. To disable the ability to select additional zones while editing work orders. (Default)
FortinetAlwaysRecommendGlobalZone	**false**. The recommended zones will be based on the IP address(es) in the change request. (Default) **true**. The recommended zone will always be "Global".

Configure the brands used in automatic selection

When a change request is opened for configured brands, FireFlow will first look for an object that matches the request exactly. If none is found, the narrowest existing object that satisfies the requirements will be automatically suggested.

In such cases, FireFlow also enables you to configure the brands available for selection.

Name	Value

MinimalWiderObjectAutoSelection	A JSON array that contains all the device brands you want to support when selecting a wider object in change requests.
	For example:
	`[`
	`"ciscoaci"`
	`]`
	Default: Empty

Configure drop traffic request recommendations

FireFlow's default recommendation for drop traffic requests when an existing **allow** rule is found that perfectly matches the traffic specified in the request is to remove the existing rule.

Some device types also support disabling the rule. For supporting device types, FireFlow administrators can define that work orders always recommend disabling the rule instead of removing it.

Name	Value
RemoveOrDisableRulesInTrafficFlow	Determines whether FireFlow recommends that you remove a perfectly matching rule or disable it, when a perfect **allow** rule match is found for a drop traffic request. Relevant only for CISCO ASA or Check Point device types that support disabling rules. **0** = Remove **1** = Disable Default = **0**

Note: Restart FireFlow after configuring this parameter.

Configure new filters on user or common tenant

The following configuration parameter enables FireFlow administrators to determine whether new Cisco ACI filters are created on the user tenant, or on the common tenant.

Name	Value
CiscoACICreateNewFiltersOnCommonTenant	Determine whether new Cisco ACI filters are created on the user tenant, or on the common tenant. **user** = (Default) Filters are created on the user tenant **common** = Filters are created on the common tenant

Note: Restart FireFlow after configuring this parameter.

ActiveChange parameters

Configure logging for rules created by ActiveChange for Check Point devices

By default, ActiveChange creates rules with logging enabled (the device will track the rule's activities in logs). If desired, you can configure ActiveChange to create rules without logging.

Configuration Parameter Name	Value
`DefaultTrackOption`	**Log** To configure ActiveChange to create rules with logging. (Default) **None** To configure ActiveChange to create rules without logging.

Configuring Logging for Rules Created by ActiveChange for Juniper SRX Devices

By default, ActiveChange creates rules with logging enabled (the device will track the rule's activities in logs), and the log will be set at both the session init and session close times. If desired, you can configure ActiveChange to create rules without logging or change when the activities of the rule are logged.

Configuration Parameter Name	Value
SRXActiveChangeDefaultAddLogToNewRule	**session-init**. To configure ActiveChange to create rules with logging and set the log at the session init time. **session-close**. To configure ActiveChange to create rules with logging and set the log at the session close time. **session-init-close**. To configure ActiveChange to create rules with logging and set the log at both the session init and session close times. (Default) **none**. To configure ActiveChange to create rules without logging.

Configuring Logging for Rules Created by ActiveChange for Cisco ASA Devices

By default, ActiveChange assigns new rules on Cisco firewalls their log levels in accordance with the following criteria:

- Rules with an **Allow** action are assigned the device's default log level.
- Rules with a **Drop** action are assigned the log level, **informational**.

If desired, you can customize the log levels for each of these rule types.

Supported log levels include **emergencies**, **alerts**, **alert**, **critical**, **errors**, **error**, **warnings**, **warning**, **notifications**, **notification**, **informational**, **debugging**, **disable**, and **default**.

Configuration Parameter Name	Value
CiscoLogLevelForAllow	The desired log level for rules with an **Allow** action. The default value is the device's default log level.
CiscoLogLevelForDrop	The desired log level for rules with a **Drop** action. The default value is **informational**.

Configuring Logging for Rules Created by ActiveChange for Cisco IOS Routers

By default, ActiveChange creates rules with logging enabled (the device will track the rule's activities in logs). If desired, you can configure ActiveChange to create rules without logging.

Configuration Parameter Name	Value
`IOSLogForAllow`	**0**. To configure ActiveChange to create allow rules without logging. **1**. To configure ActiveChange to create allow rules with logging. (Default)
`IOSLogForDrop`	**0**. To configure ActiveChange to create drop rules without logging. **1**. To configure ActiveChange to create drop rules with logging. (Default)

Configuring Logging for Rules Created by ActiveChange for Fortimanager Devices

By default, rules for Fortimanager devices are created with logging enabled in the following situations:

- For rules with an "allow" action, logging is enabled only for security events.
- For rules with a "drop" action, logging is always enabled.

If desired, you can customize the log levels for each of these rule types.

Configuration Parameter Name	Value
`FortinetLevelForAllow`	**no**. Rules with the action "allow" will be created with logging disabled. **security**. Rules with the action "allow" will only be created with logging enabled for security events. (Default) **all**. All rules with the action "allow" will be created with logging enabled.

Configuration Parameter Name	Value
`FortinetLogSessionsStartForAllow`	**0**. Logs for "allow" rules are generated when the session starts. **1**. Logs for "allow" rules are generated when the session ends. (Default) **Note:** This parameter is only relevant when `FortinetLevelForAllow` is set to `all`.
`FortinetLogCaptureForAllow`	**0**. Logging for "allow" rules does not capture packets. (Default) **1**. Logging for "allow" rules captures packets. **Note:** This parameter is only relevant when `FortinetLevelForAllow` is set to `all`.
`FortinetLogForDrop`	**0**. Rules with the action "drop" will be created with logging disabled. **1**. Rules with the action "drop" will be created with logging enabled. (Default)

Configuring Maximum Number Rules Generated from Cisco IOS Router Work Order

Due to the specifications of some versions of Cisco IOS Routers, FireFlow only creates rules for Cisco IOS Routers with a single IP or network in either source or destination of each rule. As a result, FireFlow will recommend creating multiple such rules for a single traffic line, splitting the source and destination addresses of the requests to single networks. Considering that each change request may have multiple lines, each line may have multiple networks, and the change request may also require rules for return traffic, one change request could necessitate a very large number of rules. Therefore, FireFlow limits the number of rules recommended per single change request for Cisco IOS routers.

Configuration Parameter Name	Value
IOSMaxNumberOfRules	The desired maximum number of rules. The default value is 5000.

Configuring Implementation Behavior for Cisco Firepower

By default, FireFlow will implement changes for Cisco Firepower devices on the policy, but not install the new policy on the devices. If desired, you can change this.

Configuration Parameter Name	Value
CiscoFirepowerActiveChangeInstallPolicy	**0**. To configure ActiveChange to save changes to the policy. (Default) **1**. To configure ActiveChange to save changes to the policy and install the policy on the devices.

Configuring Implementation Behavior for Palo Alto Panorama Devices

By default, FireFlow will implement changes for Panorama/Palo Alto devices on the policy, but not commit the changes to Panorama. If desired, you can change this.

Configuration Parameter Name	Value
PanoramaActiveChangeCommit	**None**. FireFlow saves the changes to the policy only. (Default) **Panorama**. FireFlow saves the changes to the policy and commits the changes to Panorama. **Full**. FireFlow saves the changes to the policy, commits the changes to Panorama, and commits the changes to the device groups.
PanoramaActiveChangeCommit	**All**.FireFlow saves and commits all pending changes from all users. (Default) **User**. FireFlow saves and commits only pending changes made by the current user.

Configuration Parameter Name	Value
`PanoramaActiveChangeCommit`	**All**. FireFlow saves and commits all pending changes from all sessions. (Default) **Session**. FireFlow save and commits only pending changes made during the current session.

Commiting is asynchronous, and may take 30 minutes or more to complete. FireFlow will continuously poll Panoroma for the status of the commit until it completes. By default, FireFlow will send a request every 1500 milliseconds, for a maximum of 120 times (30 minutes of polling). You can optionally customize the polling interval and the maximum number of polls in AlgoSec Firewall Analyzer.

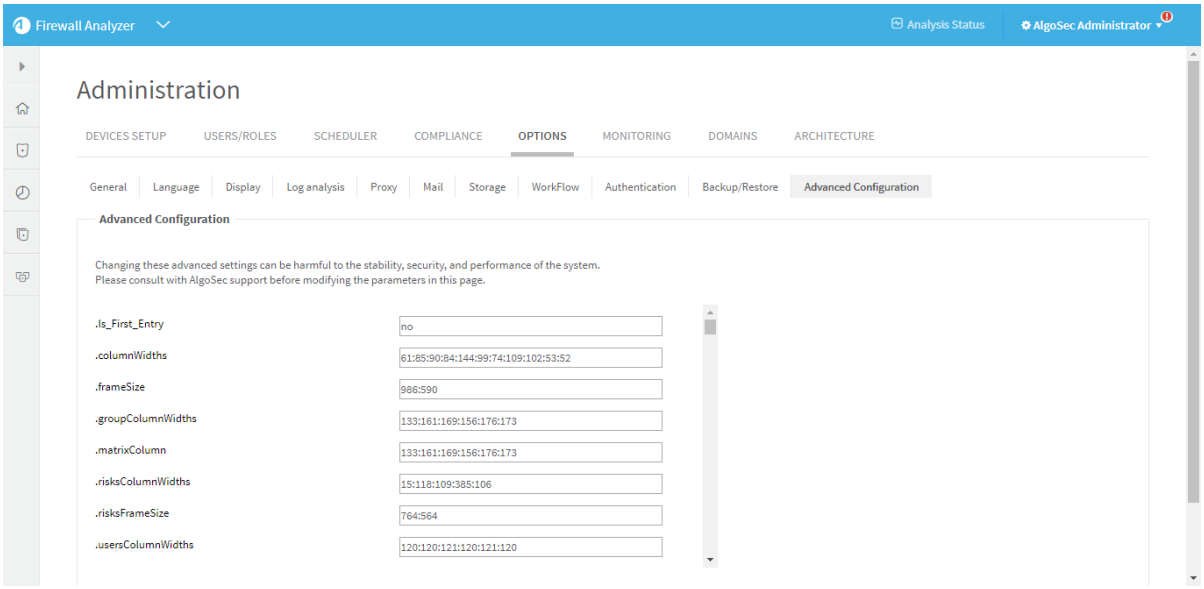
To customize polling

1. Switch to AFA.
2. In the toolbar, click your username.

   A drop-down list appears.
3. Select **Administration**.

   The **Administration** page appears, displaying the **Options** tab.
4. Click the **Advanced Configuration** tab.

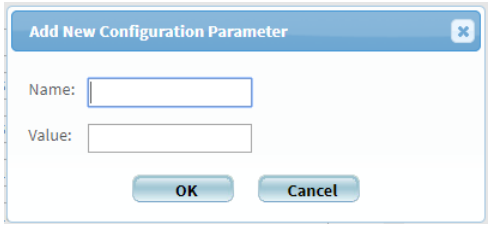
   The **Advanced Configuration** tab appears.



5. To customize the polling interval, do the following:

    a. Click **Add**.

    The **Add New Configuration Parameter** dialog box appears.



    b. In the **Name** field, `Active_Change_Commit_Poll_Interval`.

    c. In the **Value** field, type the desired interval in miliseconds.

    d. Click **OK**.

6. To customize the maximum number of polls, do the following:

    a. Click **Add**.

    The **Add New Configuration Parameter** dialog box appears.

    b. In the **Name** field, `Active_Change_Commit_Poll_Max_Tries`.

c. In the **Value** field, type the desired maximum number of polls.

d. Click **OK**.

7. Click **OK**.
8. Restart FireFlow. For details, see Restart FireFlow.

Configuring Implementation Behavior for Check Point Devices

By default, FireFlow will implement changes for Check Point devices on the policy and install the new policy on the devices. Additionally, FireFlow will re-assign the saved global policy to its managed entities (so that all lower level domains will be able to see the changes to the global policy).

If desired, you can change this. You can specify that FireFlow should only save the changes to the policy, but not install the new policy on the devices, or that FireFlow should still install the policy on the devices, but not re-assign the saved global policy to its managed entities.

Note: When re-assigning is enabled, the policy will only be re-assigned to management entities that exist in the AFA device tree.

To configure ActiveChange for Check Point R80 to install the new policy

Configuration Parameter Name	Value
`CheckPointActiveChangeInstallPolicy`	**0**. To disable installing the new policy. (Default) **1**. To enable installing the new policy.
`CheckPointActiveChangeReassign`	**None**. To not re-assign the saved policy to the managed entities. **Reassign**. To re-assign the saved policy to the managed entities. (Default)

To configure ActiveChange for Check Point device versions below R80 to install the new policy

1. Switch to AFA.
2. In the toolbar, click your username.

   A drop-down menu appears.
3. Select **Administration**.

   The **Administration** page appears, displaying the **Options** tab.
4. Click the **Advanced Configuration** tab.

   The **Advanced Configuration** page appears.
5. Click **Add**.

   The **Add New Configuration Parameter** dialog box appears.
6. In the **Name** field, type `CKP_ACTIVE_CHANGE_INSTALL_POLICY_ON_CHANGE`.
7. In the **Value** field, type one of the following:
   - Type `1` to enable installing the new policy.
   - Type `0` to disable installing the new policy. (Default)
8. Click **OK**.
9. Click **OK**.

Configure implementation behavior for FortiManager devices

By default, FireFlow will implement changes for FortiManager devices on the policy, but will not install the new policy on the devices.

You can change this as needed using the following parameter:

Configuration Parameter Name	Value
`FORTIMANAGER_ACTIVE_CHANGE_INSTALL`	**Save**. To save the current policy settings. (Default) **Install all**. Toinstall the new policy on the devices.

Configure ActiveChange for FortiManager to install the new policy

Do the following:

1. Switch to FireFlow.
2. Click the **Advanced Configuration** tab.

   The **Advanced Configuration** page appears.
3. Click **Add**.

   The **Add New Configuration Parameter** dialog box appears.
4. In the **Name** field, type `FORTIMANAGER_ACTIVE_CHANGE_INSTALL`.
5. In the **Value** field, type one of the following:
   - Type `Save` to save the current policy settings . (Default)
   - Type `Install all` to install the new policy settings on the devices.
6. Click **OK**.
7. Click **OK**.

Configure the maximum number of parallel device implementations

FireFlow offers the ability to implement on multiple devices simultaneously. By default, the maximum number of devices with which you can implement a policy change in parallel is 32. If desired, you can change this.

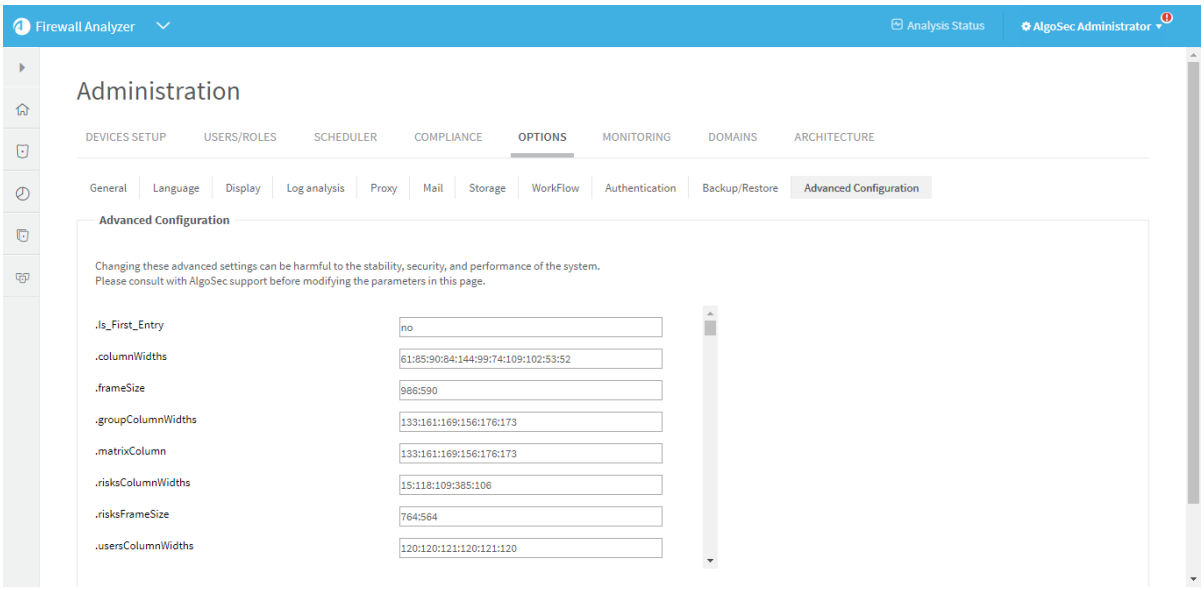
Do the following:

1. Switch to AFA. For details, see Logins and other basics.
2. In the toolbar, click your username.

   A drop-down list appears.
3. Select **Administration**.

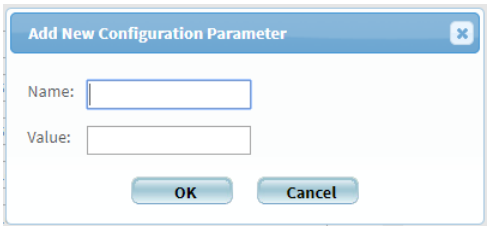
   The **Administration** page appears, displaying the **Options** tab.
4. Click the **Advanced Configuration** tab.

The **Advanced Configuration** tab appears.



5. Click **Add**.

   The **Add New Configuration Parameter** dialog box appears.



6. In the **Name** field, type `MULTI_PUSH_MAX_PARALLEL`.
7. In the **Value** field, type the number of device implementations that should be permitted to be executed in parallel.
8. Click **OK**, and then click **OK** again.
9. Restart Apache Tomcat, by doing the following:
   a. Log in to the FireFlow server using the username "root" and the related password.

b. Run the following command:

c. **service apache-tomcat restart**

Apache Tomcat is restarted.

10.

Configuring a Custom Rollback Notification for ActiveChange

FireFlow provides a rollback feature when implementation on a device fails. It is possible that a failure could occur where FireFlow has no ability to rollback the changes. If desired, you can create a custom notification with rollback instructions.

To configure a custom rollback notification for ActiveChange

- Create an html file with the desired notification, name it *<device brand name>***RecoveryProcedure.html**, and save it to `/usr/share/fireflow/local/etc/site/RecoveryProcedures`.

Example file names

- For a **Cisco ASA** - Cisco_AsaRecoveryProcedure.html
- For a **CIsco router** - Cisco_RouterRecoveryProcedure.html
- For a **Juniper SRX** - JunosRecoveryProcedure.html
- For a **Panorama** - PanoramaRecoveryProcedure.html

Enabling VMWare NSX ActiveChange Rollback

In order to allow rollback for VMWare NSX ActiveChange, it is mandatory to enable the NSX auto configuration draft save feature. If this feature is disabled, no drafts will be saved.

If this feature is disabled and you want to enable auto save on the NSX, run the following PUT request with the appropriate Basic authorization:

```
PUT /api/4.0/firewall/config/globalconfiguration
Content-Type: application/xml
<?xml version="1.0" encoding="UTF-8"?>
<globalConfiguration>
```

```
    <autoDraftDisabled>false</autoDraftDisabled>
</globalConfiguration>
```

Response example:

```
Success
```

If you want to keep this feature disabled, but still to allow the ActiveChange functionality (without being able to rollback to previous configurations (not recommended)), use the following method:

In the file `data/algosec-ms/config/ms-devicemanager-prod.properties`, modify the threshold for last draft age parameter:
`devicedriver.nsx.backupDraftAgeThresholdDays`

Note: If the age of the last draft is more than this value, implementation will be aborted.

The default value is 1 day.

To override it, use the following:

```
devicedriver.nsx.backupDraftAgeThresholdDays=30
```

Change validation parameters

Configuring Advanced Change Validation Strictness

When FireFlow performs advanced change validation, and the work order/ policy comparison determines a rule is a perfect match or more permissive, the change validation additionally verifies whether all object names used in the work order recommendation's fields are the objects used in the matched rule's fields. By default, a discrepancy in object names will not cause validation to fail. If desired, you can change this. Also, you can disable work order/ policy comparison altogether, leaving change validation to only consist of traffic simulation queries.

Configuration Parameter Name	Value
`ChangeRequestValidateObjectNames`	**0**. To set validation to pass when there is an object name discrepancy. (Default) **1**. To set validation to fail when there is an object name discrepancy. **2**. To disable work order/ policy comparison altogether.

Configuring the Change Validation Timeout Period

When a change request enters the **Validate** stage, FireFlow attempts to verify that the changes in the work order have been implemented correctly. FireFlow can only detect the change once the device is analyzed or monitored by AFA, after the change is made.

In an environment with scheduled monitoring, the default timeout period is set to the same period as the monitoring cycle. If FireFlow fails to retrieve the monitoring frequency, the timeout period is set to 15 minutes (the default monitoring frequency). Manually analyzing the device in AFA will not cause change validation to proceed. If a monitoring cycle does not occur in this period, Change validation could not be run, please recalculate appears.

In an environment without scheduled monitoring, the default timeout period is 24 hours. If the device is not manually analyzed in AFA during that time, Change validation could not be run, please recalculate appears.

If desired, you can customize the timeout period (for both monitoring and non-monitoring environments).

Configuration Parameter Name	Value
`AsyncValidationTimeout`	The desired timeout period, in seconds. The default value is 0, which causes the default behaviors described above.

Configuring Change Validation Results for F5 BIG-IP

See Configuring Initial Plan Results for F5 BIG-IP.

FireFlow logging parameters

Enabling/Disabling Debug Mode

When Debug mode is enabled, additional debug-oriented information is available in log files. Debug information will then be available to FireFlow support in a zip file of logs you can download. For details, see FireFlow troubleshooting.

Note: You must disable Debug mode once a problematic scenario has been recreated and the support zip file submitted. Leaving Debug mode enabled can affect general performance, and you will lose log history faster (days instead of weeks).

Note: You can optionally enable and disable Debug mode in the web interface. For details, see FireFlow troubleshooting.

Configuration Parameter Name	Value
`LogToFile`	**debug**. To enable Debug mode. **info**. To disable Debug mode. (Default)
`LogMaxMsgLen`	**5000**. To enable Debug mode. **300**. To disable Debug mode. (Default)

Note: After configuring these parameters, wait for approximately 5 minutes for this change to take effect. You do not need to restart Apache.

Enabling/Disabling Logging of User Permissions

If desired, you can enable logging for user permissions checking. The log will include a line every time user permissions are checked for field, change request, or system permissions. The line will include the requested permission and whether the user has the permission.

Note: These lines will appear once per unique rights request.

Configuration Parameter Name	Value
`LogPermissions`	0. To disable user permissions logging. (Default) 1. To enable user permissions logging only if the URL contains the parameter `LogPermissions=1`. 2. To enable permissions logging every time a user's permissions are checked.

Additional FireFlow parameters

This section describes how to perform various FireFlow options using FireFlow configuration parameters.

Configure how long AFA data is stored in FireFlow cache

FireFlow stores various AFA data in cache for various lengths of time. If desired, you can change how long the data is stored, by using the following procedure.

Note: Any configuration with the obsolete configuration parameter, `FirewallObjectRefreshTime`, needs to be reconfigured.

Configuration Parameter Name	Value
FAServerCmdCacheLifeTimeInSeconds	A copy of the default or current configuration, with the times modified as desired. The times are configured in seconds . See the example below for details. The default configuration for is as follows: `{ "CHECK_IF_DOMAINS_USED": 86400, "CHECK_REPORTS_BRANDS": 600, "FIREFLOW_APPLICATIONS_LIST": 86400, "FIREFLOW_FIND_LAST_REPORT_INFORMATION": 600, "FIREFLOW_FIND_LAST_REPORT_NAME": 600, "FIREFLOW_GET_GENERIC_DEVICES_BRAND": 86400, "FIREFLOW_GET_HOSTGROUPS_DEFINITION": 1200, "FIREFLOW_GET_MULTIPLE_PROTOCOL_SERVICES": 86400, "FIREFLOW_GET_SERVICE_OBJECTS_DEFINITION": 1200 }` **Example:** The following value configures the amount of time that the device objects listis stored in cache to 3 minutes (180 seconds). The change appears in bold. `{ "CHECK_IF_DOMAINS_USED": 86400, "CHECK_REPORTS_BRANDS": 600, "FIREFLOW_APPLICATIONS_LIST": 86400, "FIREFLOW_FIND_LAST_REPORT_INFORMATION": 600, "FIREFLOW_FIND_LAST_REPORT_NAME": 600, "FIREFLOW_GET_GENERIC_DEVICES_BRAND": 86400,` `"FIREFLOW_GET_HOSTGROUPS_DEFINITION":` **180**, `"FIREFLOW_GET_MULTIPLE_PROTOCOL_SERVICES": 86400, "FIREFLOW_GET_SERVICE_OBJECTS_DEFINITION": 1200 }` **Note:** For further information regarding the various time values listed above and best practices for modifying them, contact AlgoSec.

Configure queries on Juniper NSM devices to run on saved policies

By default, AFA runs all queries on the policy installed on the Netscreen device. If desired, you can configure queries to be run on the policy saved on the NSM. This enables you to validate a change was made correctly after implementing it on the NSM, but before installing it on the Netscreen device.

This configuration affects all queries in AFA. For FireFlow, this affects initial planning, work order creation, and change validation.

Note: Only new queries are executed against the saved policy. In order to query the new AFA saved policy for existing queries, re-execute the initial plans, work orders, and validations.

Configuration Parameter Name	Value
`run_collect_nsm_upon_policy_save`	**yes**. To configure queries on NSM managed devices to run on the saved policy.

Configure FireFlow to skip validation for suggested address objects

If desired, you can improve restart performance by bypassing the validation of the structure and consistency of the `SuggestedAddressObjects_Config.xml` file.

Although it is recommended to validate the consistency of the `SuggestedAddressObjects` file, in extreme cases where this file is significantly large, you may consider skipping the validation.

Configuration Parameter Name	Value
`SkipSuggestedAddressObjectsSchemeValidation`	**0**. To enable validation of the `SuggestedAddressObjects_Config.xml` file. (Default) **1**. To skip validation of the `SuggestedAddressObjects_Config.xml` file.

Customize the landing page

After logging into the *AlgoSec Security Management Suite* Firewall Analyzer or FireFlow will appear. See below for the default landing page for each user. For administrators, privileged users, and roles, you can override the default behavior by defining a landing page per user/role. For unprivileged users (requestors), you can override the default behavior by defining a landing page for all unprivileged users.

The landing page appears, according to the following precedence:

- **If a landing page is defined for the user**, that landing page will appear.
- **If no landing page is defined for the user**, but a landing page is defined for one of the user's roles, that landing page will appear.
- **If no landing page is defined for the use**r, and the user has multiple roles with different landing pages defined, the landing page is defined as FireFlow, and then AFA.
- **If no landing page is defined for the user or any of the user's roles**, the following occurs:

For administrators	AlgoSec Firewall Analyzer appears.
For privileged (AFA) users	The following occurs: • If FireFlow is licensed and activated, FireFlow appears. • Otherwise, the default AlgoSec Firewall Analyzer page appears.
For unprivileged users (requestors)	The following occurs: • If AppViz is licensed, activated, and has at least five applications, AppViz appears. • Otherwise, FireFlow appears.

Note: Only administrators and privileged (AFA) users can define landing pages. Administrators can define landing pages for themselves and others, while privileged

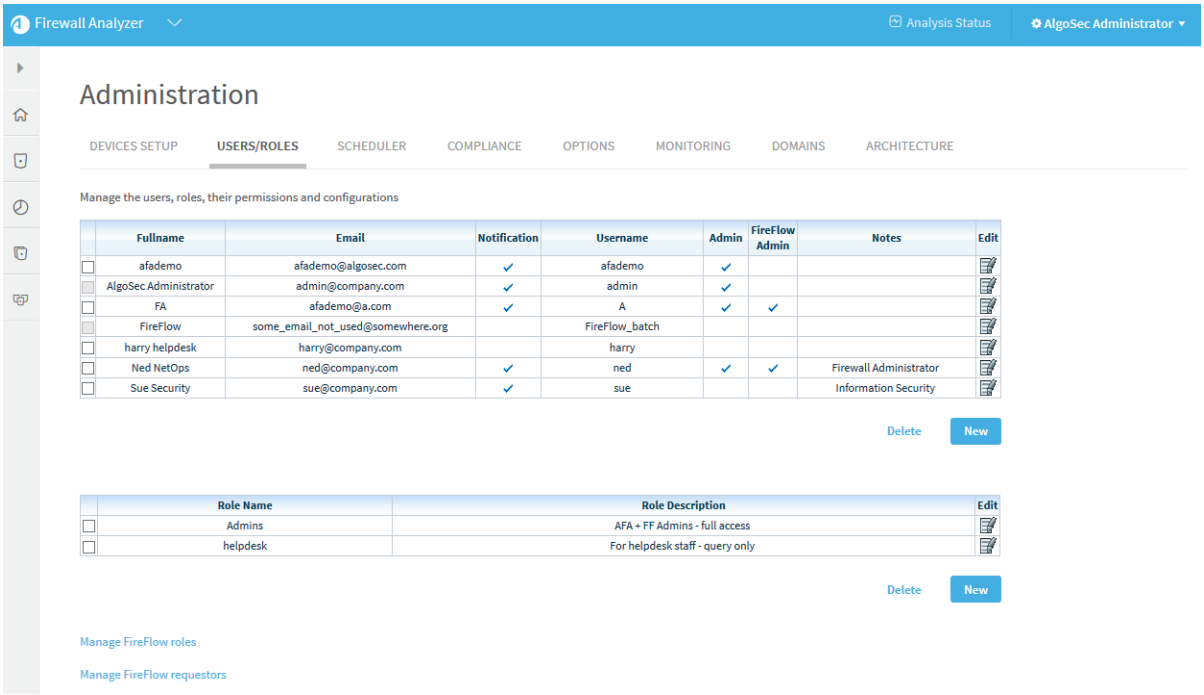
users can only define landing pages for themselves. The procedures listed below can only be performed by administrators.

To define a landing page for an administrator, privileged user, or role

1. Switch to AFA. For details, see Logins and other basics.
2. In the toolbar, click your username.
3. A drop-down menu appears.
4. Select **Administration**.

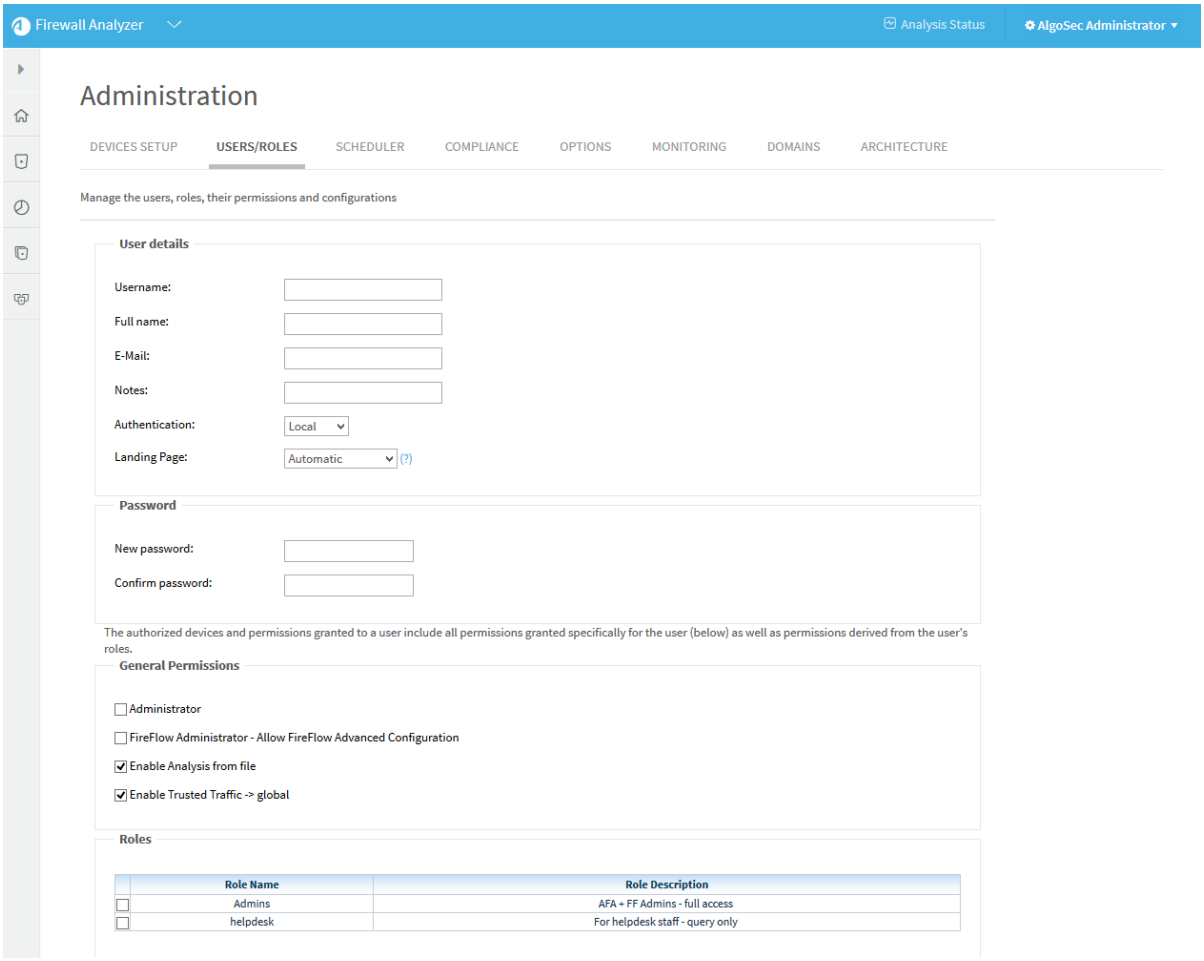
   The **Administration** page appears displaying the **Options** tab.
5. Click the **Users/Roles** tab.

   The **User and Role Management** page appears.



6. Click ✎ in the row of the desired user or role.

   New fields appear.



7. In the **User** or **Role details** area, in the **Landing page** drop-down menu, select the desired landing page.
8. Click **OK**.

To define a landing page for all unprivileged users (requestors)

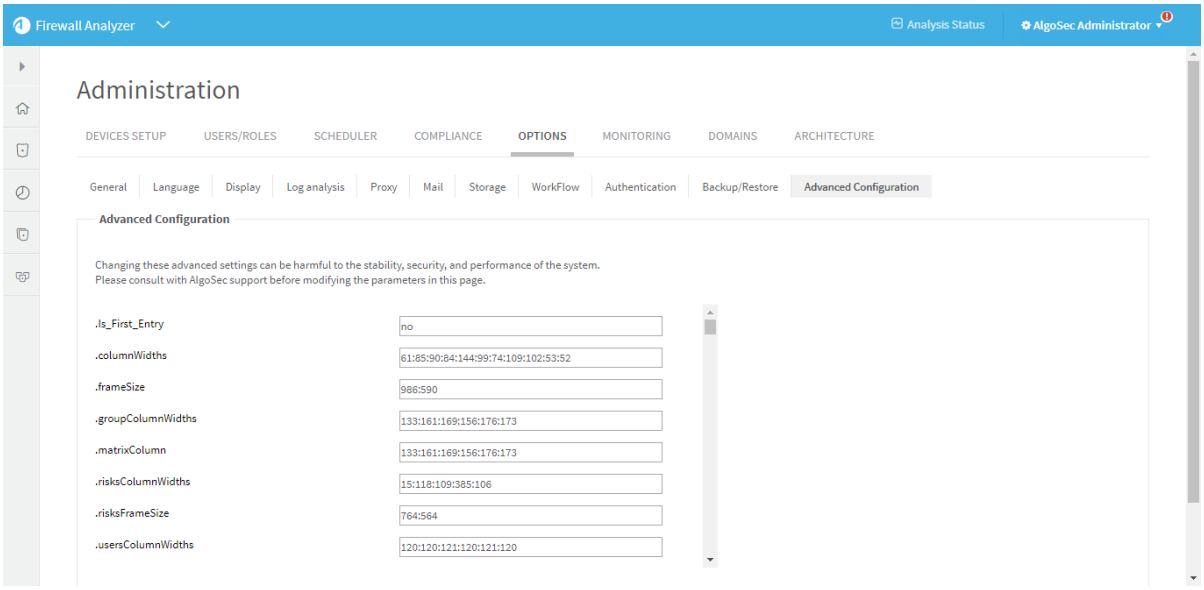
1. Switch to AFA. For details, see Logins and other basics.
2. In the toolbar, click your username.

   A drop-down menu appears.
3. Select **Administration**.

   The **Administration** page appears displaying the **Options** tab.

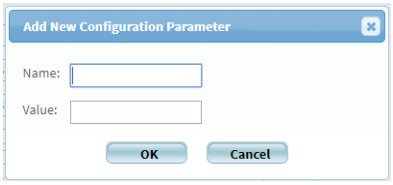
4. Click the **Advanced Configuration** sub-tab.

   The **Advanced Configuration** sub-tab appears.



5. Click **Add**.

   The **Add New Configuration Parameter** dialog box appears.



6. In the **Name** field, enter **FireFlow_Requestors_Landing_Page**.
7. In the **Value** field, enter **aff**. This sets the landing page for all unprivileged users to FireFlow.
8. Click **OK**.

Configure the maximum number of rules in a rule removal request

By default, 50 is the maximum number of rules you can add to a rule removal change request. If desired you can change this.

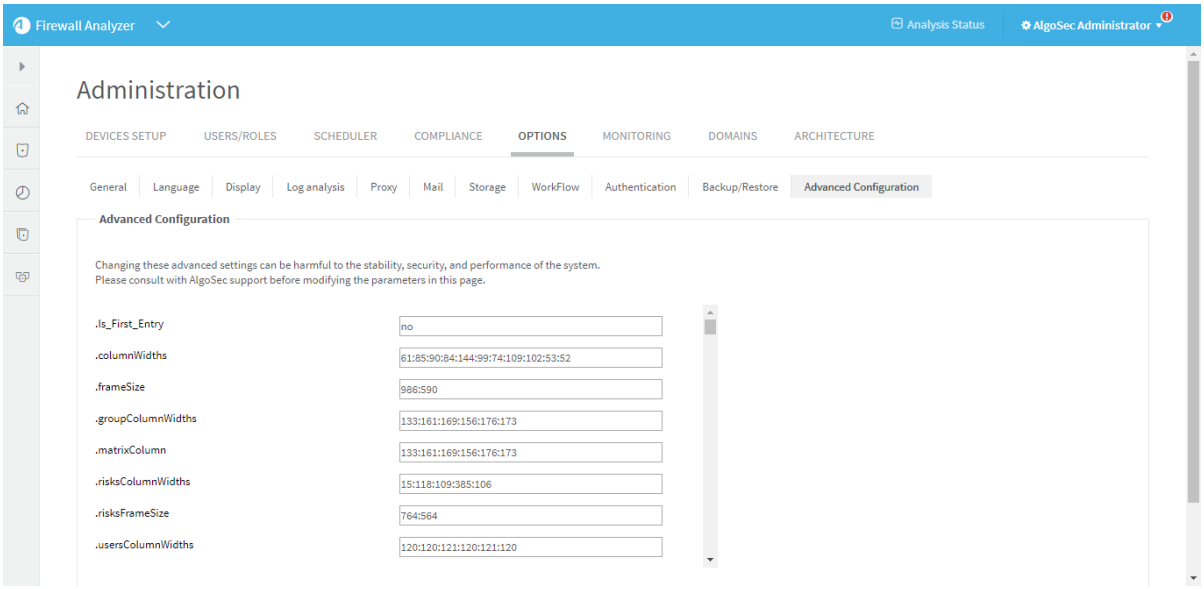
To configure the maximum number of rules in a rule removal request

1. Switch to AFA. For details, see Logins and other basics.
2. In the toolbar, click your username.

   A drop-down menu appears.
3. Select **Administration**.

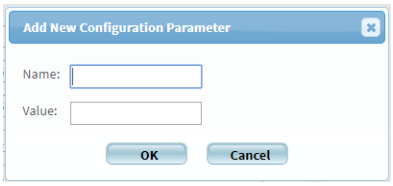
   The **Administration** page appears displaying the **Options** tab.
4. Click the **Advanced Configuration** sub-tab.

   The **Advanced Configuration** sub-tab appears.



5. Click **Add**.

   The **Add New Configuration Parameter** dialog box appears.



6. In the *Name* field, type **Rule_Selection_Limit**.
7. In the *Value* field, type the maximum number of rules.

> **Note:** The maximum recommended value is **300**. More rules than this in a single change request will severly impact performance.

8. Click **OK**.

Configure automatic approval of minor rule changes

By default, FireFlow displays any device policy rule changes in the **Auto Matching** page and attempts to match them to resolved change requests. This includes minor policy rule changes, such as enabling rule logging or updating a rule name. You can optionally configure FireFlow to automatically approve minor policy rule changes. These minor changes will then appear in the **Auto Matching** page in the **Changes Without Request - Approved** sub-list, without referring to a specific change request.

Configuration Parameter Name	Value
`IgnoreRuleFieldsInReconciliation`	A space-separated list of device policy rule fields, for which changes should be automatically approved. The supported policy rule fields are as follows: **FirewallName**, **FirewallRuleNum**, **Name**, **Comment**, **Source**, **Destination**, **Service**, **SourceExpanded**, **DestinationExpanded**, **ServiceExpanded**, **Action**, **Enable**, **Track**, **Time**, **Install**, **Vpn**, **FromZone**, **ToZone**, **ACL**, **Interface**, **SourceNat**, and **DestinationNat**. **Note: SourceExpanded**, **DestinationExpanded**, and **ServiceExpanded** are the IP addresses (and protocol/ports) represented by the rule's object names. Therefore, for example, when adding Source to the value, changes in a rule's source object names will be approved automatically, while changes to the actual source IP addresses will not. **[]** (an empty list). To specify that no changes should be automatically approved. For example, the following value configures FireFlow to automatically approve changes to rules that involve logging and/or comments only: [Track Comment]

Customize the FireFlow risk check

The FireFlow default traffic change request lifecycle includes the Approve stage, in which a risk check is performed to determine whether implementing the change specified in a change request would introduce risks. The risk check is based on device analyses produced by AlgoSec Firewall Analyzer (AFA), a comprehensive device analysis solution that is a companion product of FireFlow.

It is possible to customize the FireFlow risk check, by configuring AFA to treat certain types of traffic as non-threatening *trusted traffic* when it produces the devices analyses. This enables you to eliminate false-alarms triggered by traffic that is necessary for the organization. In addition, you can create Risk Profiles that specify the severity level of individual risks. FireFlow risk check will then use your custom Risk Profiles to detect risks of your preferred risk level classification.

Manage FireFlow users and roles

This section describes how to manage users and roles in FireFlow.

Manage FireFlow Users and Roles: Watch to learn about setting FireFlow permissions per role and user.

FireFlow users and roles

The FireFlow change request lifecycle involves multiple users, each of which is assigned one or more of the following roles:

Requestor	Users with this role can send requests to the FireFlow system asking for a device change to be made. For example, a requestor who only has access to the company DMZ might request access from their computer to an internal LAN. **Note:** Requestors cannot be assigned additional roles.
Network operations	Users with this role are responsible for processing the requestor's request, determining which device changes are required to meet the request, planning how to implement the necessary changes, and implementing the changes.
Information Security	Users with this role are responsible for determining whether the requested changes pose any risk, approving those changes, and performing auditing to ensure that all change requests are matched with implemented changes.
FireFlow Administrator	Users with this role can configure the FireFlow system and manage devices, groups of devices, and users in the system.
Read-Only	Users with this role can view the FireFlow interface, but cannot modify its contents or settings.
Controller	Users with this role are responsible for a second round of change request approval, called a review. This role is optional and used only in the Multi-Approval and Parallel-Approval workflows.

If necessary, additional roles can be defined.

Users with roles other than "requestor" are called *privileged users*.

User management procedures

The method used to add a user differs depending on which FireFlow role you intend to assign the user (and consequently, which actions the user has permission to perform). You can add, edit, and delete users as needed.

- Administrator and other privileged users are managed in AFA. For details, see Manage privileged users.
- Requestors are managed in FireFlow, either in the Web interface or directly in the Requestor Database. They are automatically assigned the requestor role. For details, see Manage requestors.

  Note: Adding requestors is only required if you want to allow use of the Requestors Web Interface.

Additionally, ASMS provides the ability to authenticate users (as well as manage users and roles) using an authentication server or single sign on.

Manage privileged users

Relevant for: Administrators

This topic describes how to manage FireFlow administrators and other privileged users. These users are managed in the AFA Administration area.

Administrators and other privileged users are managed in AFA.

Note: If ASMS is configured to authenticate users with an authentication server or Single Sign On, user credentials are not managed locally.

Add and edit privileged users

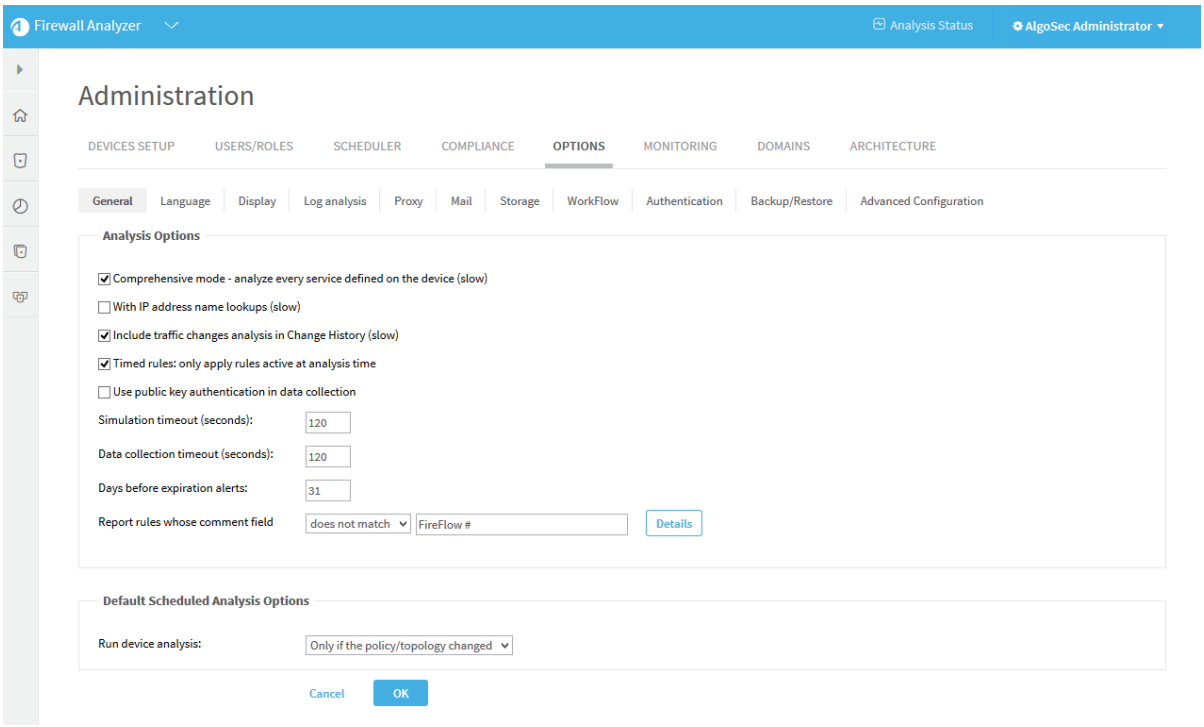
Note: It is possible to import users from a CSV file.

Do the following:

1. Switch to AFA.
2. In the toolbar, click your username.

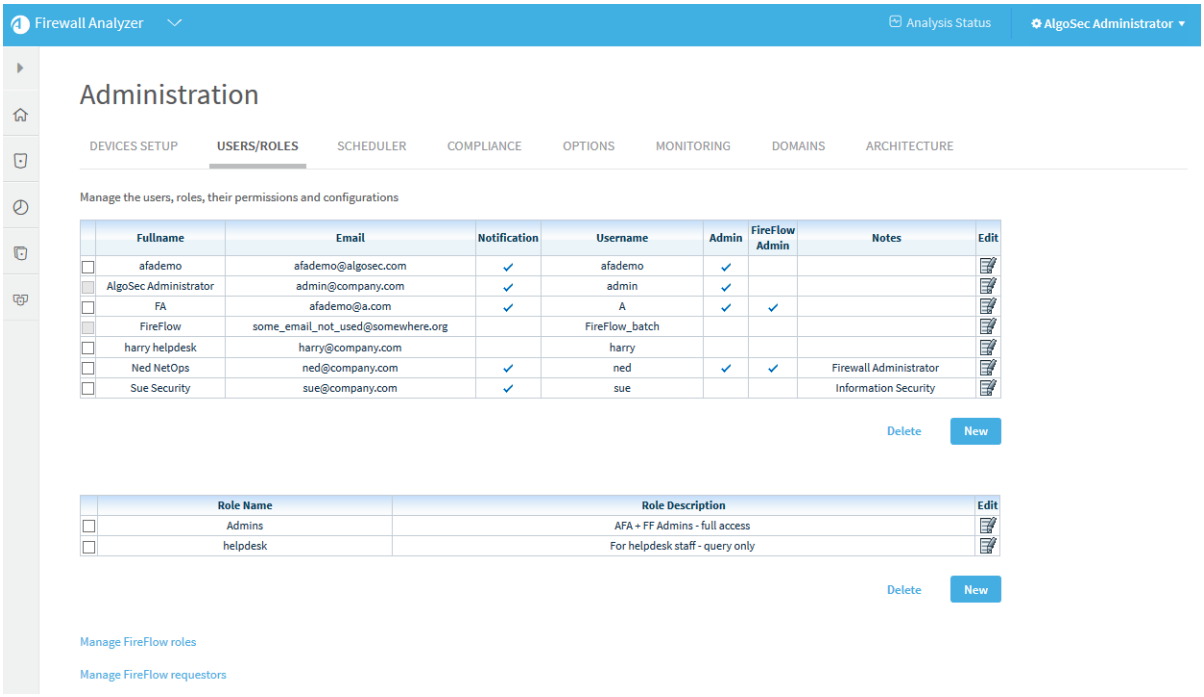
   A drop-down menu appears.
3. Select **Administration**.

   The **Administration** page appears, displaying the **Options** tab.



4. In the **Options** tab, click the **Users/Roles** sub-tab.

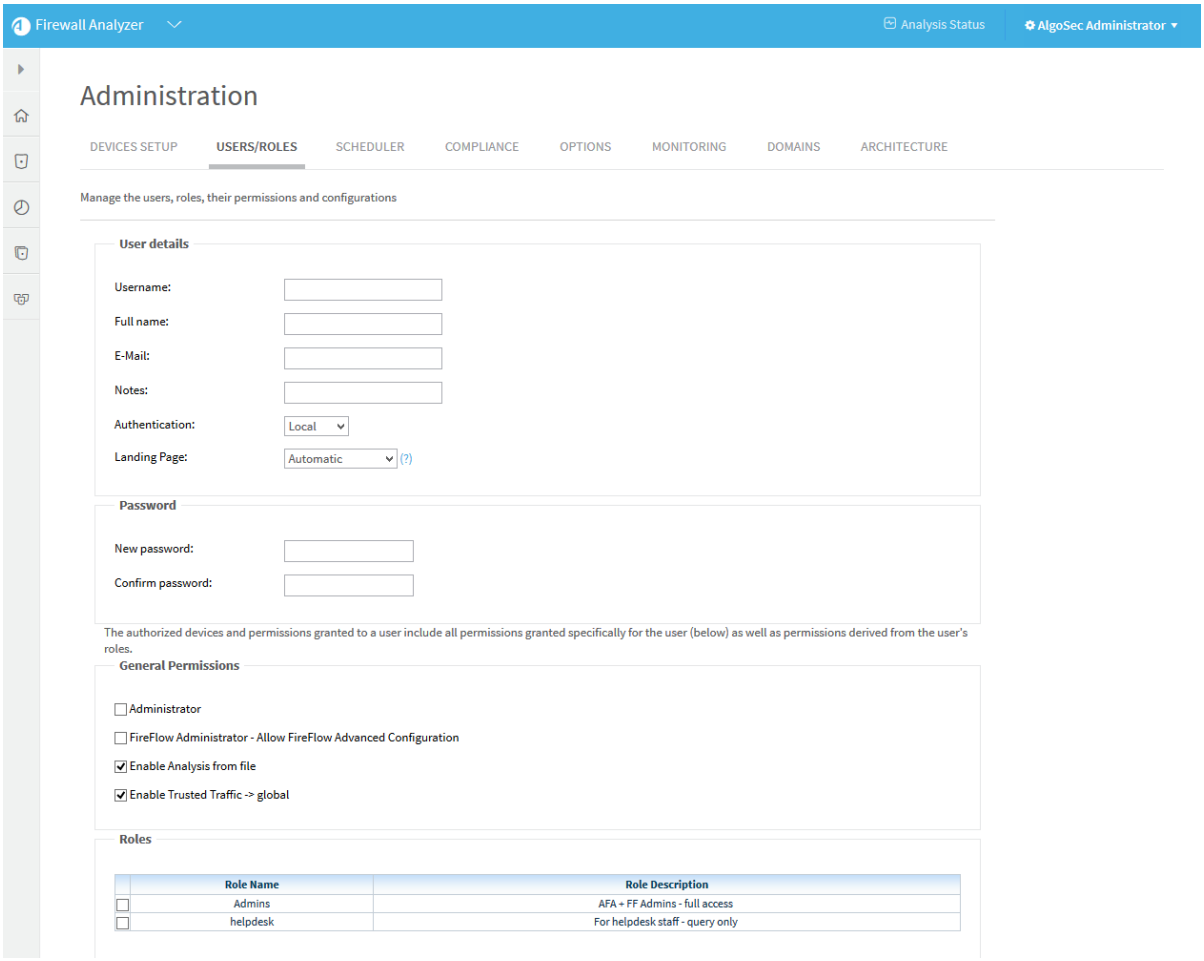
   The **User and Role Management** page appears.



5. Do one of the following:

   - To add a new user, under the list of users, click **New**.
   - To edit an existing user, click in the desired user's row.

   New fields appear.



6. Complete the fields as need. For details, see User field reference.

   Note: In order to enable the user to perform configuration and advanced configuration tasks, such as using VisualFlow to edit workflows, you must select the **FireFlow Administrator - Allow FireFlow Advanced Configuration** option.

7. In the **Roles** area, select the AFA roles to assign the user.

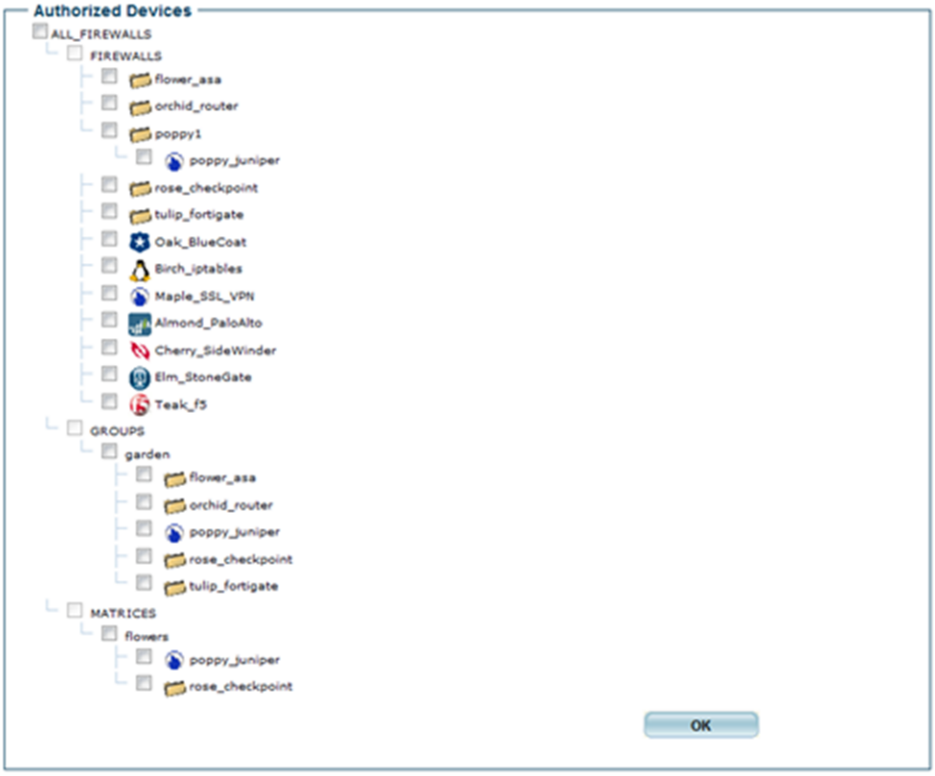
   An AFA role represents a set of permissions and access levels in AFA, and when a user is assigned a role, the user is automatically granted the permissions specified for the role.

Note: You can assign additional permissions to this user, as desired. The user will then have both the permissions inherited from their roles, as well as the permissions assigned specifically to the user.

8. Specify the devices and groups that the user should be able to view, by doing the following in the **Authorized Devices** area:

    a. Click **Select devices**.

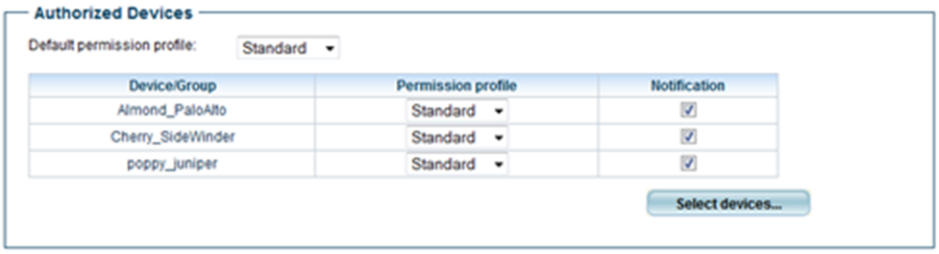
    A tree of all the devices and groups appear.



    b. Choose the desired devices and groups.

    c. Click **OK**.

    The selected devices and groups are listed in the **Authorized Devices** area. Each device or group is assigned the access level specified in the default permission profile.



d. To change the access level for a device or group, in the device or group's **Permission profile** drop-down list, select the desired access level.

e. To specify that AFA should send e-mail notifications regarding a device or group, select the device or group's **Notification** check box.

9. Click **OK**.

The user is added to ASMS.

Note: If you are adding a network operations or security information user, you must now assign the user the relevant role. If you assigned the user administrative permissions (by selecting the **Administrator** check box), the system automatically assigns the user both roles, and there is no need for further configuration.

For more details, see Manage user roles.

User field reference

The following fields are used to define FireFlow users.

In this field...	Do this...
User details	
Username	Type a username for the user. Usernames can contain any alpha-numeric character and the following special characters: "@", "_", ".", or "-".
Full name	Type the user's full name.
E-Mail	Type the user's e-mail address.

In this field...	Do this...
Notes	Type any notes about the user.
Authentication	Select how to authenticate this user: • **Local.** Authenticate the user against the local ASMS user database. • **RADIUS.** Authenticate the user against a RADIUS server. • **LDAP**. Select this option to enable user authentication against an LDAP server.
Landing Page	Select one of the three products, or **Automatic**. For more information, see Customizing the Landing Page.
Password	
New password	Type a password for the user. Passwords can contain any alpha-numeric character or any special character, excluding back ticks (`).
Confirm password	Re-type the password you entered in the **New password** field.
General Permissions	
Administrator	Select this option to make the user an administrator.
FireFlow Administrator - Allow FireFlow Advanced Configuration	Select this option to make the user a FireFlow configuration administrator. This enables the user to perform advanced configuration tasks in FireFlow.
Enable Analysis from file	Select this option to allow the user to perform analyses from configuration files.
Enable Trusted Traffic -> global	Select this option to allow the user to view trusted traffic.

In this field...	Do this...
Roles	
	Select the user roles to assign the user. The user will automatically be granted the permissions specified in the assigned roles. **Note:** You can assign additional permissions to this user, as desired. The user will then have both the permissions inherited from their roles, as well as the permissions assigned specifically to this user.
E-mail Notifications	
Changes in risks	Select this option to specify that the AFA system should send notifications to the user when there are changes in risks.
Changes in policy	Select this option to specify that the AFA system should send notifications to the user when changes are made to policies.
Every group report	Select this option to specify that the AFA system should send notifications to the user when a group report is generated.
Every report	Select this option to specify that the AFA system should send notifications to the user when a report is generated.
Every configuration change	Select this option to specify that the AFA system should send notifications to the user when configuration changes are made.
Rules and VPN Users about to expire	Select this option to specify that the AFA system should send notifications to the user when device rules and/or VPN users are about to expire. To configure the number of days before rule or VPN user expiration that AFA should send a notification, complete the **Days before expiration alerts** field in the **General** sub-tab of the **Options** tab in the Administration area. See Setting AlgoSec Firewall Analyzer Preferences.

In this field...	Do this...
Error messages	Select this option to specify that the AFA system should send error messages to the user. These include low disk space and license expiration warnings. This field is only relevant for administrators.
Changes in customization	Select this option to specify that the AFA system should send notifications to the user when customization changes are made. These include notifications about topology, trusted traffic, and risk profile customizations. This field is only relevant for administrators.
Hide change details	Select this option to omit change details from emails about new reports and from change alerts, and include only the device name and a link to the AFA Web interface. **Note:** It is possible to hide change details globally, for all users. The global setting overrides individual users' **Hide change details** setting. See Globally Hiding/Displaying Change Details.
Authorized Views and Actions	
Report	Select the report pages/information that the user can view. Select **Full Report** to indicate that the user can view all report information. Pages that are not selected will be inaccessible to the user. **Note:** A user can only be given access to **Configuration and Logs** information if they have access to the **Explore Policy** page.
Home Views	Select the **Home** page elements that the user can view. Select **All Home Views** To indicate that the user can view all **Home** page elements. Pages that are not selected will be inaccessible to the user.

In this field...	Do this...
Reporting Tool	Select this option to allow the user to access the AlgoSec Reporting Tool (ART). **Note:** Non-administration users that open the Reporting Tool will only see data relevant to the user's allowed firewalls.
Actions	Select the actions that the user can perform in AFA. Select **All Actions** to indicate that the user can perform all actions. Controls used to perform actions that are not selected will be disabled.
Authorized Devices	
Default permission profile	Select the user's default access level to devices.

Delete FireFlow privileged users

If desired, you can delete an Administrator or other privileged user. Deleted privileged users are demoted to requestors and can then be disabled in FireFlow.

Note: Deleted users are *not* removed from the FireFlow system history. They remain the owners of their change requests, and they still appear in change request histories.

Note: Deleted users' usernames and email addresses remain in the system. Since all usernames and email addresses must be unique, new users will be unable to use deleted users' usernames or email addresses. It is therefore recommended to change a user's email address before deletion, so as to enable adding the user again in the future *with their original email address*.

Do the following:

1. Switch to AFA.
2. In the toolbar, click your username.

   A drop-down menu appears.
3. Select **Administration**.

   The **Administration** page appears, displaying the **Options** tab.
4. In the **Options** tab, click the **Users/Roles** sub-tab.

   The **User and Role Management** page appears.
5. Select the check box next to the desired user.
6. Under the list of users, click **Delete**.

   A confirmation message appears.
7. Click **OK**.

   The user is deleted from AFA.

   The user is demoted to a requestor in FireFlow.
8. Disable the user in FireFlow. For details, see Manage requestors.

Disable and enable privileged users

If desired, you can disable a privileged user, so that they no longer appear in the FireFlow interface. Additionally, you can re-enable a disabled user.

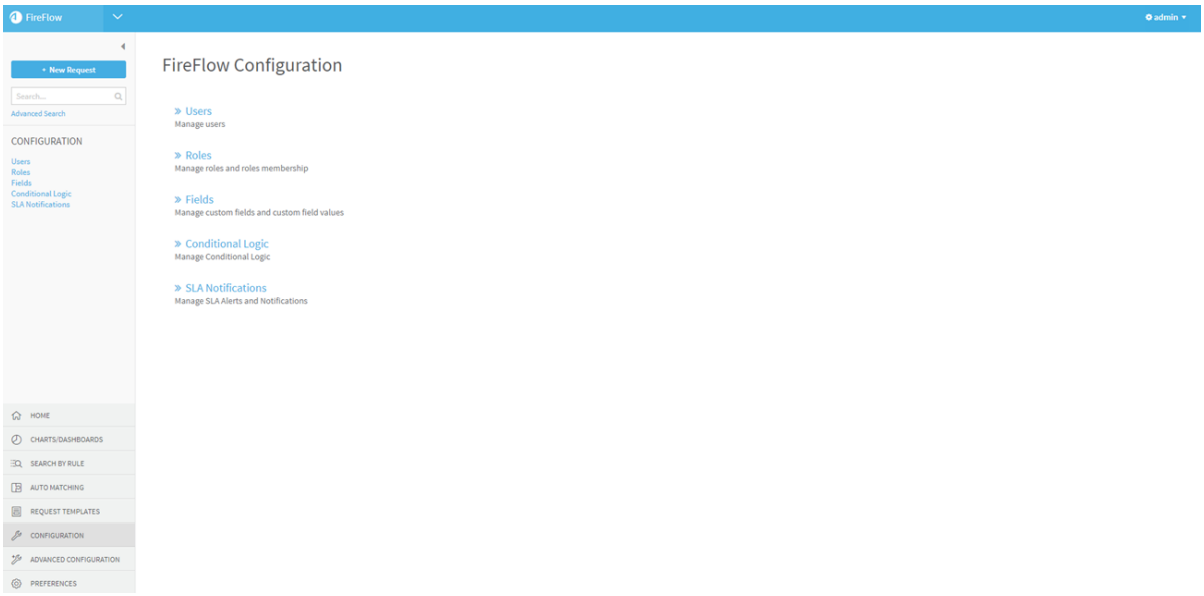
Note: Values that were entered for a user before they were disabled are retained in the FireFlow database.

Note: Users that are deleted from AFA and FireFlow are demoted to requestors and disabled.

Do the following:

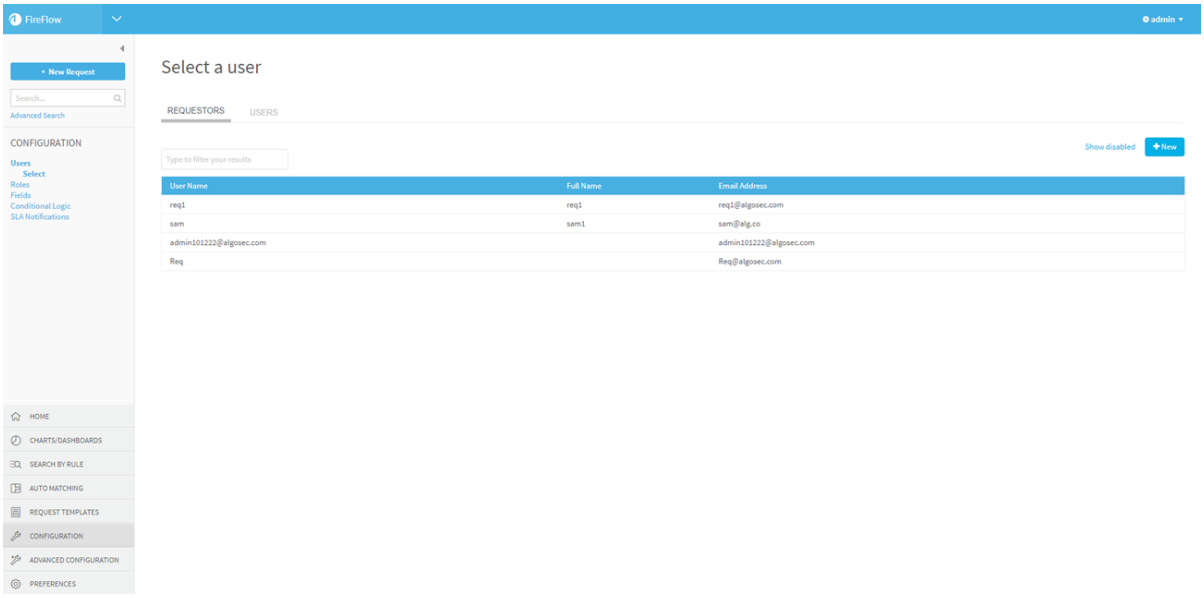
1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page appears.



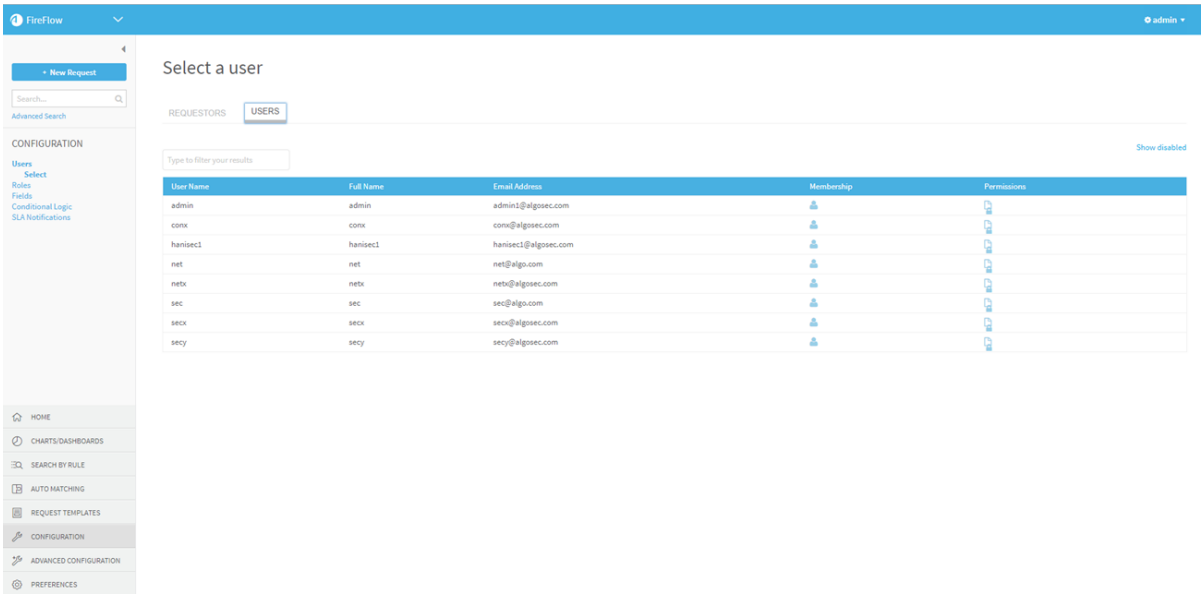
3. Click **Users**.

   The **Select a user** page appears.



4. Click the **Users** tab.

   The **Users** tab appears.



5. (Optional) To display disabled users, click the **Show disabled** link.

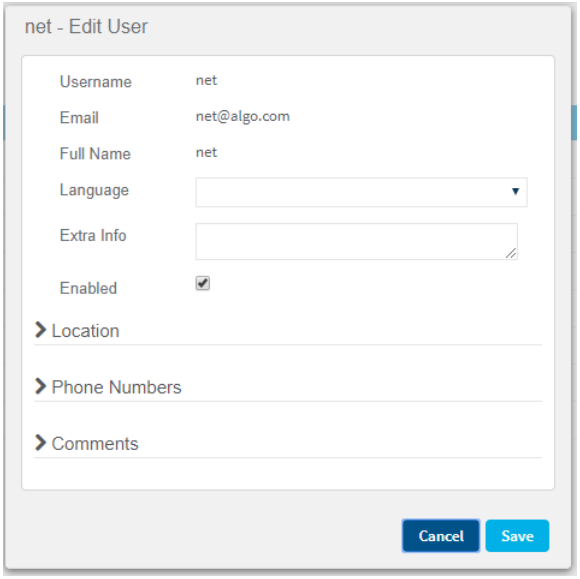
   To revert to a list which only displays enabled users, click the **Hide disabled** link.

6. (Optional) To search for the desired user, type your search in the **Type to filter your results** field.

   The users which match your search appear in the **Users** area.

7. Click the desired user's name.

   The **Edit User** window appears.



8. Do one of the following:

   - To disable the user, clear the **Enabled** check box.
   - To enable the user, check the **Enabled** check box.

9. Click **Save**.

   The user is enabled or disabled.

Manage requestors

Relevant for: Administrators

This topic describes how to manage FireFlow requestors.

FireFlow requestors can be managed by FireFlow administrators from the FireFlow Configuration area and the requestors database, and by AFA administrators from the AFA Administration area.

Manage Requester Object Views: Watch to learn how to prevent requestors from seeing the list of suggested firewall objects.

Manage requestors from AFA

AFA administrators who are not FireFlow administrators can manage requestors via the AFA Web Interface. The procedure begins in AFA and you are transferred to FireFlow.

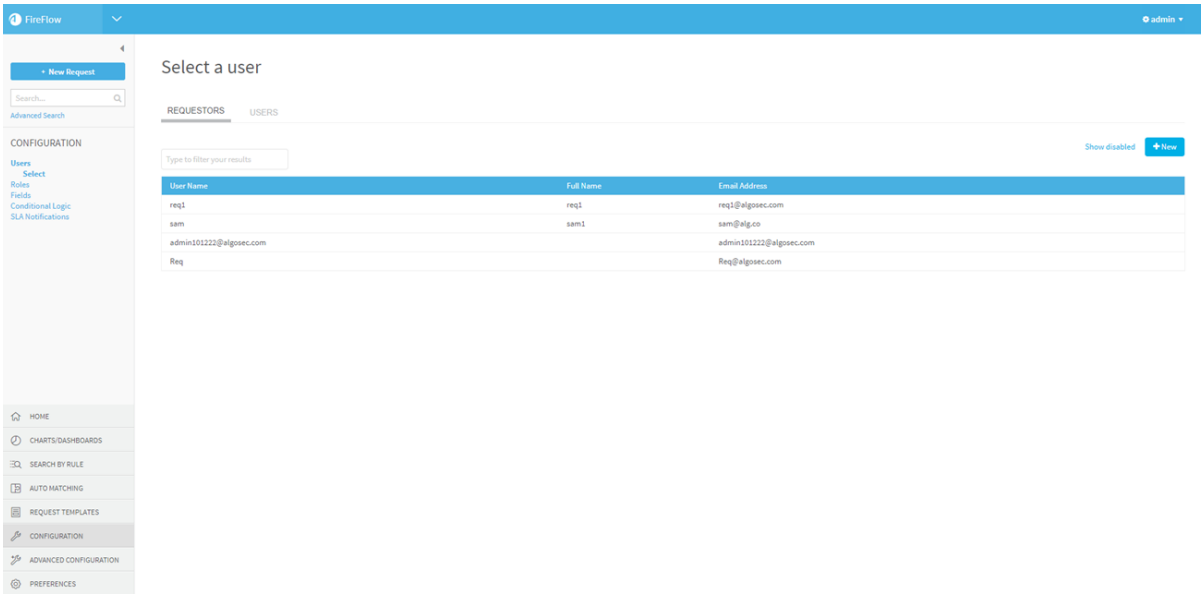
Do the following:

1. In the AFA Administration area, click the **Users / Roles** tab.

   The **User and Role Management** page appears.

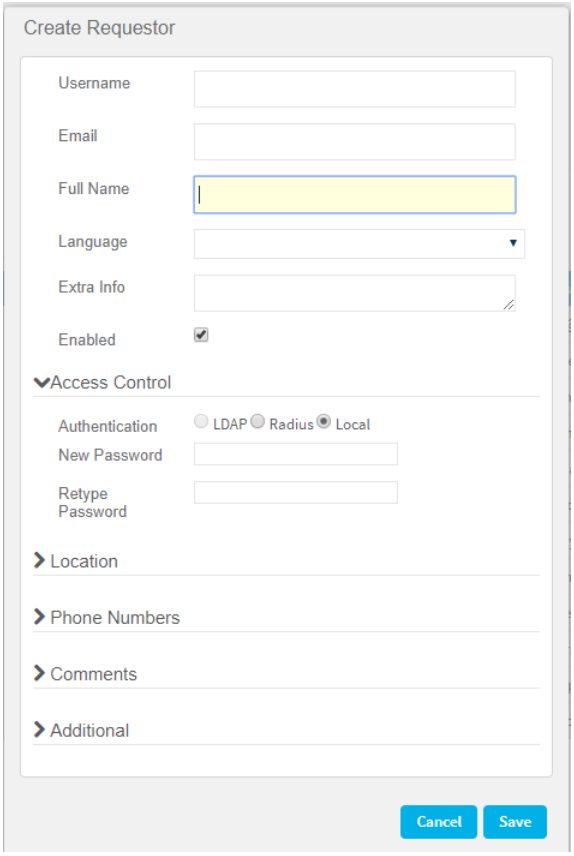
2. Click **Manage FireFlow requestors**.

   The **Select a user** page appears, displaying the **Requestors** tab.



3. Click **+ New**.

   The **Create Requestor** dialog box appears.



4. Complete the fields as needed. For details, see Requestor field reference.
5. Click **OK**.

Perform any of the following additional requestor management procedures, as needed:

Edit FireFlow requestors

Do the following:

1. In the AFA Administration area, click the **Users / Roles** tab.

   The **User and Role Management** page appears.
2. Click **Manage FireFlow requestors**.

   FireFlow opens displaying the **Requestors** tab of the **Select a user** page.
3. To display disabled requestors, click the **Show disabled** link.

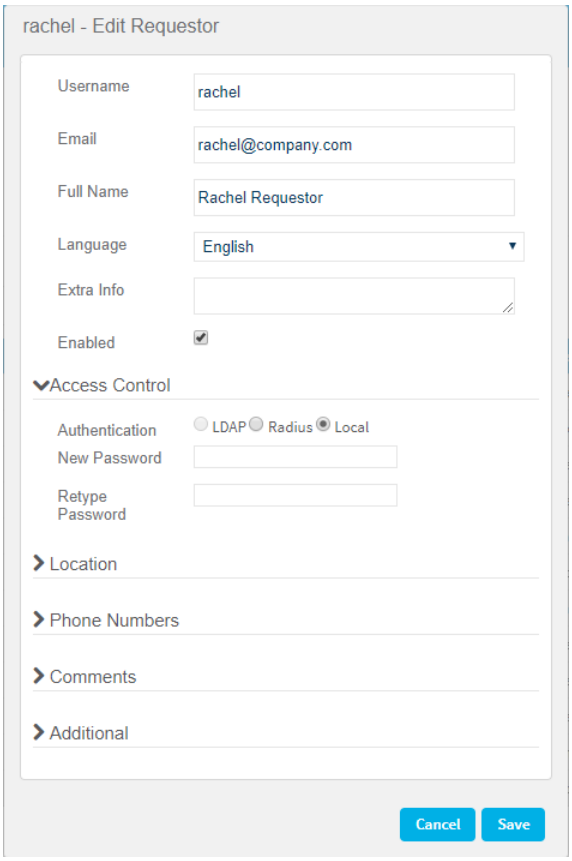
To revert to a list which only displays enabled requestors, click the **Hide disabled** link.

4. In the **Type to filter your results** field, type your search.

   The requestors which match your search appear in the **Requestors** area.

5. In the **Requestors** area, click on the desired requestor's username.

   The **Edit User** dialog box appears.



Note: If the system is configured to import user information from an LDAP server upon each login, changes to these settings may be overridden the next time the user logs in. In this case, changes to user settings must be made in the LDAP server instead of in FireFlow.

6. Complete the fields as needed. For details, see Requestor field reference.

7. Click **Save**.

Disable FireFlow requestors

Disabled requestors remain configured in FireFlow.

> **Note:** All requestor usernames and email addresses must be unique, including disabled users.
>
> If you only disable a requestor instead of deleting it, you will not be able to use that email address or username again in FireFlow.

Do the following:

1. In the AFA Administration area, click the **Users / Roles** tab.

   The **User and Role Management** page appears.
2. Click **Manage FireFlow requestors**.

   FireFlow opens displaying the **Requestors** tab of the **Select a user** page.
3. To display disabled requestors, click the **Show disabled** link.

   To revert to a list which only displays enabled requestors, click the **Hide disabled** link.
4. In the **Type to filter your results** field, type your search.

   The requestors which match your search appear in the **Requestors** area.
5. In the **Requestors** area, click on the desired requestor's username.

   The **Edit User** dialog box appears.
6. Clear the **enabled** check box.
7. Click **Ok**.

The requestor is disabled.

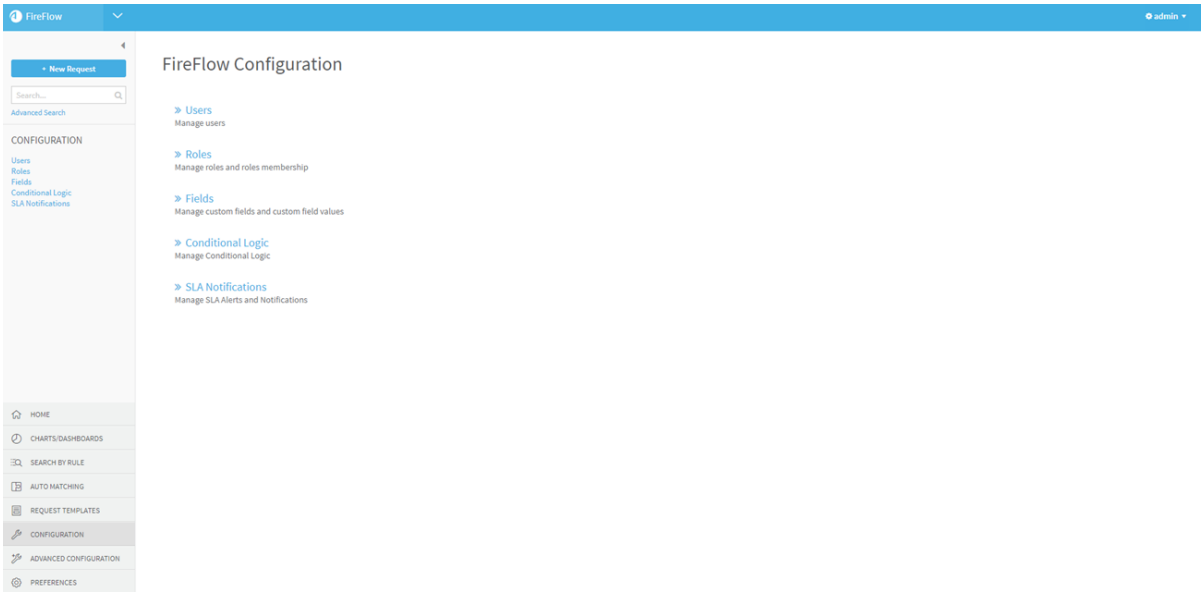
Manage requestors from FireFlow

This procedure describes how to manage requestor users from the FireFlow administration area.

Do the following:

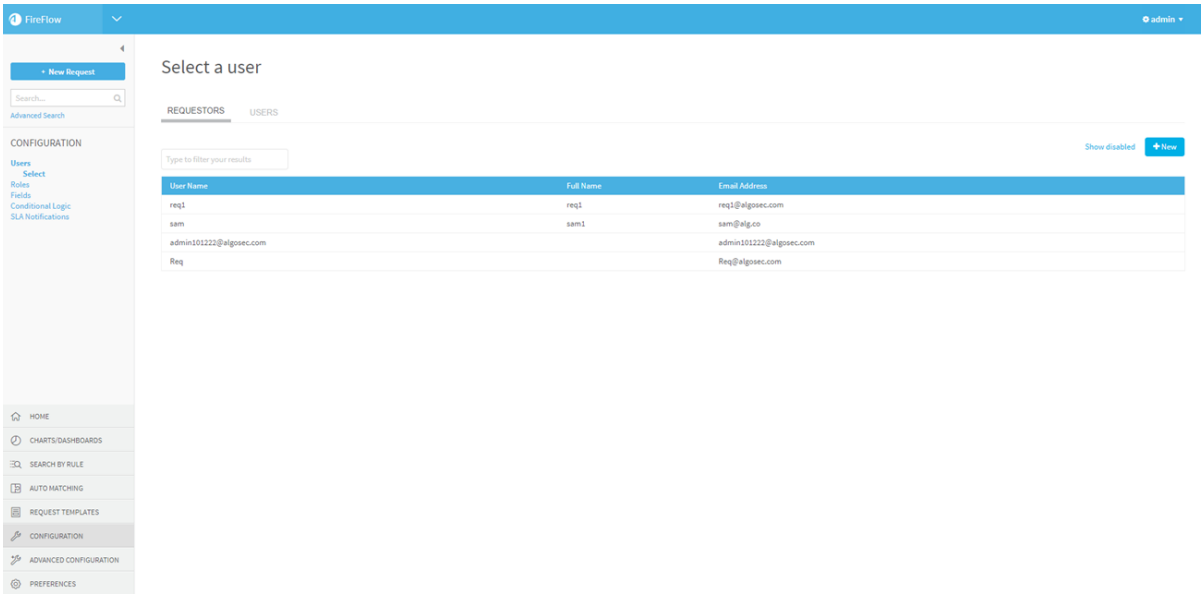
1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page appears.



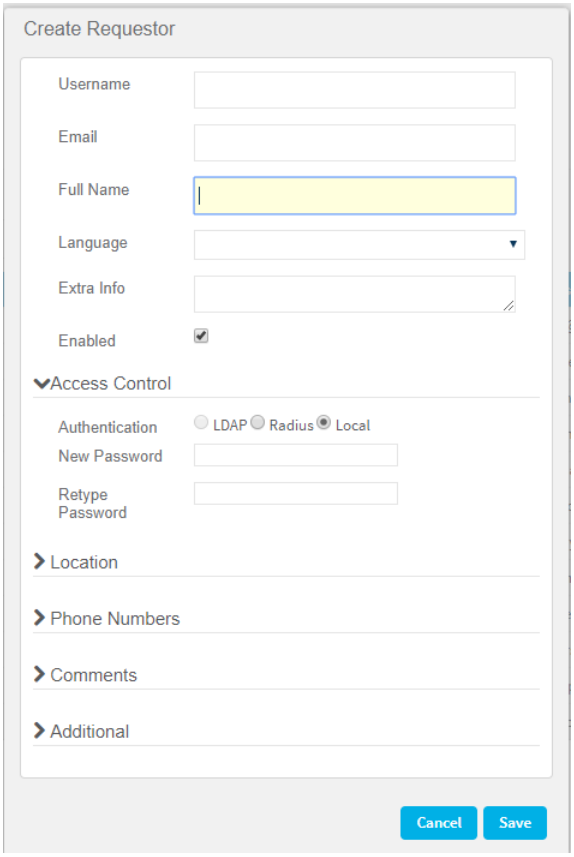
3. Click **Users**.

   The **Select a user** page appears, displaying the **Requestors** tab.



4. Click **+ New**.

   The **Create Requestor** dialog box appears.



5. Complete the fields as needed. For details, see Requestor field reference.
6. Click **OK**.

Requestor field reference

The following fields are available in either the AFA**Administration** area or the FireFlow**Configuration** area.

General fields

Username	Type the requestor's username. Usernames can contain any alpha-numeric character and the following special characters: "@", "_", ".", or "-". This field is required.
Email	Type the requestor's email address.
Full Name	Type the requestor's full name.
Language	Select the desired FireFlow interface language. All fields will be displayed in the selected language.
Extra info	Type additional information about the requestor.
Enabled	Select this option to enable the requestor to access the Requestors Web Interface.

Access Control fields

Authentication	Select the type of authentication to use for this requestor: • **Local:** Authenticate the requestor against the local AFA user database. • **Radius:** Authenticate the requestor against a RADIUS server. • **LDAP:** Select this option to enable requestor authentication against an LDAP server.
New Password	Type a password for the requestor. Passwords can contain any alpha-numeric character or any special character, excluding back ticks (`).

Retype Password	Re-type the same password you entered in the **New Password** field.

Location fields

Organization	Type the name of the requestor's organization.
Address 1	Type the requestor's primary mailing address.
Address 2	Type the requestor's secondary mailing address.
City	Type the requestor's city.
State	Type the requestor's state.
Zip	Type the requestor's zip code.
Country	Type the requestor's country.

Phone number fields

Home	Type the requestor's home telephone number.
Work	Type the requestor's work telephone number.
Mobile	Type the requestor's mobile telephone number.
Pager	Type the requestor's pager number.

Comment fields

Enter any additional comments about this requestor user.

Additional fields

If custom user fields are defined, this area displays the fields.

Complete the fields with the required information.

Manage FireFlow requestors from the requestor database

FireFlow provides a requestor management tool that enables you to add new requestors and edit existing requestors directly in the Requestor Database. The tool uses a REST

API to access the Requestor Database. This same tool can be used to export a list of requestors.

Tip: FireFlow administrators can also export the current data into a CSV file. For details, see Exporting the Requestors Database.

Do the following:

1. Create a CSV file with which to update the Requestor Database.

   For each requestor, the file should include the fields specified in CSV File Fields (see CSV File Fields).

   Note: The fields are case-sensitive.

   Note: You can save the file anywhere on the server.

2. Open a terminal, and log in using the username "root" and the related password.
3. Enter the following command:

   ```
   /usr/share/fireflow/local/extras/update_requestors.pl
   {-fCSVFile -uUsername-pPassword  [-t Timeout] [-sServerURL] |
   -iParametersFile}
   ```

   For information on the command's flags, see Requestor Database Script Flags (see Requestor Database Script Flags).

CSV File Fields

In this field...	Specify this...
UserName	The user's username. Usernames can contain any alpha-numeric character and the following special characters: "@", "_", ".", or "-". This field is required.

In this field...	Specify this...
NewUserName	A new username for the user. This field is only relevant when updating the Requestors Database.
Email	The user's email address.
Password	A password for the user. Passwords can contain any alpha-numeric character or any special character, excluding back ticks (`).
FullName	The user's full name.
HomePhone	The user's home telephone number.
Comments	Comments about this user. If the comments include a comma, line break, or quotation marks, you must enclose the comments in quotation marks.
Signature	A signature that should appear at the end of this user's messages.
Organization	The name of the user's organization.
Language	The desired FireFlow interface language. All fields will be displayed in the selected language.
ExtraInfo	Additional information about the user.
WorkPhone	The user's work telephone number.
PagerPhone	The user's pager number.
Address1	The user's primary mailing address.
Address2	The user's secondary mailing address.
City	The user's city.
State	The user's state.
Zip	The user's zip code.
Country	The user's country.

In this field...	Specify this...
Authentication	The type of authentication to use for this user. This can have the following values: • `Local`. Authenticate the user against the local AFA user database. If you select this option, you must include the `Password` field. • `Radius`. Authenticate the user against a RADIUS server. • `LDAP`. Authenticate the user against Microsoft Active Directory via LDAP.
MobilePhone	The user's mobile telephone number.
Disabled	Whether to enable the user to access the Requestors Web Interface. This can have the following values: • `0`. Enable access to the Requestors Web Interface. • `1`. Disable access to the Requestors Web Interface. The default value is 0.

Requestor Database Script Flags

Flag	Description
`-f`*CSVFile*	The full path and name of the CSV input file. This flag is relevant only when updating the Requestors Database.
`-l`*CSVFile*	The full path and name of the CSV output file. This flag is relevant only when exporting the Requestors Database.
`-u`*Username*	The user name of an AlgoSec administrator with permissions to manage requestors.
`-p`*Password*	The password of an AlgoSec administrator with permissions to manage requestors.
`-a`	Display all users, including disabled ones, in the CSV output file. This flag is relevant only when exporting the Requestors Database.

Flag	Description
`-t` *Timeout*	The timeout in seconds for each HTTP request that the tool issues against the FireFlow server. The default value is 90.
`-s` *ServerURL*	The FireFlow server URL. The default value is https://localhost.
`-i` *ParametersFile*	The parameters input file. When this flag is used, the requestors management tool will refer to a parameters input file for all flags. This is useful if you want to avoid typing a password in the command line. The parameters input file must be a text file, with each flag appearing on a different line.

Exporting the Requestors Database

You can use the requestor management tool to export a list of requestors from the Requestor Database into a CSV file.

Do the following:

1. Open a terminal, and log in using the username "root" and the related password.
2. Enter the following command:

```
/usr/share/fireflow/local/extras/update_requestors.pl
{-lCSVFile -uUsername-pPassword  [-a] [-t Timeout] [-sServerURL] |
-iParametersFile}
```

For information on the command's flags, see Requestor Database Script Flags (see Requestor Database Script Flags).

The CSV file is exported. For each requestor, the file includes the fields specified in CSV File Fields (see CSV File Fields).

Manage user roles

Relevant for: Administrators

Fireflow roles can be managed either from the FireFlow configuration area, or from the AFA**Administration** area.

Edit Role Permissions for Implementation: Watch to learn how to control granular permissions at the role level.

Assign and revoke user roles in AFA

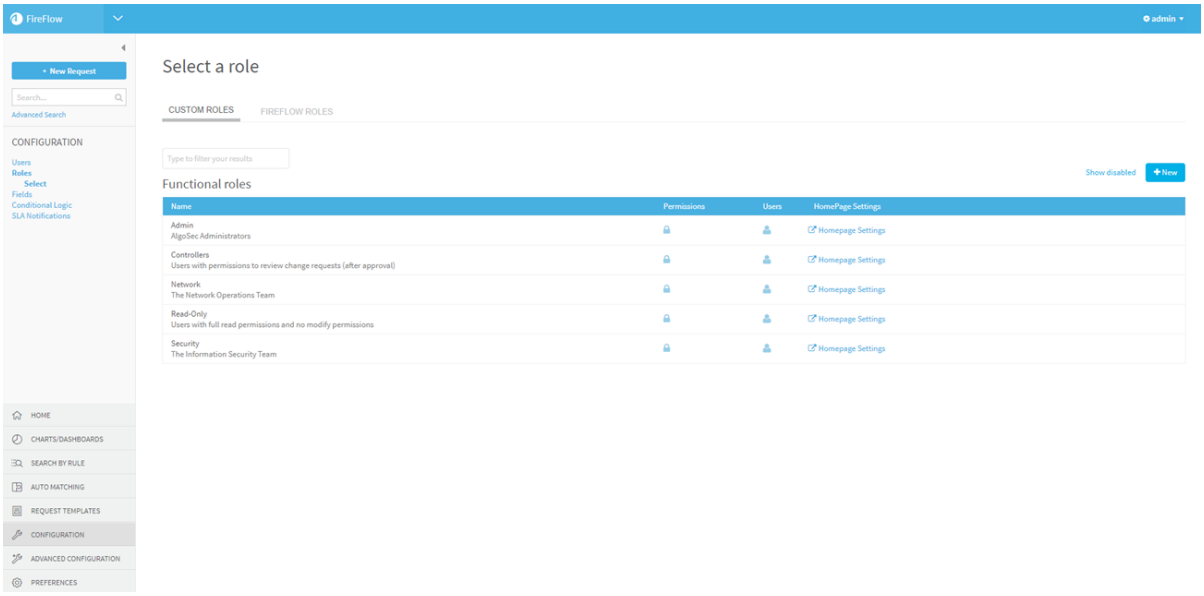
Do the following:

1. In the AFA Administration area, click the **Users / Roles** tab.

   The **User and Role Management** page appears.

2. Click **Manage FireFlow roles**.

   FireFlow opens, displaying the **Select a role** page.



3. (Optional) To display disabled roles, click the **Show disabled** link.

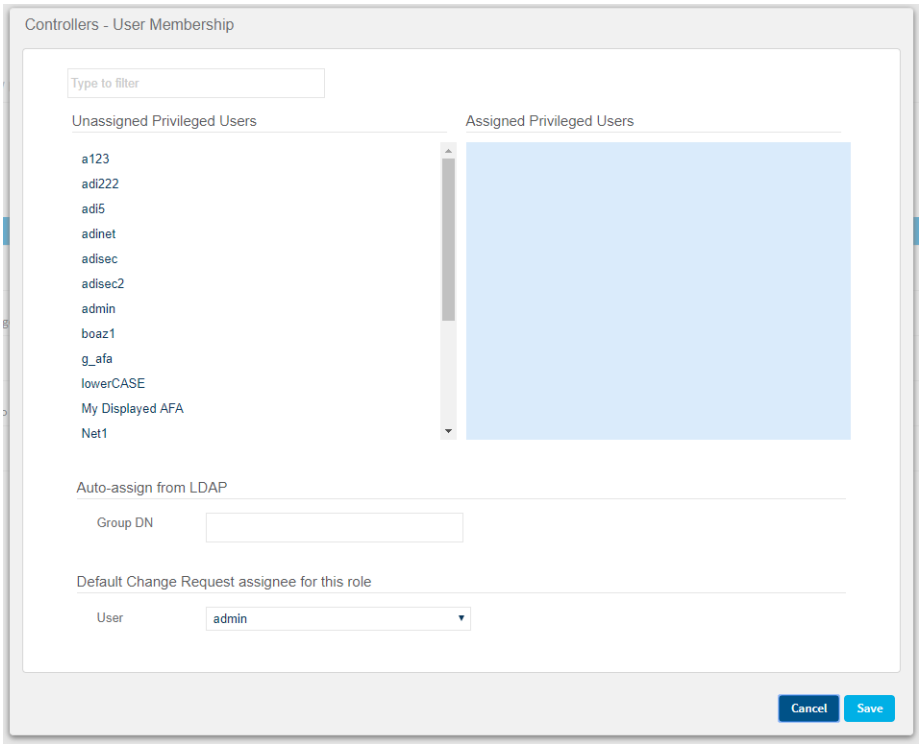
   To revert to a list which only displays enabled roles, click the **Hide disabled** link.

4. (Optional) To search for the desired role, type your search in the **Type to filter your results** field.

The roles which match your search appear in the **Functional roles** area.

5. In the row of the relevant role, click  .

   The **Users Membership** window for the role you desire appears.



6. To assign a user to the role, click on the user in the **Unassigned Privileged Users** list.
7. To revoke a role from a user, click on the user in the **Assigned Privileged Users** list.
8. Click **OK**.

The user(s) and role(s) are updated.

Assign default change request assignees in AFA

When a change request advances to certain stages in FireFlow workflows, FireFlow automatically assigns the change request to a user with a specific role. For each role, you can designate which user (amongst the users assigned the relevant role) will be assigned the change request.

Do the following:

1. In the AFA Administration area, click the **Users / Roles** tab.

   The **User and Role Management** page appears.

2. Click **Manage FireFlow roles**.

   FireFlow opens, displaying the **Select a role** page.

3. In the row of the relevant role, click  .

   The **Users Assignment** window for the role appears.

4. In the **Default Change Request assignee for this role** area, select a user in the drop-down menu.

5. Click **OK**.

The user is assigned as the default assignee for the role.

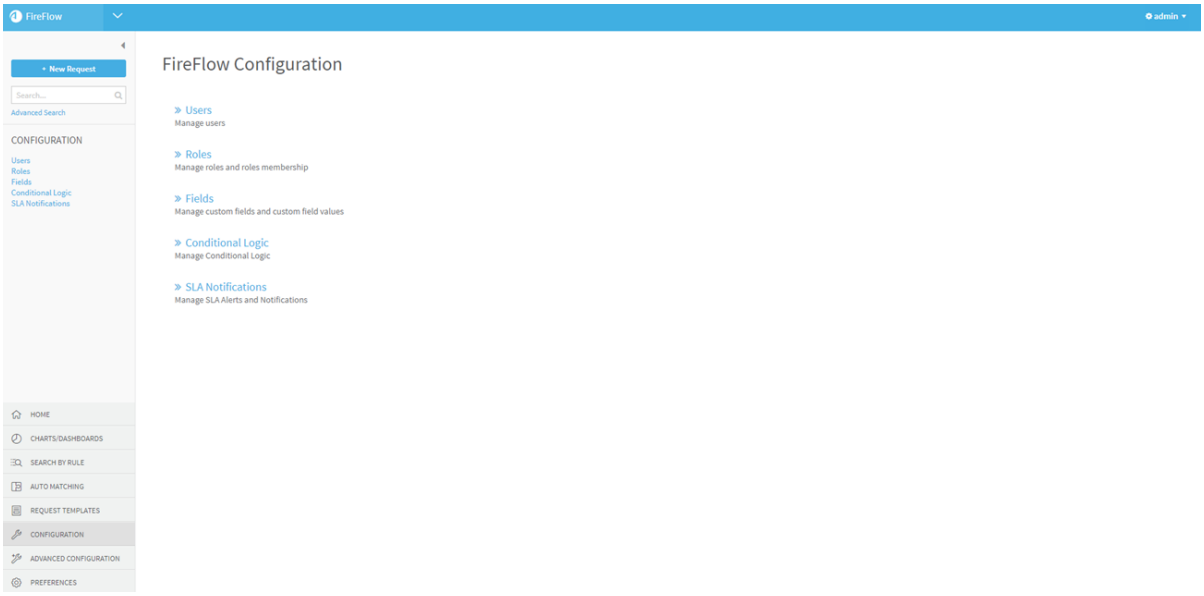
Add user roles in FireFlow

Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.

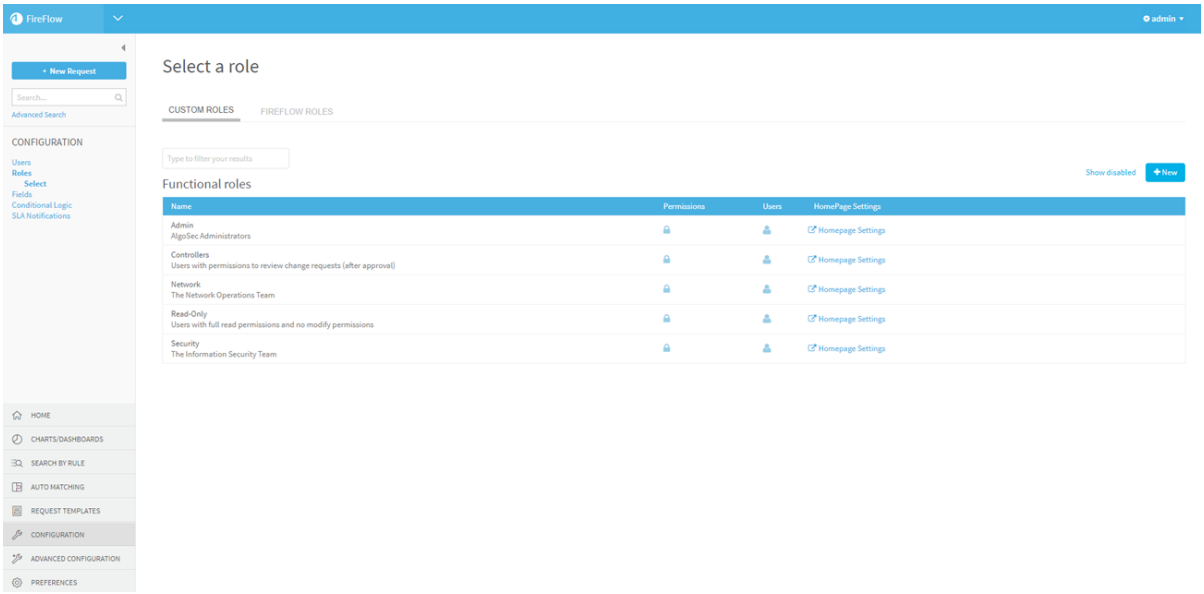
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page is displayed.



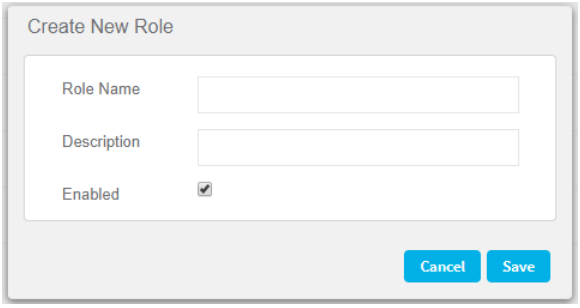
3. Click **Roles**.

   The **Select a role** page is displayed.



4. Click **+ New**.

   The **Create New Role** window is displayed.



5. Complete the fields as needed:

Role Name	Type a name for the role.
Description	Type a description of the role.
Enabled	Select this option to enable the role.

6. Click **Save**.

Continue with any of the following:

- Assign and revoke user roles in FireFlow
- Customize the FireFlow Home page
- View user membership and permissions

Edit user roles in FireFlow

Note: Do not change any of the pre-defined **Admin** user role's settings. This role consists of the AlgoSec administrators and is only used by FireFlow internally.

Note: If you change the name of a pre-defined user role (Network, Security, Controllers, or Read-Only), you must also change the role's name in all workflows.

For more details, see Manage workflow options.

Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. To edit the role's name and description, do the following:
    a. In the main menu, click **Configuration**.

       The **FireFlow Configuration** page appears.
    b. Click **Roles**.

       The **Select a role** page appears.
    c. (Optional) To display disabled roles, click the **Show disabled** link.

       To revert to a list which only displays enabled roles, click the **Hide disabled** link.
    d. (Optional) To search for the desired role, type your search in the **Type to filter your results** field.

       The roles which match your search appear in the **Functional roles** area.
    e. Click the desired role's name.

       The **Editing Role** window appears.
    f. Complete the fields as needed:

Role Name	Type a name for the role.
Description	Type a description of the role.
Enabled	Select this option to enable the role.

    g. Click **Save**.

Continue with any of the following:

- Assign and revoke user roles in FireFlow
- Customize the FireFlow Home page

- View user membership and permissions

Assign and revoke user roles in FireFlow

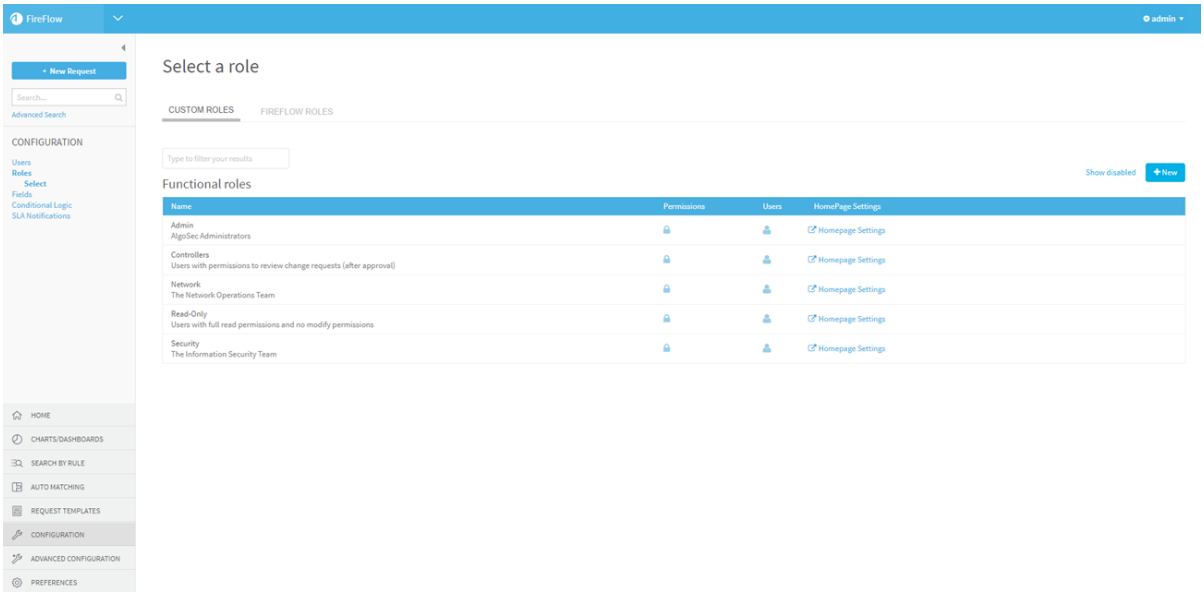
Tip: Alternately, assign all members of a specific LDAP group to a specific role. For more details, see Manage authentication servers and SSO.

Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page appears.
3. Click **Roles**.

   The **Select a role** page appears.



4. (Optional) To display disabled roles, click the **Show disabled** link.

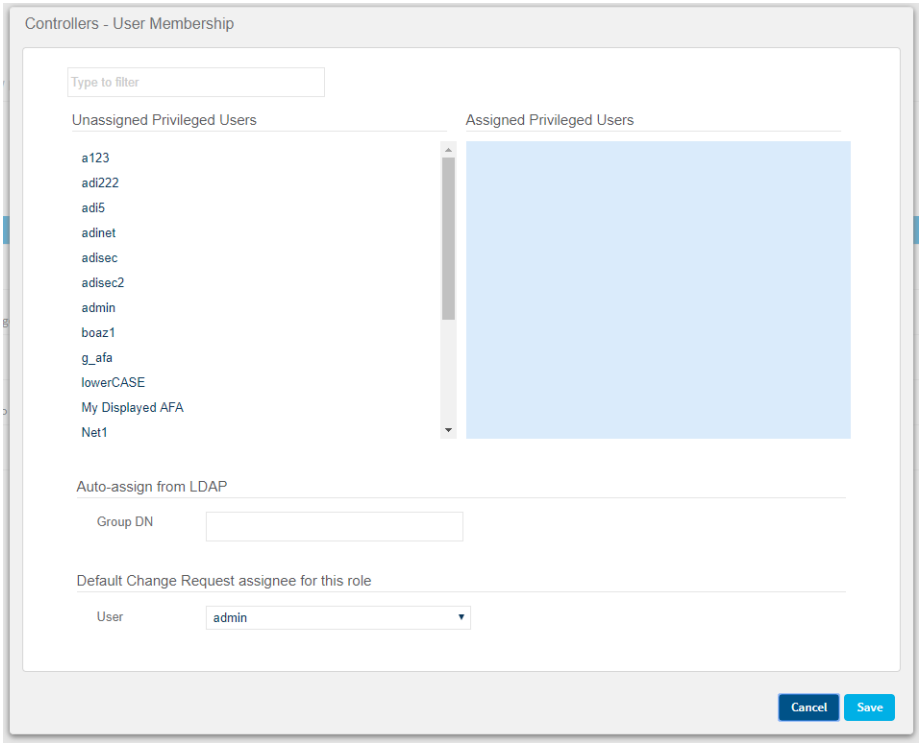
   To revert to a list which only displays enabled roles, click the **Hide disabled** link.

5. (Optional) To search for the desired role, type your search in the **Type to filter your results** field.

   The roles which match your search appear in the **Functional roles** area.

6. In the row of the relevant role, click  .

   The **Users Membership** window for the role you desire appears.



7. To assign a user to the role, click on the user in the **Unassigned Privileged Users** list.
8. To revoke a role from a user, click on the user in the **Assigned Privileged Users** list.
9. Click **OK**.

The user(s) and role(s) are updated.

Assign default change request assignees in FireFlow

When a change request advances to certain stages in FireFlow workflows, FireFlow automatically assigns the change request to a user with a specific role. For each role,

you can designate which user (amongst the users assigned the relevant role) will be assigned the change request.

Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page appears.
3. Click **Roles**.

   The **Select a role** page appears.
4. In the row of the relevant role, click  .

   The **Users Assignment** window for the role appears.
5. In the **Default Change Request assignee for this role** area, select a user in the drop-down menu.
6. Click **OK**.

The user is assigned as the default assignee for the role.

Disable or enable user roles in FireFlow

If desired, you can disable a user role, so that it no longer appears in the FireFlow interface. You can also re-enable disabled user roles.

Note: Values that were entered for the user role before it was disabled are retained in the FireFlow database.

Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.

2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page is displayed.

3. Click **Roles**.

   The **Select a role** page is displayed.

4. (Optional) To display disabled roles, click the **Show disabled** link.

   To revert to a list which only displays enabled roles, click the **Hide disabled** link.

5. (Optional) To search for the desired role, type your search in the **Type to filter your results** field.

   The roles which match your search appear in the **Functional roles** area.

6. Click the desired role's name.

   The **Editing Role** window is displayed.

7. Do one of the following:

   - To disable a role, clear the **Enabled** check box.
   - To enable a role, check the **Enabled** check box.

8. Click **Save**.

View user membership and permissions

You can view the roles and permissions that a user is assigned.

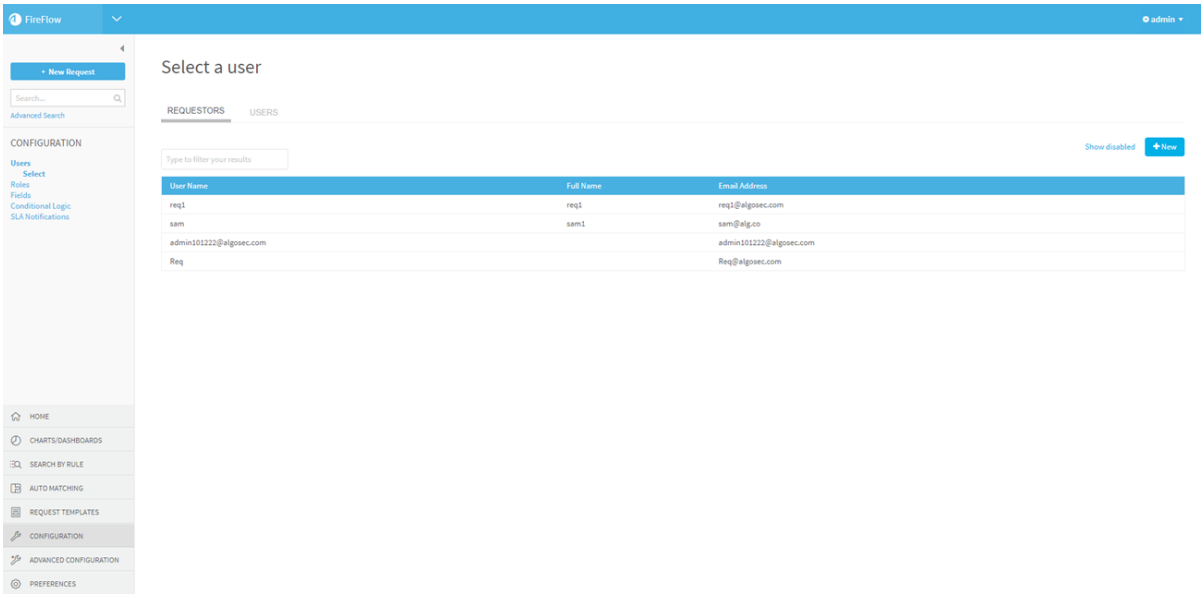
Do the following:

1. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page is displayed.

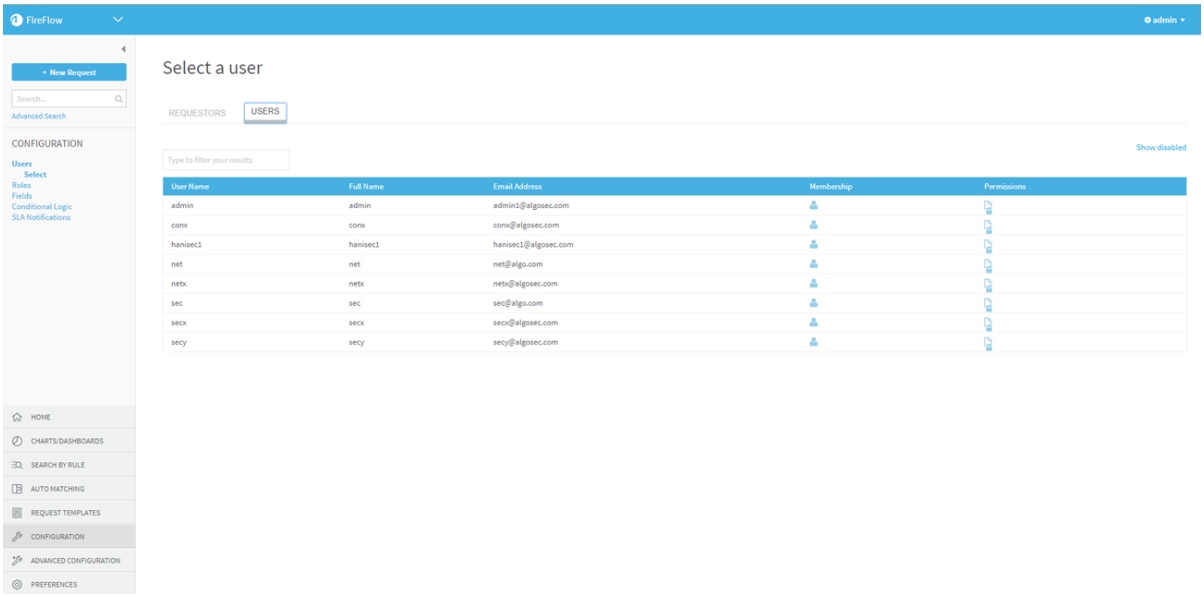
2. Click **Users**.

   The **Select a user** page is displayed.



3. Click the **Users** tab.

   The **Users** tab is displayed.



4. (Optional) To display disabled users, click the **Show disabled** link.

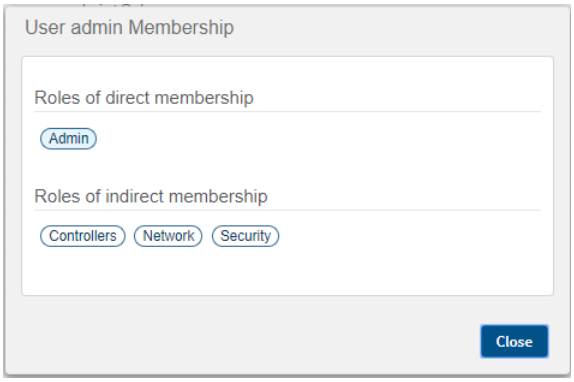
   To revert to a list which only displays enabled users, click the **Hide disabled** link.

5. (Optional) To search for the desired user, type your search in the **Type to filter your results** field.

   The fields which match your search appear in the **Users** area.

6. To view a user's role membership, click in the row of the relevant user.

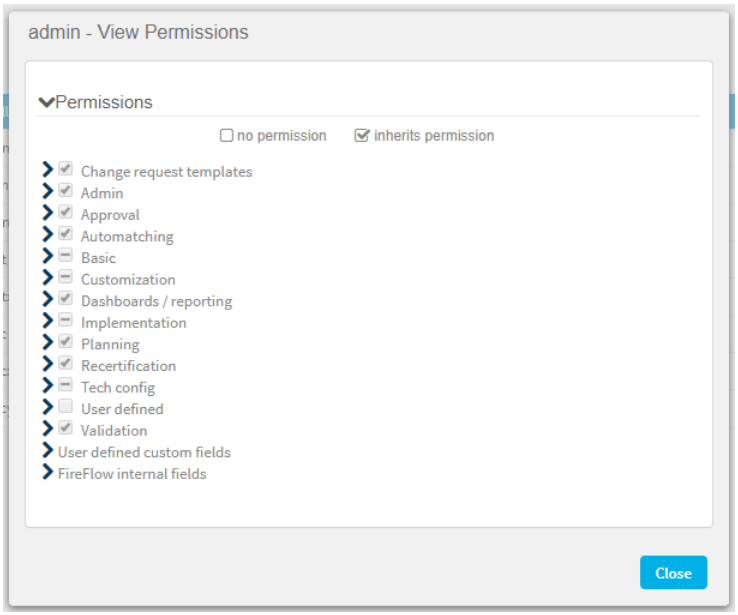
   The **User Membership** window is displayed.



   The window display's the user's direct and indirect roles.

7. To view a user's permissions, click in the row of the relevant user.

   The **View Permissions** window is displayed.



Each parent permission appears in the column. If the user is assigned all of the sub-permissions for a parent permission, the check box next to the parent permission is checked. If the user is assigned none of the sub-permissions for a parent permission, the check box next to the parent permission is unchecked. If the user is assigned some of the sub-permissions for a parent permission, a box appears in the check box next to the parent permission.

To view the sub-permissions for a parent permission, click ›.

8. Click **Close**.

Define responsible role conditions

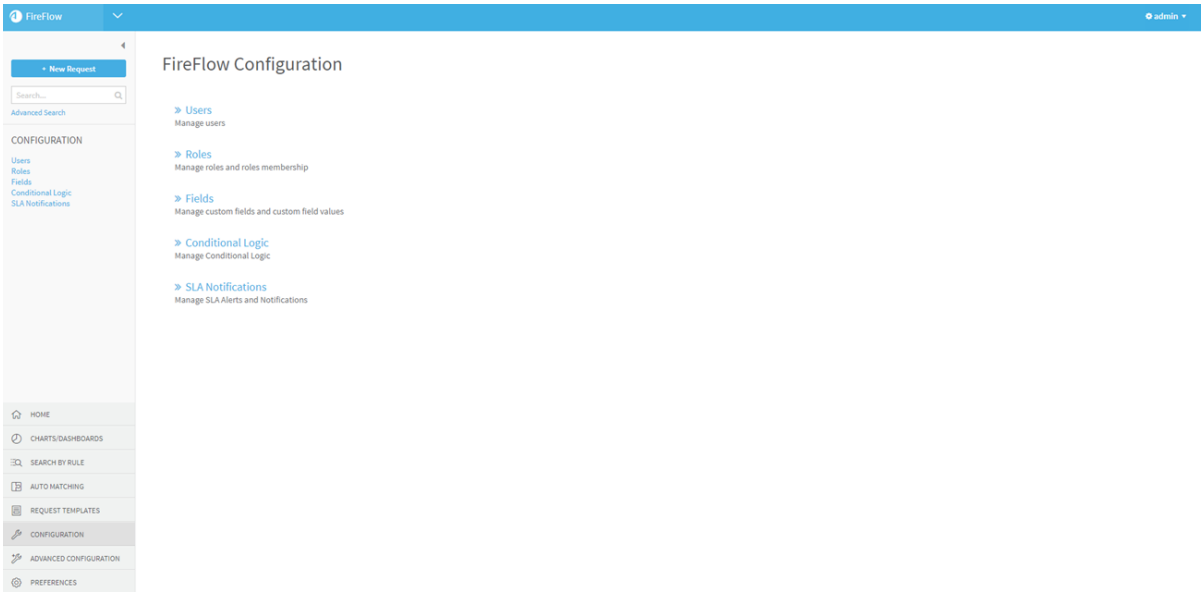
When a change request enters a new status, the responsible party for the change request may change. A specific role is responsible for the change request in the new status, and the default assignee of the role is assigned ownership of the change request when the change request enters the new status. FireFlow supports configuring custom conditions (which override the default configuration for the status) to indicate when a role should be the responsible role for the status.

Note: Conditions configured for responsible roles in the FireFlow web interface take precedence over any conditions specified with the **GetRealGroupName** (see GetRealGroupName) hook.

Do the following:

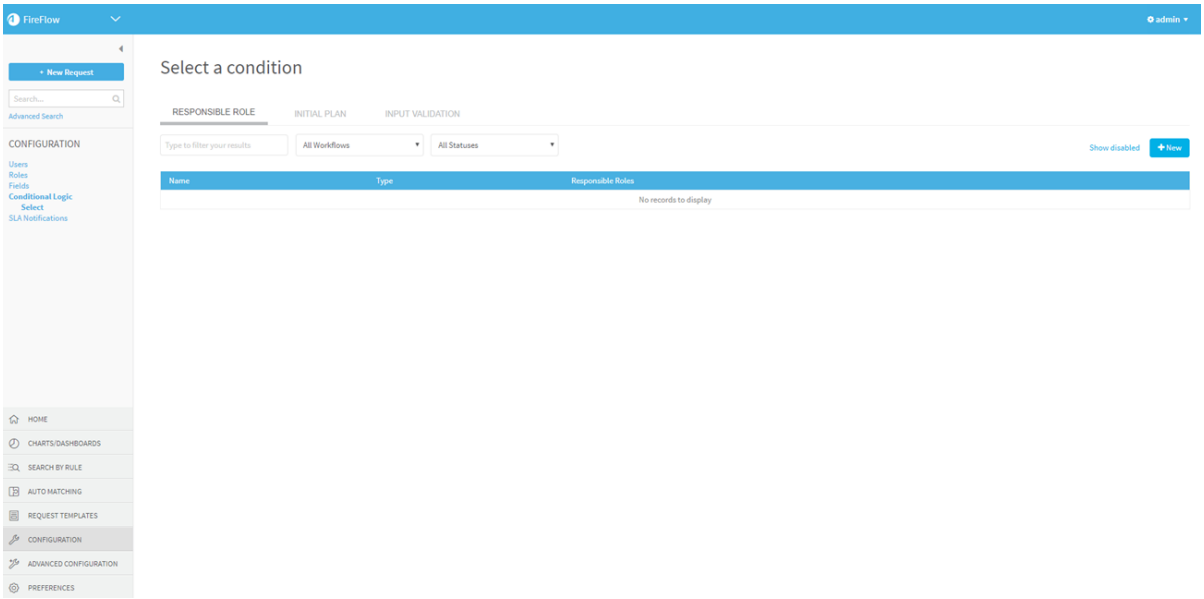
1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page appears.



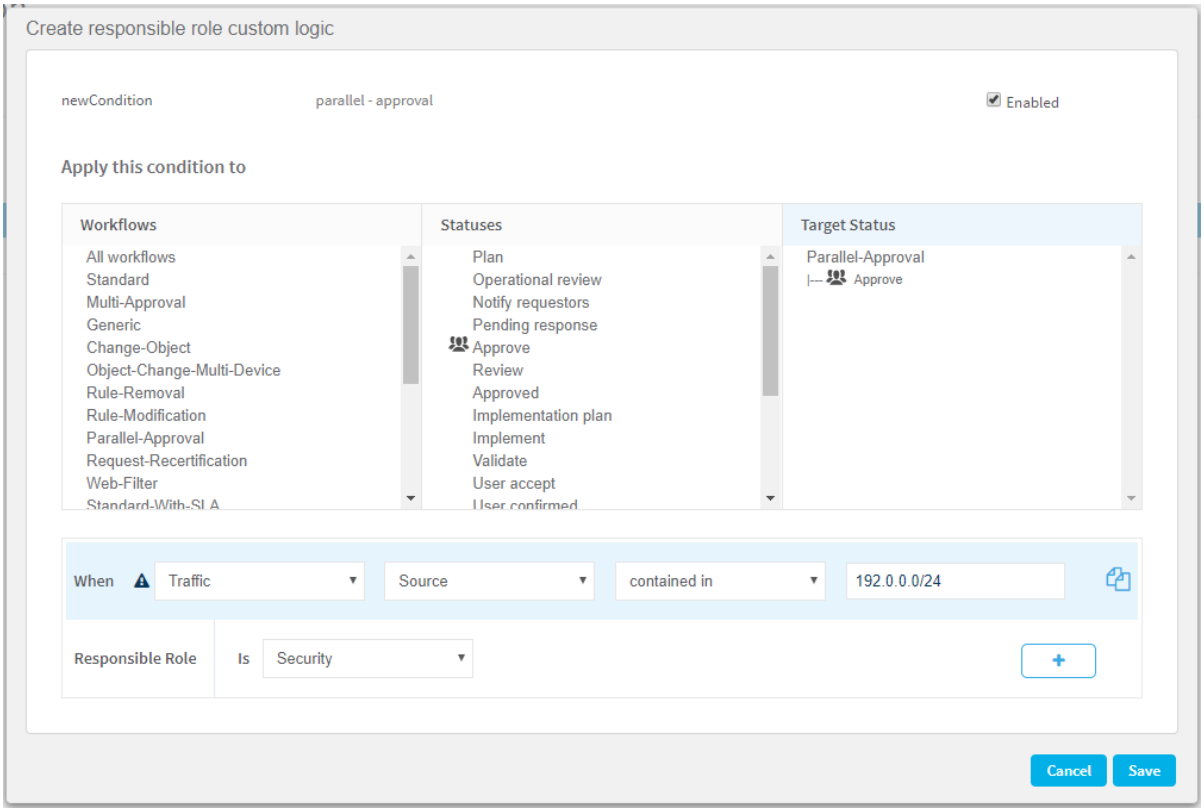
3. Click **Conditional Logic**.

   The **Select a condition** page appears.



4. Click +New.

   The **Create responsible role custom logic** window appears.



Note: Some statuses support multiple responsible role definitions, allowing you to specify a different responsible role for a slightly different scenario. These statuses are marked with the multi-condition icon: .

5. Complete the fields using the relevant information in Responsible Role Custom Logic Fields (see Responsible Role Custom Logic Fields).
6. Click **Save**.

Responsible Role Custom Logic Fields

In this field...	Do this...
Enter Condition Name	Type a name to represent the condition.

In this field...	Do this...
Enter Description	Type the description of the condition.
Enabled	Select this check box to enable the condition.
Apply this condition to	Select the relevant workflow, and then corresponding status. You can select multiple statuses from the same workflow or from different workflows. The selected statuses appear in the **Target Status** list. To remove a status, click the status in the **Target Status** list.
When	Define the condition by selecting the condition type in the drop down menu and completing the relevant fields. • For the **Custom Field** condition type, select the field, select the boolean operator, and type the value for the field. • For the **Request's Device** condition type, select the boolean operator and the device. • For the **Traffic** condition type, select the relevant endpoint(s), select the boolean operator, and type the IP address, range or CIDR for the field. **Note:** The **Traffic** condition type is only for traffic change request workflows.
Responsible Role	In the drop-down list, select the role which should be assigned to change requests which meet the defined conditions.
	Click this to duplicate a condition in order to add a different condition for the target statuses. Additional conditions allow you to specify different responsible roles for slightly different situations. **Note:** Additional conditions are only supported for some statuses. These statuses are marked with the multi-condition icon:  .
	Click this to remove a condition.

In this field...	Do this...
+	Click this to add an additional condition for the target statuses. Additional conditions allow you to specify different responsible roles for slightly different situations. **Note:** Additional conditions are only supported for some statuses. These statuses are marked with the multi-condition icon: .

Manage user permissions

Relevant for: Administrators

FireFlow enables you to assign permissions to user roles. Each permission represents an action that a user assigned the role can perform.

This section explains how to configure permissions.

Permission types

FireFlow supports the following types of permissions:

Built-in permissions	FireFlow includes a set of built-in permissions that represent specific actions users can perform.
User-defined permissions	FireFlow includes a set of user-defined permissions that are labeled **UserDefinedRight01** through **UserDefinedRight10**. Unlike the built-in permissions, which are tied to specific actions, user-defined permissions can be used to represent any custom action, in order to restrict the performance of those actions to certain users. For example, let's say you want to modify the Standard workflow so that it includes a custom action called "First Approve", and you want to restrict this action to users who have "First Approval" permissions. Since "First Approval" permissions do not exist in the FireFlow system, you can decide that **UserDefinedRight01** will represent "First Approval" permissions, and assign these permissions to the desired user roles. **Note:** You cannot rename user-defined permissions.

When assigning permissions to a user role, all those assigned the role (both users and sub-roles) will automatically inherit the permissions. This enables you to quickly configure a new user's permissions, by simply assigning the user the desired role.

You can assign permissions to the following types of user roles:

Custom roles	Includes Network, Security, and any other roles defined by a user.
FireFlow roles	FireFlow roles include: • **System roles**. Includes Everyone, Privileged, and Unprivileged (requestors). • **Per-request roles**. Includes Cc, Requestor, and Owner.

Permissions assigned to a per-request role are only relevant for users who are filling that role in relation to a specific change request.

For example, if you assign "ShowTicket" permissions to the Requestor role, then a user who is the requestor for a specific change request will be able to view that change request.

The same user will not be able to view other change requests for which they are not the requestor, unless the user is also assigned a system or custom role with "ShowTicket" permissions.

Note: The AdminCc per-request role is not in use and should be ignored.

Configure built-in permissions for roles

Note: By default, both the Network and Security user roles can view matching output, but only the Security user role can perform manual matching. Furthermore, both these user roles can view change records in FireFlow and modify their summary or comment on the change records. If desired, you can change these settings for these user roles or any other user role.

Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page is displayed.
3. Click **Roles**.

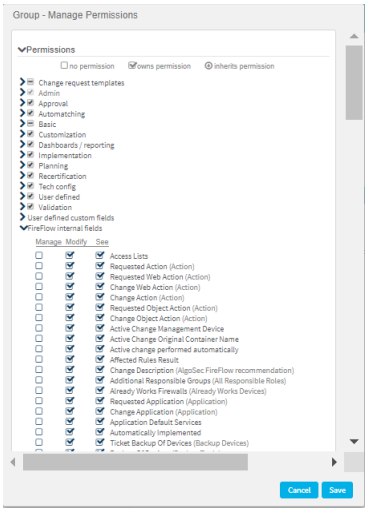
   The **Select a role** page is displayed.
4. If you want to assign permissions to a FireFlow role, click the **FireFlow Roles** tab.

   The **FireFlow Roles** tab is displayed.
5. (Optional) To display disabled roles, click the **Show disabled** link.

   To revert to a list which only displays enabled roles, click the **Hide disabled** link.
6. (Optional) To search for the desired role, type your search in the **Type to filter your results** field.

   The roles which match your search appear in the **Functional roles** area.
7. In the row of the relevant role, click .

   The **Manage Permissions** window for the role you desire appears.



Each parent permission appears in the column. If the role is assigned all of the sub-permissions for a parent permission, the check box next to the parent permission is checked. If the role is assigned to none of the sub-permissions for a parent permission, the check box next to the parent permission is unchecked. If the role is assigned some of the sub-permissions for a parent permission, a box appears in the check box next to the parent permission.

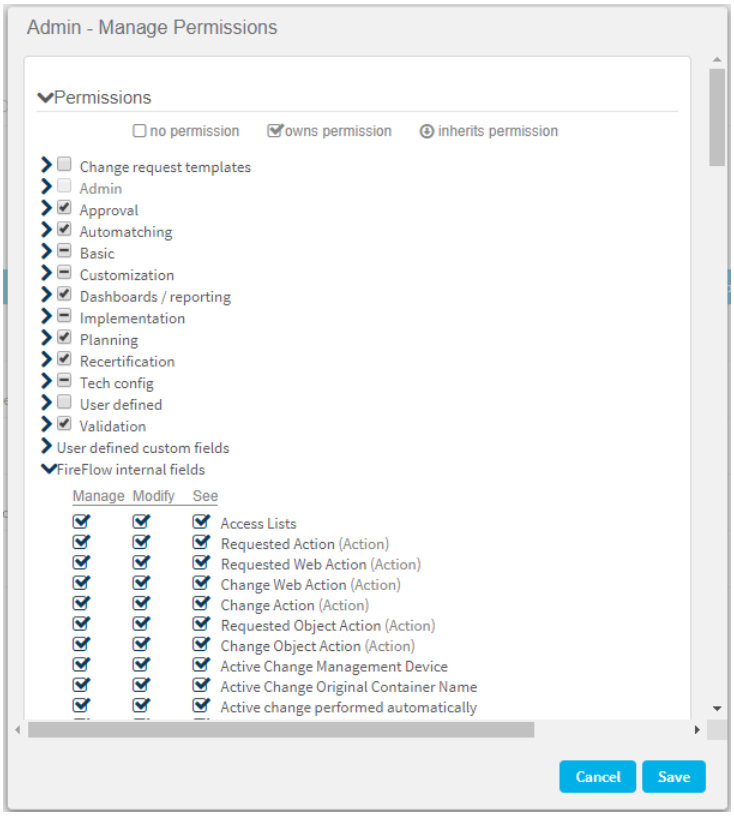
8. To view the sub-permissions for a parent permission, click ›.

   If the role is not assigned the sub-permission, the check box next to the sub-permission is unchecked. If the role is directly assigned a sub-permission, the check box next to the sub-permission is checked. If the role inherits the sub-permission from another role, a circled arrow appears next to the sub-permission.

   For descriptions of some of the built-in permissions, see Built-in Permissions (see Built-in Permissions).

   User defined custom fields and FireFlow internal fields

   Regarding **User defined custom fields** and **FireFlow internal fields**:



- Users assigned a role with permission to **Manage** the field can view and modify the field's definition (for example, they can modify the field's name, disable it, and so on).
- Users assigned a role with permission to **Modify** the field can modify the fields value, but not view the field.
- Users assigned a role with permission to **See** the field can view the field.

9. To assign a permission, select the check box next to the desired permission.

   Note: It is recommended to select permissions similar to those of the pre-defined Security and/or Network roles.

10. To revoke a permission, clear the check box next to the desired permission.
11. To set the role to inherit the permissions of another role, do the following:

a. In the **Inherit from other roles** area, select the desired role in the drop-down list.

b. Click **Add Role**.

12. To set the role not to inherit the permissions of another role, in the **Inherit from other roles** area, click **x** next to the desired role.
13. Click **Save**.

The role's permissions are saved.

Built-in Permissions

Permission	Description
Change request templates	Allows users with the role to view and use the selected request templates.
Automatching	All of the following permissions are sub-permissions of the **Automatching** parent permission.
DeleteMatches	Allows users with the role to delete matching output for all change requests. This right is required for manual matching.
ModifyChanges	Allows users with the role to modify or comment on change records.
ModifyMatches	Allows users with the role to modify matching output for all change requests. This right is required for manual matching.
ShowChanges	Allows users with the role to view change records for all change requests.
ShowMatches	Allows users with the role to view matching output for all change requests.

Configure user-defined permissions for roles

Do the following:

1. Choose an unused user-defined permission (**UserDefinedRight01** through **UserDefinedRight10**) to represent the permission to perform a certain custom action.

   For example, if you want to modify the Standard workflow so that it includes a custom action called "First Approve", and you want to restrict this action to users who have "First Approval" permissions, you would choose **UserDefinedRight01** to represent the permission to perform the "First Approve" custom action.

2. Assign the user-defined permission to the user roles that should be allowed to perform the custom action, by doing the following:

   a. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.

   b. In the main menu, click **Configuration**.

      The **FireFlow Configuration** page is displayed.

   c. Click **Roles**.

      The **Select a role** page is displayed.

   d. If you want to assign permissions to a FireFlow role, click the **FireFlow Roles** tab.

      The **FireFlow Roles** tab is displayed.

   e. (Optional) To display disabled roles, click the **Show disabled** link.

      To revert to a list which only displays enabled roles, click the **Hide disabled** link.

   f. (Optional) To search for the desired role, type your search in the **Type to filter your results** field.

      The roles which match your search appear in the **Functional roles** area.

   g. In the row of the relevant role, click  .

      The **Manage Permissions** window for the role you desire is displayed.

h. Click › next to **User defined**.

   The sub-permissions appear.

i. Check the check box for the user-defined permission you are using.

   In our example, you would assign **UserDefinedRight01** permissions to the user roles that should be allowed to perform the "First Approve" action.

3. Modify the custom action to restrict its use to users with the selected user-defined permission.

For more details, see Manage workflow options.

Manage authentication servers and SSO

This section describes how manage all abilities related to authentication servers, such as LDAP or RADIUS, and Single Sign on (SSO).

Note: Since data is imported only upon user login, the data stored for users who log in infrequently may be outdated.

Import LDAP user data (LDAP or RADIUS server)

This section describes how to import LDAP user data, such as phone numbers, when authenticating with an LDAP or RADIUS server.

In addition to importing the data, FireFlow can also automatically assign user roles based on the LDAP group membership. To import data that doesn't exist in FireFlow, create a custom field in FireFlow for this data.

Note: If both automatic creation of requestors upon authentication *and* importing user data from an LDAP server are enabled, then upon LDAP authentication, a requestor may be automatically created in FireFlow and assigned an AFA role.

In this case, the user will remain a requestor and not a privileged user, regardless of the AFA role assigned. For more details, see Enable or disable automatic user creation.

Note: A requestor cannot be converted to a privileged user and vice versa, by changing the user's roles via LDAP import. A user's system role is permanent.

Do the following:

1. In AFA, configure LDAP or RADIUS user authentication.

   You must select the **Fetch user data from LDAP** check box and complete the fields in the **Mapping to LDAP Fields** area.

2. To enable automatically assigning FireFlow roles to all members of an LDAP group, do the following:

   a. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.

   b. In the main menu, click **Configuration**.

      The **FireFlow Configuration** page appears.

   c. Click **Roles**.

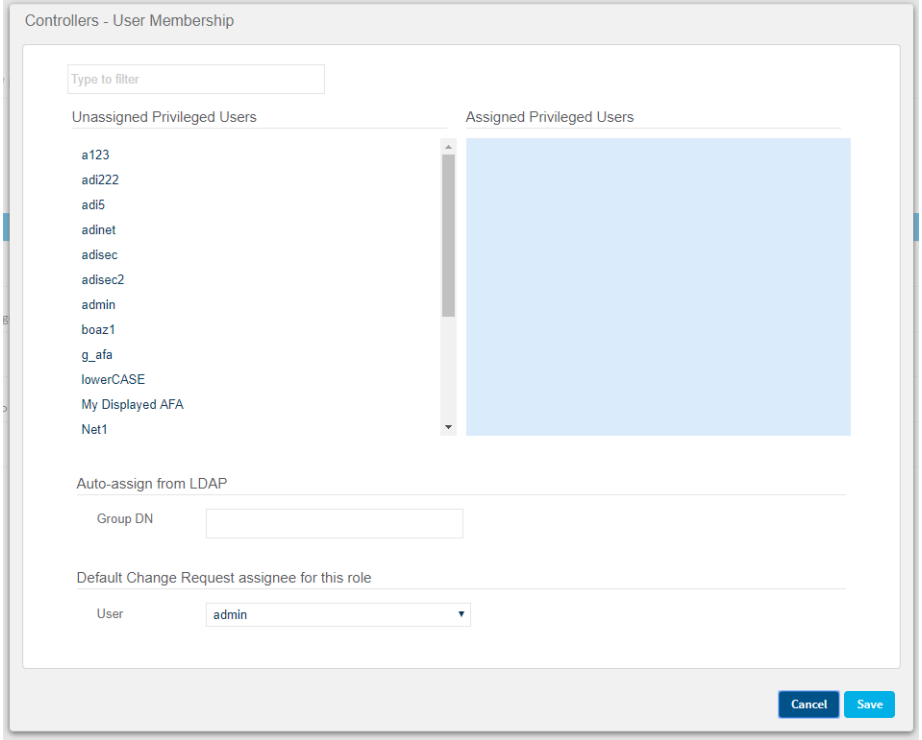
      The **Select a role** page appears.

   d. (Optional) To search for the desired role, type your search in the **Type to filter your results** field.

      The roles which match your search appear in the **Functional roles** area.

   e. In the row of the relevant role, click  .

      The **Users Assignment** window for the role you chose appears.



f. In the **Auto-assign from LDAP** area, in the **Group DN** field, type the name of the LDAP group.

g. Click **Save**.

All members of the specified LDAP group will automatically be assigned the role.

3. To import fields from the server to fields in FireFlow, do the following:

   a. For each field that exists on the server but not in FireFlow, add a custom field in FireFlow. For more details, see Manage custom fields.

   > **Note:** Do not add custom fields that have the same name as an existing field in FireFlow. Doing so will cause import from the server to fail.

   b. Map the fields on the server to fields in FireFlow by doing the following:

4. Switch to the AFA**Administration** area > **Advanced Configuration** tab.

   The **Advanced Configuration** page appears.

5. Click **Add**.

   The **Add New Configuration Parameter** dialog box appears.

6. In the **Name** field, type `LDAP_AttrCustom`.

7. In the **Value** field, type a list of custom FireFlow fields and the parallel LDAP fields in the following format:

   ```
   FF_Field1,LDAP_Attr1;FF_Field2,LDAP_Attr2;...
   ```

   Where:

   - `FF_FieldX` is the name of a user field in FireFlow to which you want to import data. This can be a fireflow field or a user-defined custom field.
   - `LDAP_AttrX` is the name of a user field on the LDAP server from which you want to export data.

   For example, in order to map a user-defined custom field called "Department" to an LDAP attribute called "department", include the following in the semi-colon delimited list:

   ```
   Department,department
   ```

8. Click **OK**.

9. Click **OK**.

Import LDAP or IDP user data (SSO)

When Authenticating with SSO, you can configure FireFlow to fetch user data from either the SSO response itself (from the IdP server), or from a separate call to an LDAP server. When fetching data from the IdP or LDAP server, you can retrieve data such as email or a phone number. When fetching data from an LDAP server, you can additionally retrieve group membership.

When fetching data from either an LDAP or IdP, you can map the imported data to the relevant field in FireFlow.

In AFA, configure SSO user authentication.

Select the **Fetch User Data** checkbox, choose the source of user data: **LDAP** or **IDP**, and complete the relevant fields.

Enable or disable automatic user creation

If RADIUS and/or LDAP authentication is configured, and a requestor who does not exist in FireFlow attempts to log in to FireFlow, FireFlow will check the inputted user credentials against the RADIUS or LDAP server. If the username and password pair exists in either database, then by default the requestor will be automatically added to the FireFlow local user database and logged in.

Note: If both automatic creation of requestors upon authentication *and* importing user data from an LDAP server are enabled, then upon LDAP authentication, a requestor may be automatically created in FireFlow and assigned a role in AFA or FireFlow. In this case, the user will remain a requestor and not a privileged user, regardless of the role assigned.

If desired, you can disable the automatic creation of requestors. Authenticated requestors will be logged in, without being added to the local user database.

Use the generic procedure for overriding system defaults, and define the following parameter:

Configuration Parameter Name	Value
`AutoCreateRequestors`	**0**. To disable automatic creation of requestors. **1**. To enable automatic creation of requestors. (Default)

For more details, see Override FireFlow system defaults.

Manage workflows

This section explains how to add, edit, and delete workflows in VisualFlow. It also explains how to modify the set of conditions determining when each workflow should be assigned.

VisualFlow enables you to add, edit, and delete custom workflows in a Web interface, without any need to manually edit the workflow XML files.

For details, see:

- Built-in workflows
- Get started in VisualFlow
- Manage workflows
- Manage workflow statuses
- Modify FireFlow stages
- Manage workflow actions
- Working with SLAs
- Apply / discard workflow changes
- Examples using VisualFlow
- Manage workflow options

VisualFlow Basics: Watch to learn about working with VisualFlow.

Built-in workflows

FireFlow assigns each change request to a workflow that controls the change request's lifecycle, including the actions that can be performed on the change request, the behavior associated with each action, and the possible change request statuses.

Default workflow selection

In order to determine which workflow to use for a change request, FireFlow performs the following steps:

1. FireFlow refers to the template that the requestor selected for the change request.
2. If the template specifies a workflow, FireFlow assigns the change request to that workflow.
3. If the template does not specify a workflow, then FireFlow refers to a set of conditions that determine which workflow should be assigned.
4. If FireFlow fails to assign a workflow based on the set of conditions, then FireFlow assigns the change request to the default workflow.

Built-In workflow reference

FireFlow comes with the following set of built-in workflows, located under `/usr/share/fireflow/local/etc/Workflows/`:

Workflow	File Name	Description	Lifecycle Stages
Basic	`Basic_Config.xml`	This is the default workflow, resulting in the default change request lifecycle. It is Used by traffic change requests.	• Request • Plan • Approve • Implement • Validate • Match • Resolved • Audit
Standard	`Standard_ Config.xml`	This workflow is used by traffic change requests. For installations older than version 6.5, this is the default workflow. Upgrading from v6.4 or below will not set the Basic workflow as the default.	• Request • Plan • Approve • Implement • Validate • Match • Resolved • Audit

Workflow	File Name	Description	Lifecycle Stages
Generic	`Generic_ Config.xml`	This workflow is used for change requests that are not related to traffic. As such, no device change planning or matching of device changes to the change request are required, and these stages (Plan and Match) are omitted.	• Request • Approve • Implement • Validate • Resolved • Audit
Multi-Approval	`Multi-Approval_ Config.xml`	This workflow is used for change requests that require approval from multiple users. It therefore includes an extra stage (Review) that is performed by a controller user.	• Request • Plan • Approve • Review • Implement • Validate • Match • Resolved • Audit
Parallel-Approval	`Parallel-Approval_ Config.xml`	This workflow is used for change requests that require approval from two users in parallel. It therefore includes an extra change request approval stage called Review that is performed by a controller.	• Request • Plan • Approve • Review • Implement • Validate • Resolved • Audit

Workflow	File Name	Description	Lifecycle Stages
Change-Object	`Change-Object_Config.xml`	This workflow is used for change requests for modifying device objects.	• Request • Plan • Approve • Implement • Validate • Resolved • Audit
Rule-Removal	`Rule-Removal_Config.xml`	This workflow is used for change requests that are for removing device rules.	• Request • Approve • Implement • Validate • Resolved
Rule-Modification	`Rule-Modification_Config.xml`	This workflow is used for requests that are for modifying a rule's source, destination, service or application fields.	• Request • Approve • Implement • Validate • Resolved
Web-Filter	`Web-Filter_Config.xml`	This workflow is used for change requests that are for filtering Web connections. It is relevant for Symantec Blue Coat devices only.	• Request • Plan • Approve • Implement • Validate • Match • Resolved • Audit

Workflow	File Name	Description	Lifecycle Stages
IPv6-Traffic	`IPv6-Traffic_Config.xml`	This workflow is used by traffic change requests with IPv6 traffic. **Note:** Many automated functionalities that are provided for IPv4 traffic are not supported for the IPv6 traffic workflow.	• Request • Plan • Approve • Implement • Validate • Match • Resolved • Audit
Automatic-Traffic-Change	`Automatic-Traffic-Change_Config.xml`	This workflow is used by traffic change requests with "allow" traffic only. All of the lifecycle stages proceed automatically.	• Request • Plan • Approve • Implement • Validate • Match • Resolved • Audit
Request-Recertification	`Request-Recertification_Config.xml`	This workflow is used to determine whether an Allow rule that was added to a device policy as the result of an expired traffic change request is still relevant. If the rule is no longer relevant, a rule removal request is created to remove it.	• Request • Approve • Implement • Validate • Resolved • Audit
Bulk-Rules-Addition	`Bulk-Rules-Addition_Config.xml`	This workflow is used for bulk rules addition, like populating a new device.	• Request • Plan • Implement • Match • Resolved • Audit

Workflow	File Name	Description	Lifecycle Stages
Bulk-Rule-Removal	`Bulk-Rule-Removal_Config.xml`	This workflow is used for bulk rule removal.	• Request • Plan • Implement • Match • Resolved • Audit
Object-Change-Multi-Device	`Object-Change-Multi-Device.xml`	This workflow is used for change requests for modifying device objects on multiple devices.	• Request • Plan • Approve • Implement • Validate • Resolved • Audit

You cannot modify the built-in workflows; however, you can create new ones as desired. For your convenience, FireFlow allows you to create variations of existing workflows (both built-in and custom ones), by duplicating the relevant workflow and then modifying it.

Furthermore, you can modify the set of conditions determining which workflow should be assigned, when the template does not specify a workflow.

Manage your workflows in VisualFlow. While workflows are XML files, we do not recommend making manual updates directly to the files, except where explicitly instructed.

Get started in VisualFlow

Relevant for: Administrators

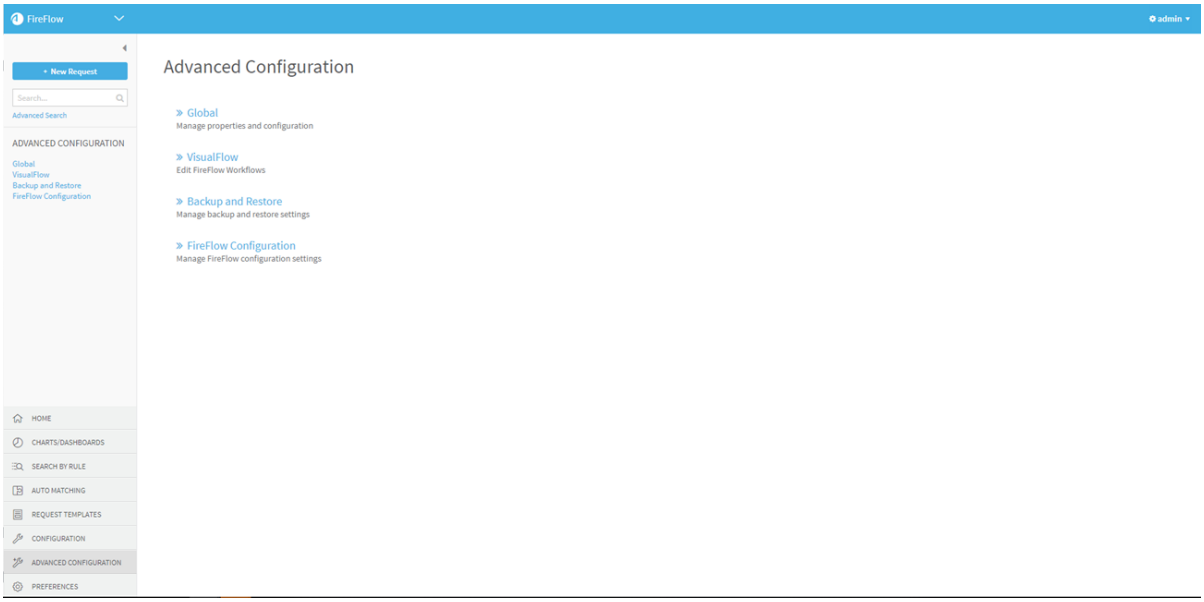
This section contains all the information you need in order to get started using VisualFlow.

Accessing VisualFlow

To access VisualFlow

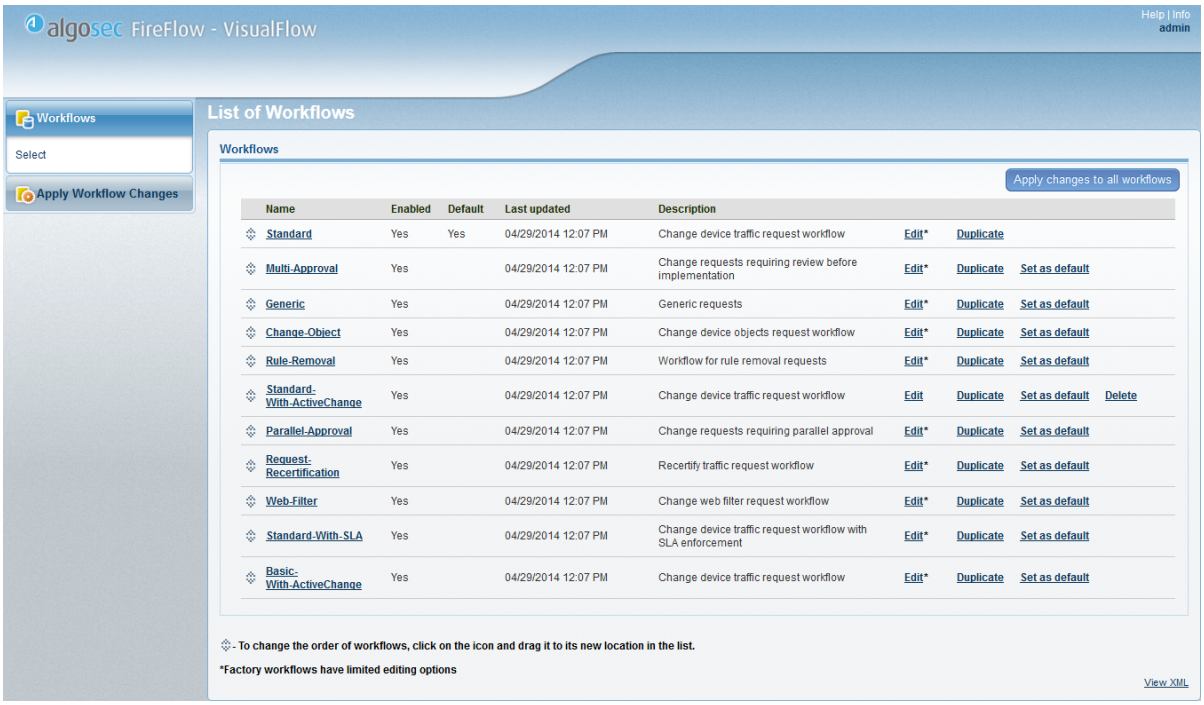
1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Advanced Configuration**.

   The **Advanced Configuration** page is displayed.



3. Click **VisualFlow**.

VisualFlow opens in a new browser tab, displaying the **List of Workflows** page.



The VisualFlow user interface consists of the following major elements:

- **Main menu:** Used for navigating between the VisualFlow pages.
- **Workspace:** Displays the VisualFlow page selected in the main menu. When viewing a specific workflow, the workspace includes the workflow's layout. For more details, see Manage workflows.
- **Toolbar:** Displays your username and a link to information about the VisualFlow version.

To exit VisualFlow, close the browser tab.

View workflow layouts

A workflow's *layout* is a graph that includes all actions and statuses in the workflow, each of which can be clicked for further viewing and editing.

To view a workflow layout

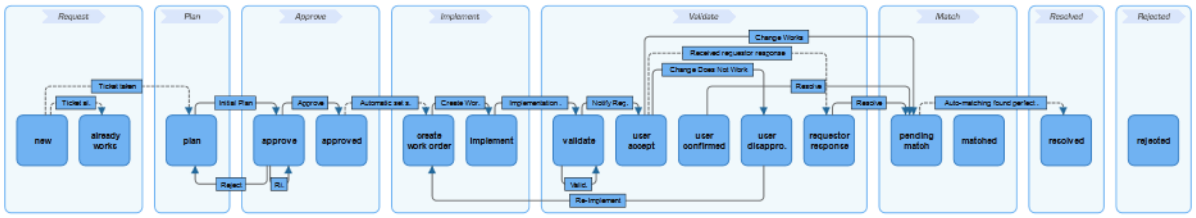
1. In the VisualFlow main menu, click **Workflows**.

   The **List of Workflows** page is displayed.

2. Do one of the following:

   - Click on the desired workflow's name.
   - Next to the desired workflow, click **Edit**.

   The **Edit Workflow** page opens with the workflow's details, and the **Layout** area displays the workflow's layout.



   For information on the various layout elements, click **Show legend** or see the following table.

3. To zoom in, click the  icon.

   The workflow layout is magnified. Use the scroll bar to view the desired part of the layout.

4. To zoom out, click the  icon.

   The workflow layout returns to its regular size.

5. To print the workflow layout:

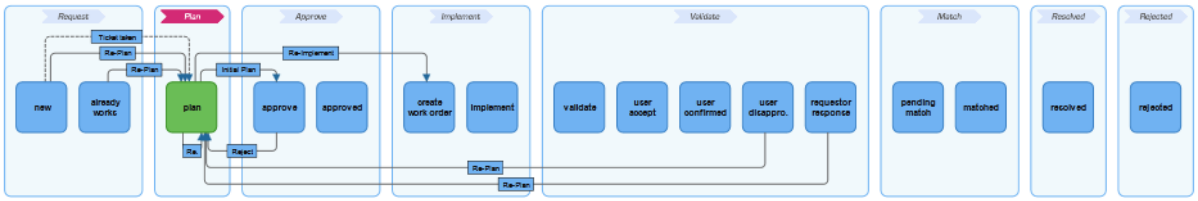
   a. Click  .

      The workflow layout opens in a new tab.

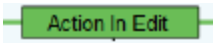
   b. Use your browser's Print button to print the layout.

6. To view only the layout elements that are related to a specific action or status, click on the desired action/status.

   The **Edit Action** or **Edit Status** page appears, and the **Layout** area displays only those elements that are directly related to the selected action/status.



Workflow Layout Elements

This element...	Represents...
	A single workflow stage.
	A status. Click to edit the status's details.
	A status that is currently being edited.
	An action.
	An action that is currently being edited.
	Indicates that an action can be clicked for editing.
	Indicates that an action cannot be clicked for editing.

This element…	Represents…
	A conditional action.
	A parallel action.

Manage workflows

This topic describes how to manage workflows created in VisualFlow.

Add workflows

Adding new workflows is done by creating a copy of an existing workflow and then modifying the copy.

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

   The **List of Workflows** page is displayed.

2. Next to an existing workflow on which you would like to base the new workflow, click **Duplicate**.

3. Click **OK**.

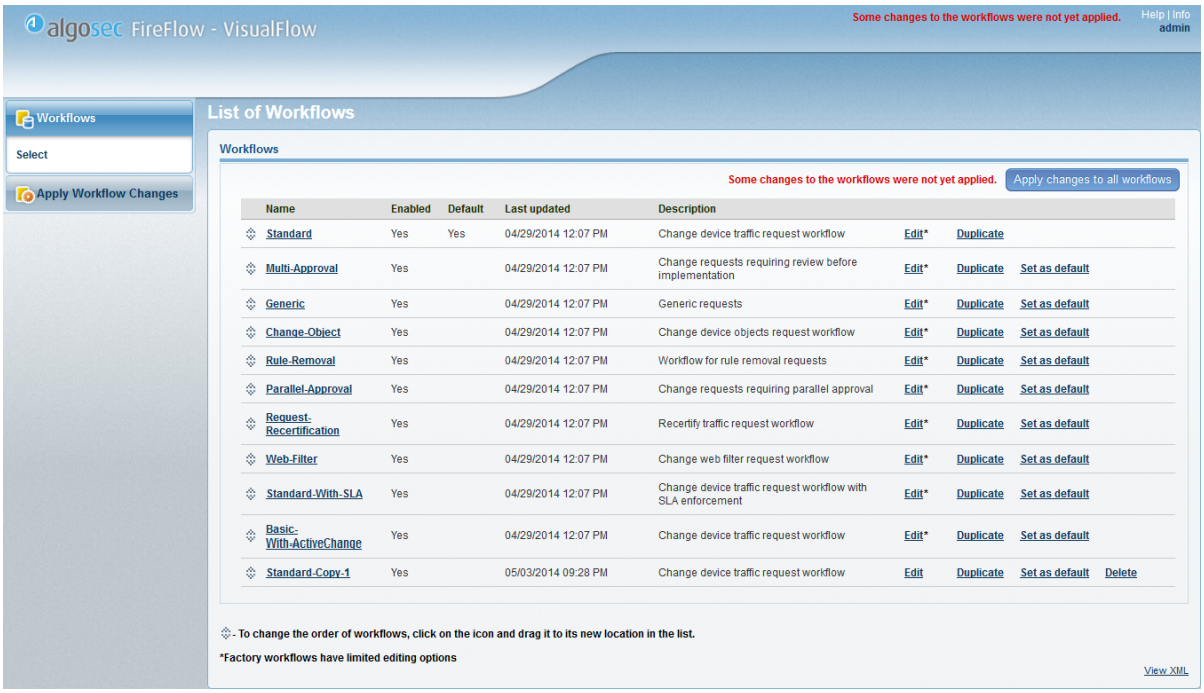
   A new workflow appears at the bottom of the workflows list. Its name is *OriginalWorkflow*-Copy-*Number*, where:

   - *OriginalWorkflow* is the name of the workflow you copied.
   - *Number* is a number used to differentiate between copies of the duplicated workflow.

   A confirmation message appears.

   Example

For example, if you duplicated the Standard workflow, and there is already a workflow called Standard-Copy-1, then the new workflow will be called Standard-Copy-2.

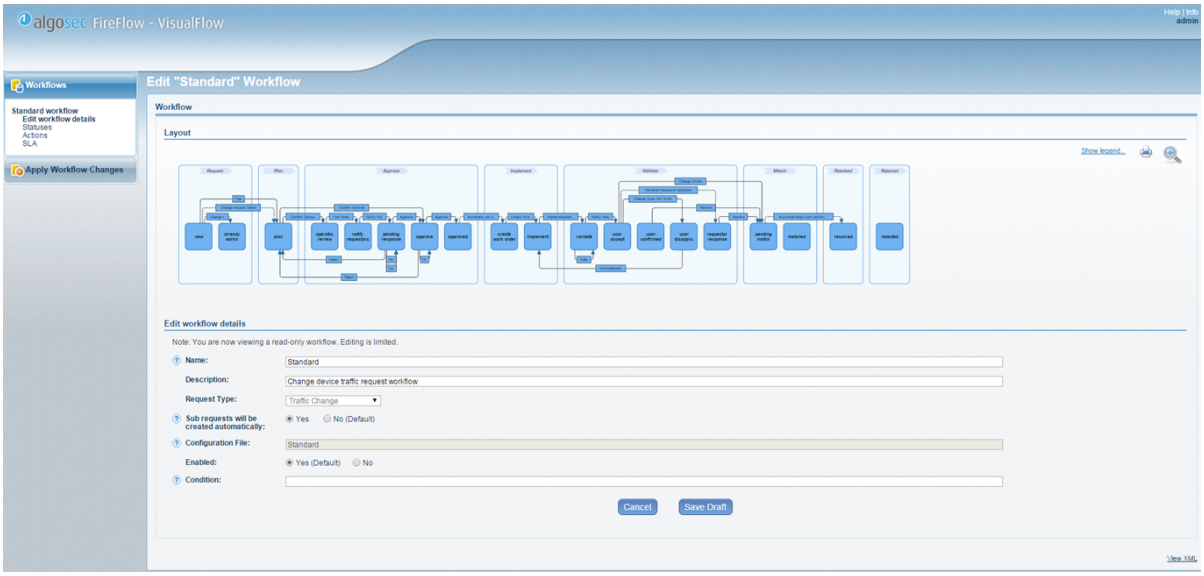


A message at the top of the screen informs you that changes have been made to the workflows.

4. Do one of the following:

   - Next to the new workflow, click **Edit**.
   - Click on the workflow's name.

   The **Edit Workflow** page opens with the workflow's details.



5. In the **Edit workflow details** area, complete the fields using the information in Workflow Details Fields (see Workflow Details Fields).
6. Click **Save Draft**.
7. Add, edit, and delete workflow statuses as desired.

   Continue with any of the following:

   - Manage workflow statuses
   - Modify FireFlow stages
   - Manage workflow actions
   - Working with SLAs
   - Apply / discard workflow changes

Workflow Details Fields

In this field...	Do this...
Name	Type a name for the workflow.
Description	Type a description of the workflow.

In this field...	Do this...
Request Type	Select the request type for the workflow. The workflow can only be used with request templates with the same request type. **Note:** After upgrading to version 6.6, please define request types for all custom workflows. While upgrading to versions 6.7 and higher, if there are workflows without specified request types, a warning appears.
Sub requests will be created automatically	Select this to create sub-requests automatically. This is relevant for Request type: Traffic change. This enables you to automatically create per-devices requests, after the Initial Plan stage, without having to wait for the results to be displayed.
Configuration File	Type a prefix for the workflow file name associated with this workflow. The workflow file is named *Prefix*`_Config.xml`, where *Prefix* is the string you enter in this field. By default, the prefix is the workflow's name.
Enabled	Specify whether this workflow should be enabled, by choosing one of the following: • **Yes**. The workflow is enabled and will appear in the FireFlow interface. • **No**. The workflow is disabled. It will not appear in the FireFlow interface, and no change requests will have this workflow. The default value is **Yes**.
Condition	Type the condition under which a workflow should be assigned to change requests, when the change request's template does not specify a workflow. For more details, see Workflow condition syntax.

Edit workflows

Note: You can edit the workflow details of built-in workflows; however, you cannot change their statuses and actions.

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

   The **List of Workflows** page is displayed.

2. Do one of the following:

   - Next to the new workflow, click **Edit**.
   - Click on the workflow's name.

   The **Edit Workflow** page opens with the workflow's details.

3. To edit the workflow's details, do the following:

   a. In the **Edit workflow details** area, complete the fields as needed. For details, see Workflow Details Fields.

   b. Click **Save Draft**.

   A message at the top of the screen informs you that changes have been made to the workflows.

Continue with any of the following:

- Manage workflow statuses
- Modify FireFlow stages
- Manage workflow actions
- Working with SLAs

Workflow condition syntax

A workflow's **Condition** field contains a query that specifies the condition under which the workflow should be assigned to change requests when the change request's template does not specify a workflow. The query is composed of pairs in the following format:

```
field = 'value'
```

Where `field` is a supported field in FireFlow, and `value` is the field's value. For example, the following query specifies that the change request priority must be "1":

```
Priority = '1'
```

You can use `!=` to indicate "not". For example, the following query specifies that the change request must not have a priority of "1":

```
Priority != '1'
```

It is possible to use Boolean operators between field-value pairs.

For example, the following query specifies that the change request priority must be "1", and the owner must be John Smith:

```
Priority = '1' AND Owner = 'John Smith'
```

For more intricate queries, you can use parentheses to group field-value pairs and operators. For example, the following query specifies that the change request priority must be "1" or "2", and the owner must be John Smith or Sue Michaels.

```
(Priority = '1' OR Priority = '2') AND (Owner = 'John Smith' OR Owner
= 'Sue Michaels')
```

Supported Fields

There are two types of supported fields:

- **Standard fields**. These fields should be written as they appear in Standard Fields (see Standard Fields). For example:

  ```
  Subject = 'Allow Web Access'
  ```

- **Custom fields.** These fields include those listed in Custom Fields (see Custom Fields), as well as any fields added by users. They should be used in the following format:

  ```
  'CF.{field}'
  ```

Where *field* is the name of the custom field.

For example:

```
'CF.{Firewall Brand}' = 'Check Point'
```

Standard Fields

Field	Description
Id	The change request ID number.
Subject	The change request subject.
Content	Text that appears in the original change request description or in a comment or reply added to the change request.
Content-Type	The file type of an attachment attached to the change request.
Filename	The filename of an attachment for the change request.
Status	The change request status.
Owner	The user who is the current change request owner.
Creator	The user who is the change request creator.
LastUpdatedBy	The user who last updated the change request.
Requestor.EmailAddress	The requestor's email address.
Requestor.Name	The requestor's username.
Requestor.RealName	The requestor's full name.
Requestor.Nickname	The requestor's nickname.
Requestor.Organization	The requestor's organization.
Requestor.Address1	The requestor's primary mailing address.
Requestor.Address2	The requestor's secondary mailing address.
Requestor.WorkPhone	The requestor's office telephone number.

Field	Description
Requestor.HomePhone	The requestor's home telephone number.
Requestor.MobilePhone	The requestor's mobile telephone number.
Requestor.PagerPhone	The requestor's pager telephone number.
Requestor.id	The requestor's ID.
Cc.EmailAddress	The email address of a user who receives copies of email messages for the change request.
Cc.Name	The username of a user who receives copies of email messages for the change request.
Cc.RealName	The full name of a user who receives copies of email messages for the change request.
Cc.Nickname	The nickname of a user who receives copies of email messages for the change request.
Cc.Organization	The organization of a user who receives copies of email messages for the change request.
Cc.Address1	The primary mailing address of a user who receives copies of email messages for the change request.
Cc.Address2	The secondary mailing address of a user who receives copies of email messages for the change request.
Cc.WorkPhone	The office telephone number of a user who receives copies of email messages for the change request.
Cc.HomePhone	The home telephone number of a user who receives copies of email messages for the change request.
Cc.MobilePhone	The mobile telephone number of a user who receives copies of email messages for the change request.
Cc.PagerPhone	The pager telephone number of a user who receives copies of email messages for the change request.
Cc.id	The ID of a user who receives copies of email messages for the change request.

Field	Description
Owner.EmailAddress	The owner's email address.
Owner.Name	The owner's username.
Owner.RealName	The owner's full name.
Owner.Nickname	The owner's nickname.
Owner.Organization	The owner's organization.
Owner.Address1	The owner's primary mailing address.
Owner.Address2	The owner's secondary mailing address.
Owner.WorkPhone	The owner's office telephone number.
Owner.HomePhone	The owner's home telephone number.
Owner.MobilePhone	The owner's mobile telephone number.
Owner.PagerPhone	The owner's pager telephone number.
Owner.id	The owner's ID.
Created	The date on which the change request was created.
Resolved	The date on which the change request was resolved.
Last.Updated	The date on which the change request was last updated.
Due	The change request's due date.
Priority	The change request's priority.
RefersTo	The ID numbers of change requests to which this change request refers, separated by spaces.
ReferredToBy	The ID numbers of change requests that refer to this change request, separated by spaces.

Custom Fields

Field	Description
Expires	The date on which this change request will expire.
Requested Source	The IP address, IP range, network, or device object, as specified in the original request.
Requested Destination	The IP address, IP range, network, device object, as specified in the original request.
Requested Service	The device service or port for the connection, as specified in the original request.
Requested Action	The device action to perform for the connection, as specified in the original request.
Requested Source NAT	The source NAT value to which the connection's source should be translated, as specified in the original request.
Ticket Template Name	The name of the change request's template.
Requested Destination NAT	The destination NAT value to which the connection's destination should be translated, as specified in the original request.
Requested Port Translation	The port value to which the connection's port should be translated, as specified in the original request.
Workflow	The workflow assigned to the change request.
Owning Role	The user role that currently owns the change request.
Requested NAT Type	The type of NAT (**Static** or **Dynamic**), as specified in the original request.
CMS ticket id	The ID number of a related change request in an external change management system that is integrated with FireFlow.
Firewall Name	The name of the device.
Firewall IP Address	The IP address of the device.
Firewall Brand	The device vendor.

Field	Description
Firewall Management Server	The device management server name.
Firewall Policy	The device security policy.
Firewall Last Report	The last report generated for the device.
Firewall Last Report Date	The date and time at which the last report for this device was generated.
Change Description	The change description.
Change Source	The IP address, IP range, network, or device object, as planned during the Plan stage.
Change Destination	The IP address, IP range, network, or device object, as planned during the Plan stage.
Change Service	The device service or port for the connection, as planned during the Plan stage.
Change Action	The device action to perform for the connection, as planned during the Plan stage.
Change Source NAT	The source NAT value to which the connection's source should be translated, as planned during the Plan stage.
Change Destination NAT	The destination NAT value to which the connection's destination should be translated, as planned during the Plan stage.
Change Port Translation	The port value to which the connection's port should be translated, as planned during the Plan stage.
Change NAT Type	The type of NAT (**Static** or **Dynamic**), as planned during the Plan stage.
Change Implementation Notes	The words that appear in the change request's implementation notes, if the change request has completed the Implement stage.

Field	Description
Request Risk Check Result	The number and/or and severity of risks that implementation of the planned change would entail.
Initial Plan Result	The results of initial planning.
Form Type	The type of form used for the change request (**Traffic Change**, **Object Change**, or **Generic Change**).
Change Validation Result	The results of change validation.
Risks Number	The number of risks detected for the planned change, if the change request has completed the risk check in the Approve stage.
Risks Details	Details about the risks detected for the planned change, if the change request has completed the risk check in the Approve stage.
Translated Source	The change request's source, as translated to IP addresses.

Requested Object Action	The requested action in an object change request.
	• For network objects on non-Check Point devices, this can have the following values:
	  • `AddIPsToObject`
	  • `RemoveIPsFromObject`
	  • `NewObject`
	  • `DeleteObject`
	• For service objects or network objects on Check Point devices, this can have the following values:
	  • `AddValuesTo`
	  • `RemoveValuesFrom`
	  • `New`
	  • `Edit`
	  • `Delete`

Field	Description
Translated Destination	The change request's destination, as translated to IP addresses.

Change Object Action	The action for an object change request, as specified during the Plan stage.
	• For network objects on non-Check Point devices, this can have the following values:
	  • `AddIPsToObject`
	  • `RemoveIPsFromObject`
	  • `NewObject`
	  • `DeleteObject`
	• For service objects or network objects on Check Point devices, this can have the following values:
	  • `AddValuesTo`
	  • `RemoveValuesFrom`
	  • `New`
	  • `Edit`
	  • `Delete`

Translated Service	The change request's service, as translated to ports.
Requested Object Name	An object's name, as specified in the original object change request.
Automatically Implemented	An indication of whether the requested change should be automatically implemented.
Change Object Name	An object's name, as specified for an object change request in the Plan stage.
Already Works Firewalls	The devices on which the requested change already works.
Requested IPs To Add	The IP addresses or protocols to add to an object, as specified in the original object change request.

Field	Description
Change IPs To Add	The IP addresses or protocols to add to an object, as specified for an object change request in the Plan stage.
Requested IPs To Remove	The IP addresses or protocols to remove from an object, as specified in the original object change request.
Change IPs To Remove	The IP addresses or protocols to remove from an object, as specified for an object change request in the Plan stage.
Requested Object Scope	The object scope, as specified in the original object change request.
Change Object Scope	The object scope, as specified for an object change request in the Plan stage.
Is Work Order Editable	An indication of whether the work order is editable.
Is Active Change Applicable	An indication of whether ActiveChange can be used to implement the requested change.
Object Change Validation Result	The results of object change validation.
Create tickets from attachment	An indication of whether the change request was created from a file.
Affected Rules Result	The device rules that are affected by a suggested object change request.
Firewall Provider-1	The name or IP address of the MDSM managing the device. This field is relevant for Check Point devices only.

Supported Boolean Operators

Supported boolean operators include the following:

Operator	Description
AND	Both of the field-value pairs joined by this operator must be true. In the following example, the condition is only met for new change requests owned by John Smith: `Status = 'new' AND Owner = 'John Smith'`
OR	One or both of the field-value pairs joined by this operator must be true. In the following example, the condition is met for change requests that are new, change requests that are owned by John Smith, and new change requests owned by John Smith: `Status = 'new' OR Owner = 'John Smith'`

Workflow conditions example

In the following example, the workflow will be assigned when the change request's template does not specify a workflow, and one of the following conditions are met:

- The change request's priority is greater than 7.
- The requestor's email address includes the string "company.com".
- The value of the custom field called "Project" is "Infrastructure".

```
(Priority > 7) OR (Requestor.EmailAddress LIKE 'company.com')
OR ('CF.{Project}' = 'Infrastructure')
```

Reorder workflows

You can control the order in which workflows appear in VisualFlow.

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

   The **List of Workflows** page is displayed.
2. In the list of workflows, click  next to a workflow you want to move, and drag it to the desired location in the list.

Setting a default workflow

When FireFlow fails to assign a workflow based on a change request's template or workflow conditions, it automatically uses the default workflow.

Only one workflow can be the set as the default workflow. By default, the Basic workflow is the default workflow.

Note: For FireFlow installations v6.4 and older, the default workflow is the Standard workflow. Upgrading from v6.4 or below will not set the Basic workflow as the default.

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

   The **List of Workflows** page is displayed.
2. Next to the desired workflow, click **Set as default**.
3. Click on the workflow's name.

The workflow is marked as the default workflow in the **Default** column.

Delete workflows

Note: You cannot delete built-in workflows. For more details, see Built-in workflows.

Note: If you delete a workflow, then any change requests that are assigned to that workflow will be re-assigned to the default workflow the next time they are accessed. Furthermore, if their current status does not exist in the default workflow, the change requests will transition to the "new" status.

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

   The **List of Workflows** page is displayed.

2. Next to the desired workflow, click **Delete**.

   A confirmation message appears.

3. Click **OK**.

The workflow is deleted.

A message at the top of the screen informs you that changes have been made to the workflows.

Manage workflow statuses

Relevant for: Administrators

You can add, edit, reorder, and delete statuses in a workflow.

Add workflow statuses

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

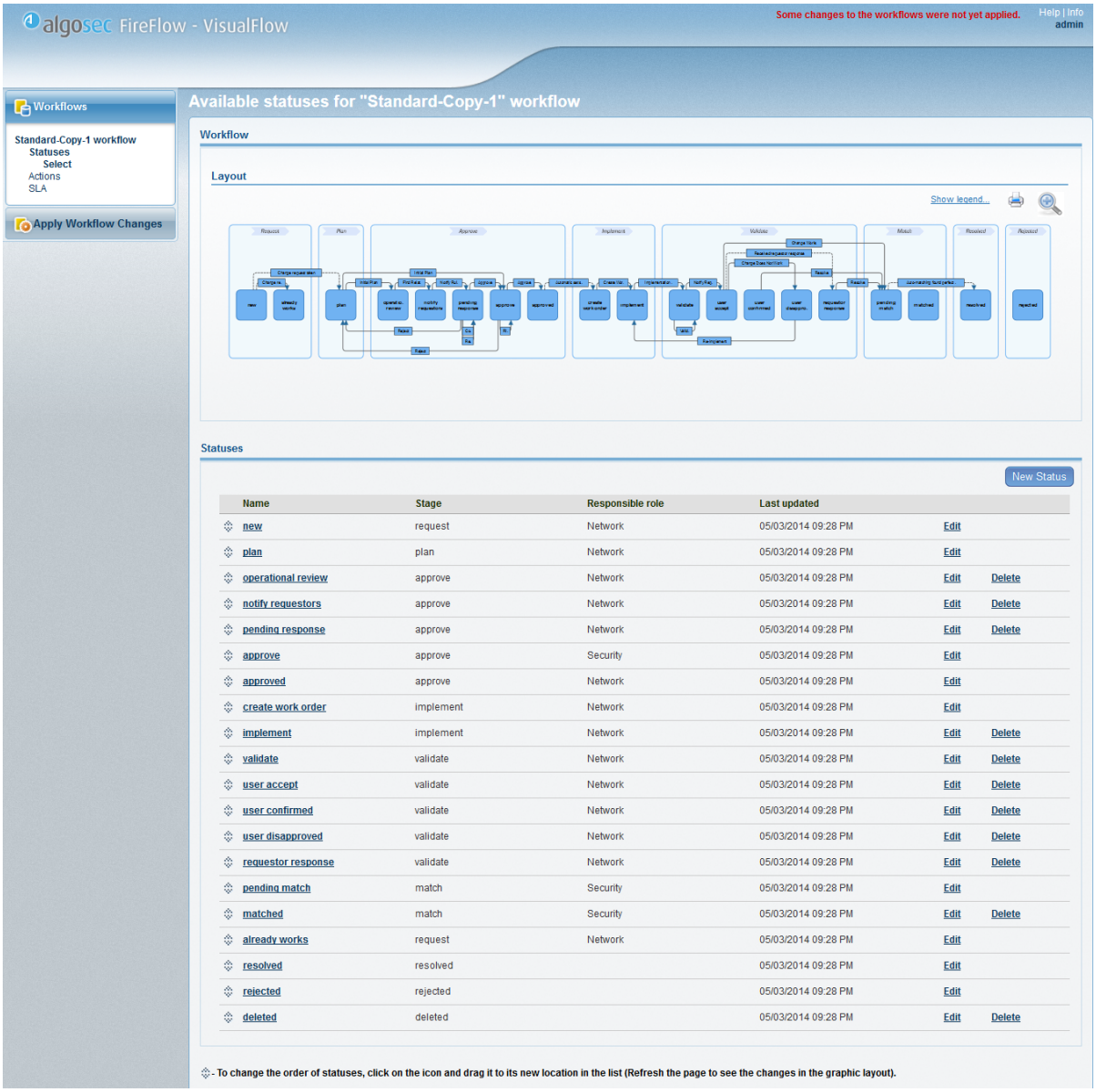
   The **List of Workflows** page is displayed.

2. Next to the desired workflow, click **Edit**.

   The **Edit Workflow** page opens with the workflow's details.

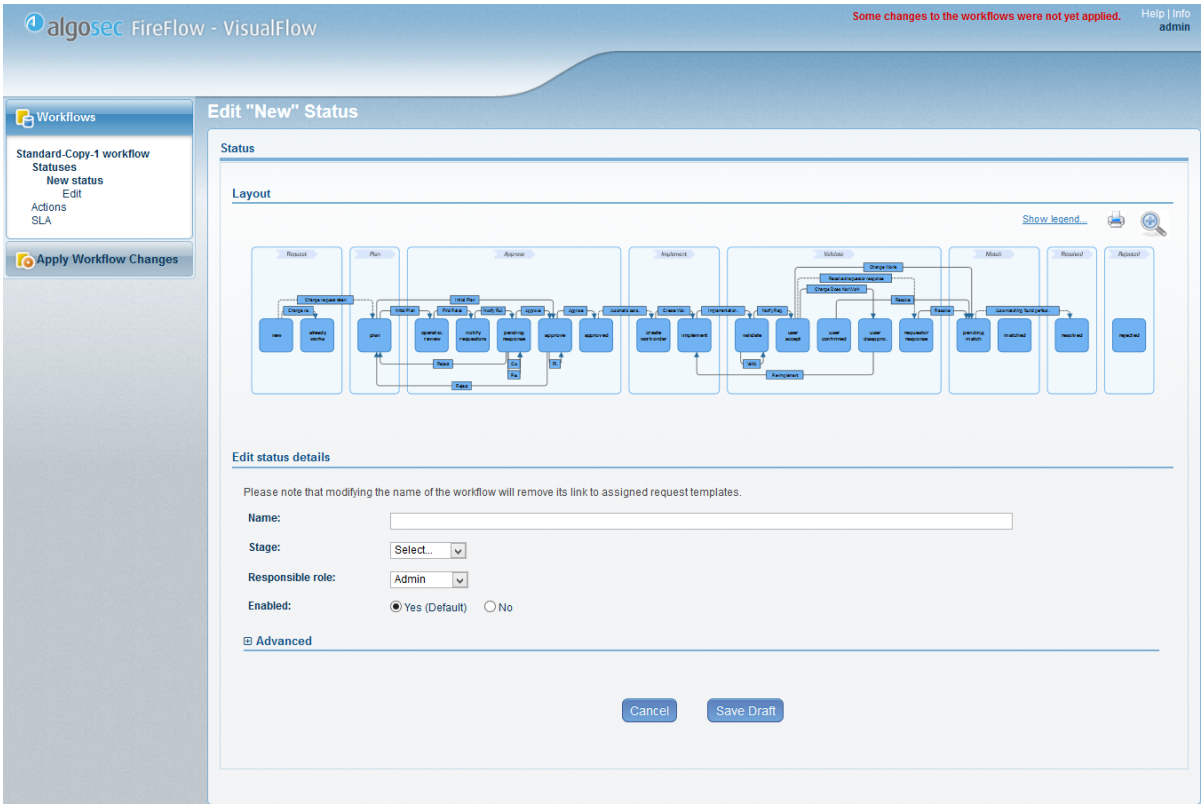
3. In the VisualFlow main menu, click **Statuses**.

   The **Available statuses** page is displayed.



4. Click **New Status**.

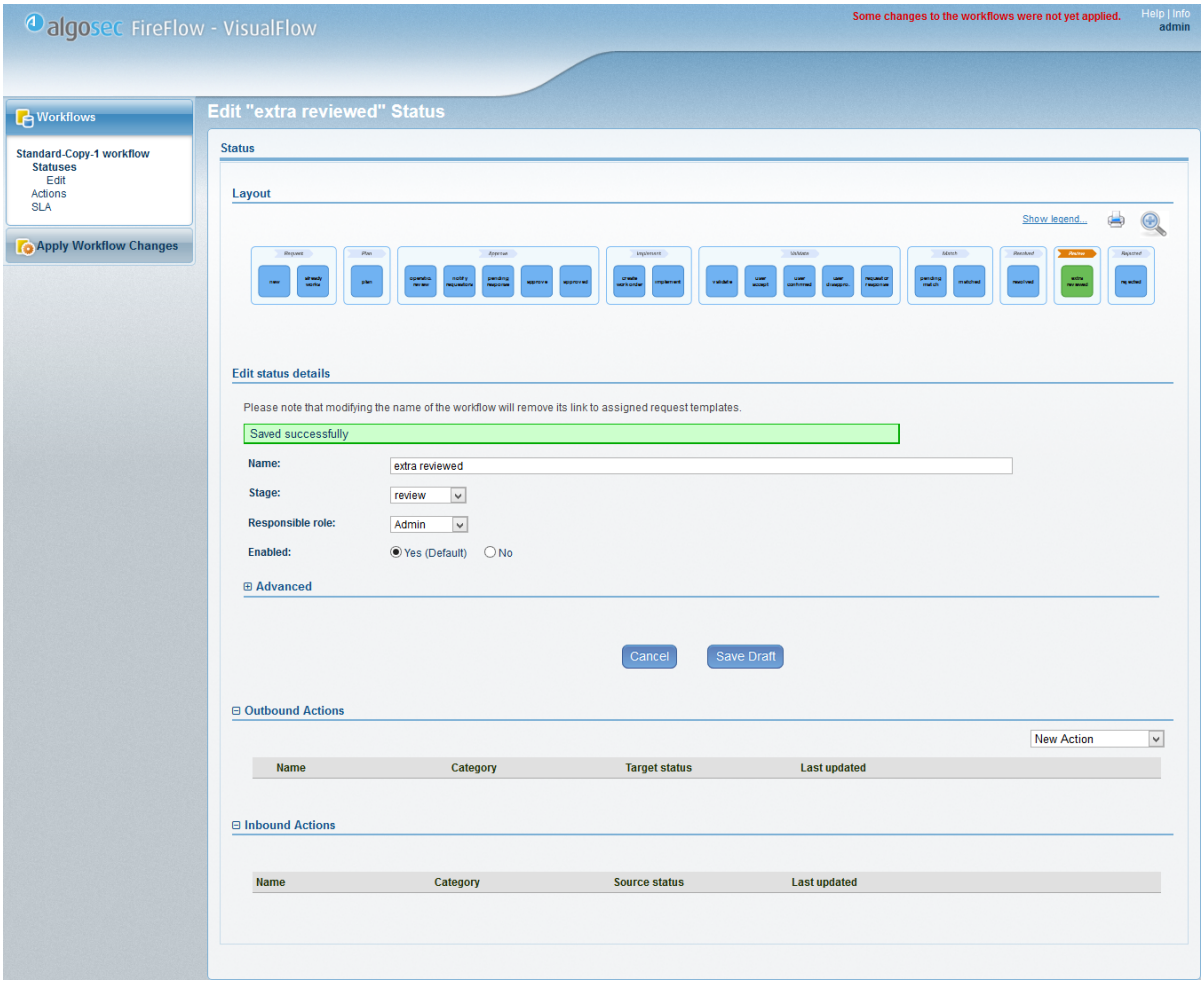
The **Edit Status** page is displayed.



5. Complete the fields using the information in Status Fields (see Status Fields).
6. Click **Save Draft**.

   The status is added to the workflow's list of available statuses and to the workflow.

   The **Outbound Actions** and **Inbound Actions** areas are displayed.



7. Add, edit, or delete actions for this status. For details, see Manage workflow actions.
8. Click **Save Draft**.

The status is added to the workflow's list of available statuses and to the workflow.

Status Fields

In this field...	Do this...
Name	Type the name of the status as it appears in the FireFlow interface. This is also a unique key. The name can include up to 50 characters of the Latin character set. Spaces are allowed. This field is mandatory. **Note:** Some statuses cannot be renamed. When editing such a status, this field is read-only.
Stage	The name of the image used in the lifecycle diagram at the top of the change request page. This field is mandatory. For more details, see Modify FireFlow stages.
Responsible role	Select the single user role responsible for change requests in this status. **Note**: Usually, this role is configured to see these change requests in its **Home** page. For more details, see Customize the FireFlow Home page. When an action is performed on the change request, and the action transitions the change request to a new status for which the change request owner is not responsible, the change request is re-assigned to the default assignee of the new status's responsible role, and the current user is re-directed to their **Home** page. If you want to designate a new responsible role for the status, first create the role in the FireFlow **Configuration** page, then access VisualFlow again. The new role will appear in this list, and you can select it. This field is mandatory.
Additional responsible roles	All user roles that are responsible for change requests in this status, other than the role specified in the **Responsible role** field. This field is read-only, and it only appears for statuses that are the source status of a parallel action.

In this field...	Do this...
Enabled	Specify whether this status should be enabled, by choosing one of the following: • **Yes:** The status is enabled and will appear in the FireFlow interface. • **No:** The status is disabled. It will not appear in the FireFlow interface, and no change requests will have this status. The default value is **Yes**. **Note:** Some statuses cannot be disabled. When editing such a status, this field either does not appear or is read-only.
Advanced	Expand this area to display the **Advanced** fields.
Allow editing traffic fields	Specify whether it is possible to plan the change when a change request is in this status. Planning the change involves modifying any of the following fields: • Source • Destination • Service • Action • NAT Choose one of the following: • **Yes:** These fields can be modified. • **No:** These fields cannot be modified. The default value is **No**.

In this field...	Do this...
Allow editing device	Specify whether it is possible to change the device when a change request is in this status. Choose one of the following: • **Yes:** The device can be modified. • **No:** The device cannot be modified. The default value is **Yes**. **Note:** For object change requests, this field will always behave as it is set to yes when the **Allow editing traffic fields** field is set to yes, and no when the **Allow editing traffic fields** field is set to no.
Next status when mail or comment is received from requestor	Select the *next* status to assign the change request, when incoming correspondence from the change request's unprivileged requestor to the change request occurs. If this field is not set, then the change request status will not change upon incoming correspondence. This field only appears for statuses where an email response is possible.
Await Requestor's Response	Specify whether a change request should appear in the **Change Requests Awaiting Response** page for unprivileged users. The default value is **No**.
Mark change request as closed	Specify whether a change request in this status is considered "closed", by choosing one of the following: • **Yes:** Consider the change request "closed", and display it in the **Closed Change Requests** tab in the FireFlow requestor interface. • **No:** Do not consider the change request "closed". The default value is **No**. This field does not appear for the "new" status.

In this field...	Do this...
Stage still incomplete	Specify whether there are additional statuses that a change request must achieve before completing the stage, by choosing one of the following: • **Yes:** There are additional statuses that a change request must achieve before completing this stage. • **No:** This is the last status in the stage. The stage will be marked with a check mark. The default value is **No**. This field must be set to **No** for exactly one status per stage.
Display Initial Plan Results	Specify whether to display initial plan results at this stage, by choosing one of the following: • **Yes:** Display initial plan results at this stage. • **No:** Do not display initial plan results at this stage. The default value is **No**.
Display Risk Check Results	Specify whether to display risk check results at this stage, by choosing one of the following: • **Yes:** Display risk check results at this stage. • **No:** Do not display risk check results at this stage. The default value is **No**.
Display Create Work Order Results	Specify whether to display the work order at this stage, by choosing one of the following: • **Yes:** Display the work order at this stage. • **No:** Do not display the work order at this stage. The default value is **No**.

In this field...	Do this...
Display Validation Results	Specify whether to display the validation results at this stage, by choosing one of the following: • **Yes:** Display the validation results at this stage. • **No:** Do not display the validation results at this stage. The default value is **No**.
Perform Active Change Automatically	Specify wheter FireFlow should automatically initiate active change at this stage, by choosing one of the following: • **Yes:** Automatically perform active change at this stage. • **No:** Do not automatically perform active change at this stage. The default value is **No.** This field only appears for the "implement" status.
Status after new	Select the status to which the change request should transition after it has been assigned an owner. This field only appears for the "new" status.

Edit workflow statuses

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

   The **List of Workflows** page is displayed.

2. Do one of the following:

   - Click on the desired workflow's name.
   - Next to the desired workflow, click **Edit**.

   The **Edit Workflow** page opens with the workflow's details.

3. Do one of the following:

   - To go directly to the desired status, click the status in the workflow layout.
   - To select the status from a list of statuses:

i. In the VisualFlow main menu, click **Statuses**.

   The **Available statuses** page is displayed.

ii. Next to the desired status, click **Edit**.

   The **Edit Status** page is displayed.

4. Complete the fields as needed. For details, see Status Fields .

   If you expanded the **Advanced** area, additional fields appear.

5. Add, edit, or delete actions for this status.

6. Click **Save Draft**.

Reorder statuses

You can control the order in which statuses appear in a workflow's list of available statuses.

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

   The **List of Workflows** page is displayed.

2. Do one of the following:

   - Click on the desired workflow's name.
   - Next to the desired workflow, click **Edit**.

   The **Edit Workflow** page opens with the workflow's details.

3. In the VisualFlow main menu, click **Statuses**.

   The **Available statuses** page is displayed.

4. In the list of statuses, click  next to a status you want to move, and drag it to the desired location in the list.

Delete statuses

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

   The **List of Workflows** page is displayed.

2. Do one of the following:

   - Click on the desired workflow's name.
   - Next to the desired workflow, click **Edit**.

   The **Edit Workflow** page opens with the workflow's details.

3. In the VisualFlow main menu, click **Statuses**.

   The **Available statuses** page is displayed.

4. Next to the desired status, click **Delete**.

   A confirmation message appears.

   Note: Some statuses cannot be deleted. These statuses do not have a **Delete** link next to them.

   Note: If a status is the source or target of an action, or if the status is used in one or more SLOs, you must disassociate those actions/SLOs from the status before you can delete it.

   For details, see Manage workflow actions and Working with SLAs .

5. Click **OK**.

The status is deleted from the workflow's list of available statuses and from the workflow.

Modify FireFlow stages

This topic describes how to modify FireFlow stages (tabs).

Do the following:

1. Export VF workflows into XML files (Apply changes to all workflows button).
2. Edit the relevant workflow XML file in **/usr/share/fireflow/local/etc/site/Workflows/** using an editor.

   Near the end you'll see the <images> tag.

   These are the stages (tabs). There are possibly different stages when the ticket is in different statuses. Below you will see the standard workflow for traffic ticket. When the ticket is rejected it only has 4 stages (tabs). When it is deleted it has no stages (tabs). Otherwise, the default is 7 stages (tabs). You can add an 8th one there.

   ```
   <images>
   <currentStatus name="default">
   <image name="new" />
   <image name="open" />
   <image name="check" />
   <image name="implement" />
   <image name="validate" />
   <image name="reconcile" />
   <image name="resolved" />
   </currentStatus>
   <currentStatus name="rejected">
   <image name="new" />
   <image name="open" />
   <image name="check" />
   <image name="rejected" />
   </currentStatus>
   <currentStatus name="deleted" />
   </images>
   ```

3. Import XML files into WF (**Discard all changes** button).
4. Continue working normally in VF. For each status you will be able to choose the new stage you added in the **Stage** drop-down menu.

Manage workflow actions

Add workflow actions

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

   The **List of Workflows** page is displayed.

2. Do one of the following:

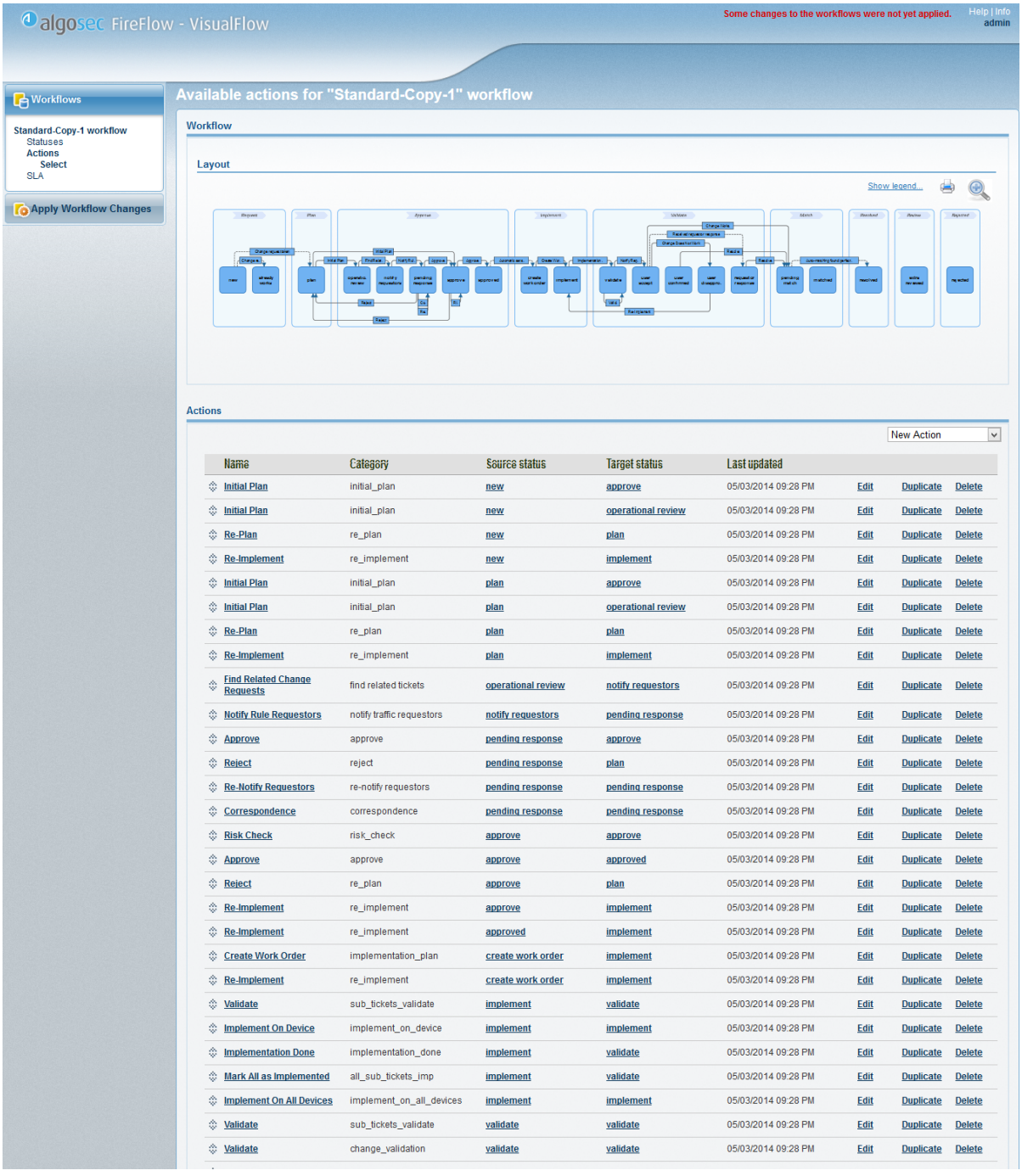
   - Click on the desired workflow's name.
   - Next to the desired workflow, click **Edit**.

   The **Edit Workflow** page opens with the workflow's details.

3. Do one of the following:

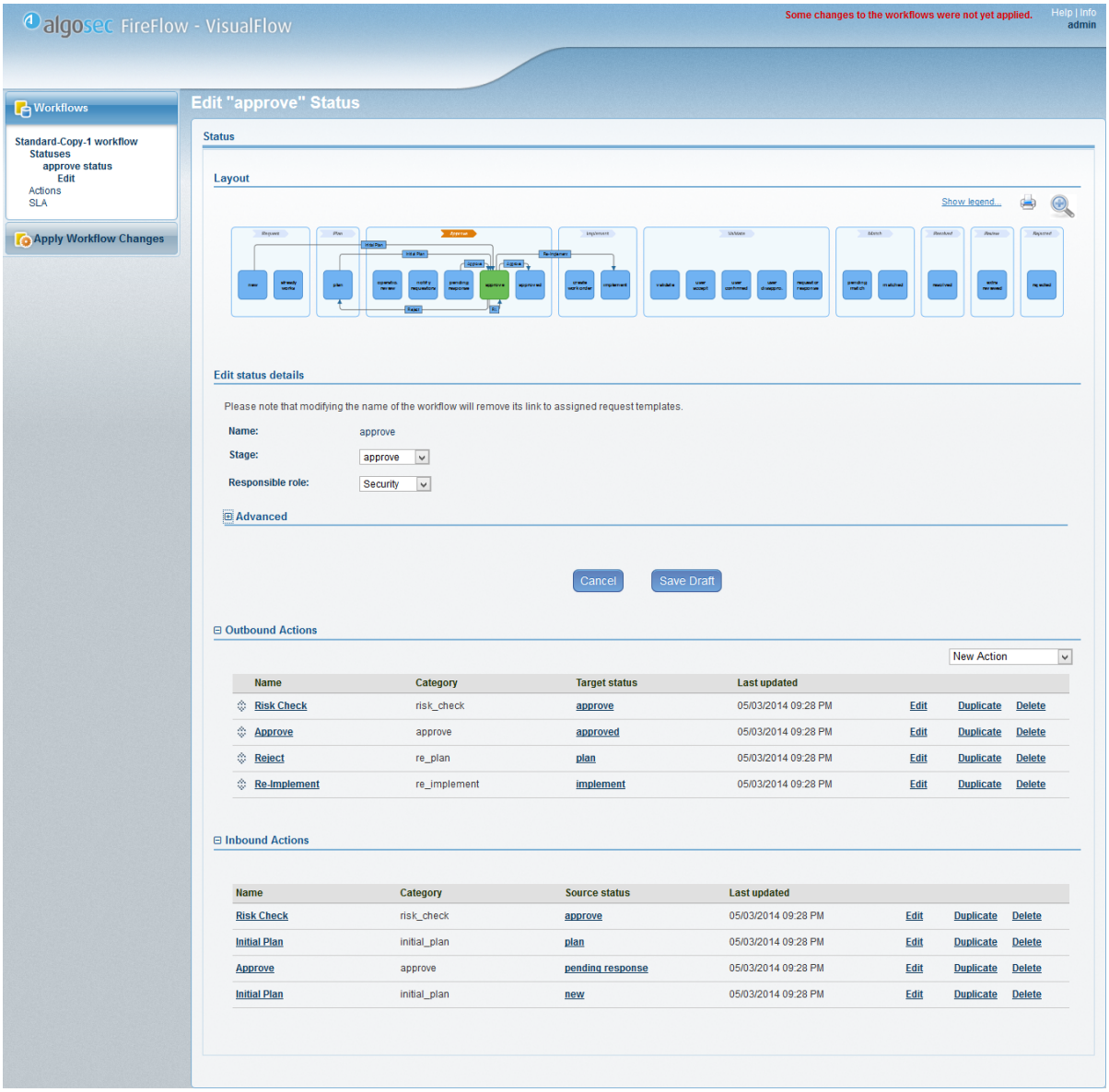
   In the VisualFlow main menu, click Actions.

   The **Available actions** page is displayed with a list of actions used in the workflow.



In the workflow layout, click on a status to which you want to add an action.

The **Edit Status** page is displayed with a list of inbound and outbound actions for the status.



4. Do one of the following:

   Add a new action from scratch, in the New Action drop-down list, select the new action's type

   An action's type describes what it does. For more details, see Action Type.

   Add a new action that is based on an existing action

1. Next to the desired existing action, click **Duplicate**.

   A confirmation message appears.

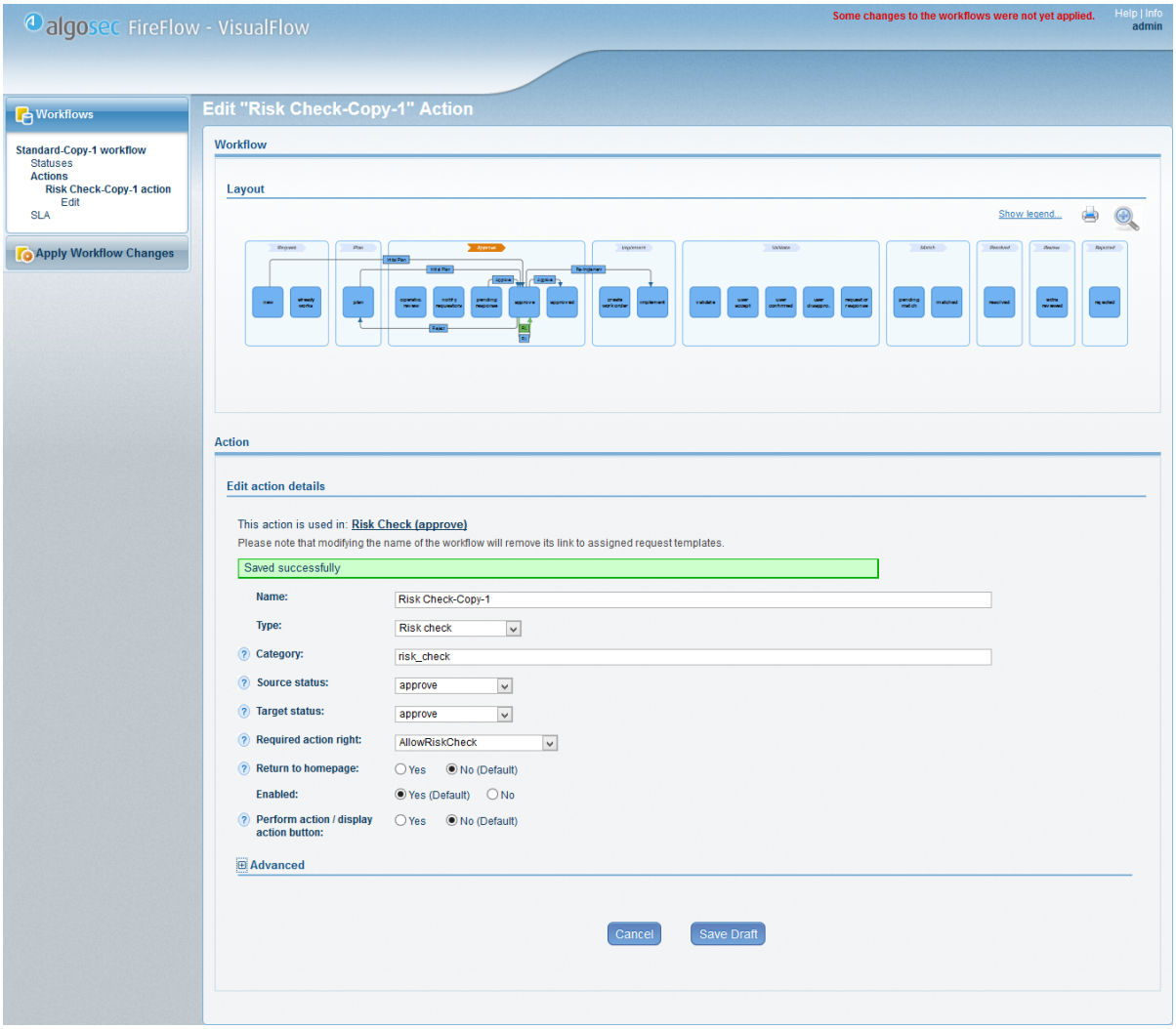
2. Click **OK**.

   The new action is named *OriginalAction*-Copy-*Number*, where:

   - *OriginalAction* is the name of the action you copied.
   - *Number* is a number used to differentiate between copies of the duplicated action.

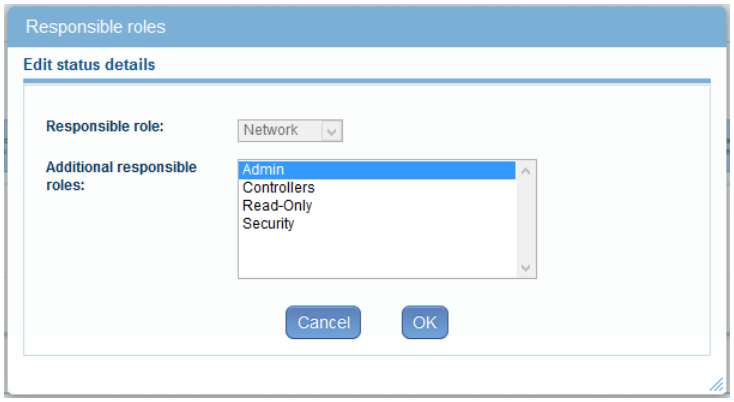
For example, if you duplicated an action called Risk Check, and there is already an action called Risk Check-Copy-1, then the new action will be called Risk Check-Copy-2.

The **Edit Action** page is displayed.



5. Complete the fields using the information in Action Fields (see Action Fields).
6. If you set the **Parallel** field to **Yes**, set the action's responsible roles by doing the following:
    a. Click the **Set responsible roles** link.

        The **Responsible roles** dialog box appears.



The **Responsible role** field displays the user role responsible for change requests in this status.

b. In the **Additional responsible roles** list, select the additional user roles responsible for change requests in this status.

To select multiple user roles, press **Ctrl** while you click on the desired user roles.

c. Click **OK**.

7. Click **Save Draft**.

The action is added to the list of actions.

Action Type

This action type...	Does this...
Change status	Changes the status of the change request.
Internal comment	Adds a comment to the change request that is hidden from the requestor.
Reply to user	Adds a comment to the change request that is seen by the requestor. Includes sending an email to the requestor. Includes sending an email to the requestor.
Modify custom field	Allows a user to modify one or more custom fields.

This action type...	Does this...
Authenticate with custom field	Allows a user to modify one or more custom fields as "Modify custom field" action, but in addition it requests from the user to re-enter their password and verify it. Fill in this action with the following data: Category: approve Source status: approve Target status: approved Required action right: AllowApprove All check-boxes with label that include "display action button": select "Yes" Modify Field Title: type title Field Name: select fields.
Take ownership	Assigns the user ownership of a change request.
Assign	Allows a user to assign ownership of a change request to another user.
Initial plan	Performs initial planning. Relevant only for traffic change requests. It is recommended to consult with AlgoSec before using this action type.
Risk check	Performs a risk check. Relevant only for traffic change requests. It is recommended to consult with AlgoSec before using this action type.
Implementation plan	Creates a work order. It is recommended to consult with AlgoSec before using this action type.
Manual reconcile	Opens a dialog box that allows a user to manually match the change request with a change record. Relevant only for traffic change requests. It is recommended to consult with AlgoSec before using this action type.

This action type...	Does this...
No change record	Opens a dialog box that allows a user to manually match the change request, while specifying that there is no associated change record. Relevant only for traffic change requests. It is recommended to consult with AlgoSec before using this action type.
Change validation	Performs validation of a traffic change request. Relevant only for traffic change requests. It is recommended to consult with AlgoSec before using this action type.
Review work order	Enables a user to view an existing work order and edit it. Relevant controls will appear in the UI only for Check Point and Juniper devices. Relevant only for traffic change requests. It is recommended to consult with AlgoSec before using this action type.
Active change	Enables a user to implement planned changes via ActiveChange. Relevant controls will appear in the UI only for supported devices and supported workflows.
Object change validation	Performs validation of an object change request. Relevant only for object change requests. It is recommended to consult with AlgoSec before using this action type.
Affected rules	Finds affected rules for an object change request. Relevant only for object change requests. It is recommended to consult with AlgoSec before using this action type.
Related tickets	Finds change requests that are related to a change request. Relevant only for rule removal requests. It is recommended to consult with AlgoSec before using this action type.

This action type...	Does this...
Notify requestors	Enables a user to notify other users regarding the impending removal/disablement of a device rule. Relevant for rule removal requests only. It is recommended to consult with AlgoSec before using this action type.
View correspondence	Allows a user to view correspondences with other users regarding the impending removal/disablement of a device rule. Relevant only for rule removal requests. It is recommended to consult with AlgoSec before using this action type.
Rule removal validation	Performs validation of a rule removal request. Relevant only for rule removal requests. It is recommended to consult with AlgoSec before using this action type.

Action Fields

In this field...	Do this...
Name	A unique key value for the action. Used when the action's behavior is to be overridden for a specific status. This field is mandatory. It is only available when working with a workflow's list of actions.
Type	Select the action's type, which describes what it does. See Action Types (see Action Type). This field is mandatory. It is only available when working with a workflow's list of actions.
Category	Type the action's category. You can create categories and assign similar actions to them. When editing an action, the **Edit action details** area will display links to other actions belonging to the same category.

In this field...	Do this...
Source status	Use the fields in this area to specify the status or statuses from which the change request must transition, before this action can be performed.
Target status	Use the fields in this area to specify the status or statuses to which the change request will transition when the action is performed.
Required action permission	Specify whether the user must be granted a specific permission, in order for the action to appear for each change request in a drop-down list, by selecting the relevant permission. **Note:** This is a cosmetic issue only. Actions that require the user to have a specific permission will not succeed if the user does not have the permission.
Return to homepage	Specify whether the user should be re-directed to the **Home** page after executing the action, by choosing one of the following: • **Yes:** Redirect the user to the **Home** page. • **No:** The user should remain on the current page. The default value is **No**.
Enabled	Specify whether this action should be enabled, by choosing one of the following: • **Yes:** The action is enabled and will appear in the FireFlow interface. • **No:** The action is disabled and will not appear in the FireFlow interface. The default value is **Yes**.

In this field...	Do this...
Perform action/ display action button	Specify whether the action should be available via an explicit button, by choosing one of the following: • **Yes:** Make the action available via a button. The button will always be visible. • **No:** Do not make the action available via a button. The default value is **No**. **Note:** When the **Risk check** and **Implementation plan** actions are configured to run asynchronously, there is no action button for these actions, and this field specifies whether asynchronous computation should begin when the change request reaches the source status of the action. This is the default configuration.
Advanced	Expand this area to display the **Advanced** fields.
Conditional target status	Use the fields in this area to specify a set of conditional target statuses that the change request can transition to. FireFlow will check the conditions in the order listed; therefore, if the first condition is met, FireFlow will not check the second condition, and so on. If none of the conditions are met, the change request will transition to the status specified in the **Edit action details** area's **Target status** field, by default.
Target status	Select a new status that the change request should transition to when the action is performed, if the condition(s) in the **Condition** field are met.
Condition	Type an XQL query specifying the conditions under which the change request will transition to the status specified in the **Target Status** field. For example, to specify the condition that the number of risks must be zero, type: `Ticket[RisksNumber = "0"]` For more details, see Action condition syntax.
Message to user	Type a message that should appear onscreen when transitioning to the new status.

In this field...	Do this...
+	Click this button to add another conditional target status.
Parallel	Specify whether the action will be performed in parallel to a second, identical action. Choose one of the following: • **Yes:** The action will be performed in parallel to a second, identical action. • **No:** The action will be performed sequentially to all other actions. The default value is **No**. It is possible to add more parallel action logic. For details, see Add parallel action logic. This field is enabled only for statuses of the following types: **Change status**, **Internal comment**, and **Reply to user**.
action completed when	The strategy used to determine whether the parallel action has been completed. To specify that the action should be considered completed only when all responsible roles have performed it, select **all**. If desired, you can configure other strategies. For example, you can configure a strategy specifying that if a specific role performs the action, then the action should be considered completed; otherwise, FireFlow should wait for all other roles to perform the action. For information on configuring additional strategies, contact AlgoSec.
Perform action/ display action button when field is empty	Specify whether the action should be available via an explicit button *only if* a specific change request field is empty, by selecting the relevant change request field. **Note:** When the **Risk check** and **Implementation plan** actions are configured to run asynchronously, there is no action button for these actions, and this field specifies whether asynchronous computation should begin when the change request reaches the source status of the action if the specific change request field is empty at that time. This is the default configuration.

In this field...	Do this...
Display action button when current user is the owner	Specify whether the action should be available via an explicit button *only if* the current user is the change request's owner. Choose one of the following: • **Yes:** Display the action button if the current user is the change request's owner. • **No:** Do not make displaying the action button dependent on whether the current user is the change request's owner. The default value is **No**. **Note:** When the **Risk check** and **Implementation plan** actions are configured to run asynchronously, there is no action button for these actions, and this field specifies whether asynchronous computation should begin when the change request reaches the source status of the action (regardless of the current user). This is the default configuration.
Display action button when current user is not the owner	Specify whether the action should be available via an explicit button *only if* the current user is *not* the change request's owner. Choose one of the following: • **Yes:** Display the action button if the current user is not the change request's owner. • **No:** Do not make displaying the action button dependent on whether the current user is the change request's owner. The default value is **No**. **Note:** When the **Risk check** and **Implementation plan** actions are configured to run asynchronously, there is no action button for these actions, and this field specifies whether asynchronous computation should begin when the change request reaches the source status of the action (regardless of the current user). This is the default configuration.

In this field...	Do this...
Perform action/ display action button when change request is unassigned	Specify whether the action should be available via an explicit button *only if* the change request is not assigned to a user. Choose one of the following: • **Yes:** Display the action button if the change request is not assigned to a user. • **No:** Do not make displaying the action button dependent on whether the change request is assigned to a user. The default value is **No**. **Note:** When the **Risk check** and **Implementation plan** actions are configured to run asynchronously, there is no action button for these actions, and this field specifies whether asynchronous computation should begin when the change request reaches the source status of the action, if the change request is not assigned to a user at that time. This is the default configuration.
Perform action/ display action button when field value is true	Specify whether the action should be available via an explicit button *only if* a specific change request field's value is "true", by selecting the relevant change request field. **Note:** When the **Risk check** and **Implementation plan** actions are configured to run asynchronously, there is no action button for these actions, and this field specifies whether asynchronous computation should begin when the change request reaches the source status of the action, if the specific change request field's value is "true" at that time. This is the default configuration.

In this field...	Do this...
Perform action/ display action button when field value is one of the values listed	Specify whether the action should be available via an explicit button *only if* a specific change request field's value is one of the values in the comma separated list of values. **Note:** When the **Risk check** and **Implementation plan** actions are configured to run asynchronously, there is no action button for these actions, and this field specifies whether asynchronous computation should begin when the change request reaches the source status of the action if the specific change request field's value is one of the values in the list at that time. This is the default configuration.
Modify Field Title	Type the message that should appear when this action is performed, instructing the user to complete the field specified in the **Field Name** field. This field is only relevant if the **Type** field's value is **Modify custom field**.
Display action button if condition is true	Type an XQL query specifying the conditions under which the action should be available via an explicit button. You can use the variable `__CurrentUser__` to specify that a value in the condition should be the current user. For example, to specify that the requestor is not the current user, type: `Ticket[Requestor/EmailAddress != "__CurrentUser__"]` For more details, see Action condition syntax.
Field Name	If the action requires a field's value as input, select the field's name. To select multiple fields, hold down the **CTRL** key while clicking on the desired fields. This field is only relevant if the **Type** field's value is **Modify custom field**.

In this field...	Do this...
Display in workflow layout	Specify whether the action should be displayed in the workflow layout when viewing a workflow, by choosing one of the following: • **Yes:** Display the action in the workflow layout. • **No:** Do not display the action in the workflow layout. The default value is **No**. **Note:** When viewing a status for which this action is an outbound action, the action will be displayed in the workflow layout, regardless of this attribute's value.
Applies to change requests of type	Select the check boxes next to the types of change requests for which the action is relevant, and for which the action should appear. This can be one or more of the following: • **Regular:** The action is relevant to regular change requests. A regular change request is relevant to only one device. • **Parent:** The action is relevant to parent requests. A parent request is relevant to multiple devices and has a sub-request for each device. • **Sub request:** The action is relevant to sub-requests. A sub-request is relevant to one device, out of the multiple devices that are relevant to its parent request. If you do not select any of the check boxes, the action will be relevant to all change request types.
User confirmation needed	Specify whether a confirmation message should appear when a user performs the action, by choosing one of the following: • **Yes:** Display a message when the action is performed. • **No:** Do not display a message when the action is performed. The default value is **No**.

In this field...	Do this...
Mail content	Type the default text that will appear in the main message box when commenting on a change request or replying to the user. This field is relevant only for actions of the type **Reply to user** and **Internal comment**.
Set 'auto-matching status'	Specify whether after the action is performed, the change request's "auto-matching status" should be set to a specific value, and the change request should be displayed in the **Auto Matching** page, by selecting the relevant status. The default value is **No**.
Traffic fields required	Specify whether certain change request fields are mandatory, in which case if the fields are not filled in when the action is performed, a message will appear prompting the user to fill them in. The fields in question are: • Source • Destination • Service • Action • Firewall Choose one of the following: • **Yes:** These fields are mandatory. • **No:** These fields are optional. The default value is **No**.
Hide from 'Other' actions menu	Specify whether the action should *not* appear for each change request in a drop-down list. Choose one of the following: • **Yes:** Hide this action in the drop-down list. • **No:** Display this action in the drop-down list. The default value is **No**.

In this field...	Do this...
Allow this action for unprivileged users	Specify whether unprivileged users should be allowed to perform this action, by choosing one of the following: • **Yes:** Allow unprivileged users to perform this action. • **No:** Do not allow unprivileged users to perform this action. The default value is **No**.
Return to parent request	Specify whether after the action is performed on a sub-request, the user should be redirected to the parent request, by choosing one of the following: • **Yes:** Redirect the user to the parent request. • **No:** The user should remain on the current page. The default value is **No**.
Return to homepage and display sub requests	Specify whether after the action is performed on a parent request, the user should be redirected to the **Home** page, which displays a list of the parent request's sub-requests. Choose one of the following: • **Yes:** Redirect the user to the **Home** page with a list of the parent request's sub-requests. • **No:** The user should remain on the current page. The default value is **No**. This field is relevant only for actions of the type **Change status**, **Reply to user** and **Internal comment**.

In this field...	Do this...
Display action button when the user is assigned to the responsible role	Specify whether the action should be available via an explicit button *only if* the current user is assigned the responsible role. Choose one of the following: • **Yes:** Display the action button if the current user is assigned the responsible role. • **No:** Do not make displaying the action button dependent on whether the current user is in the responsible role. The default value is **No**. **Note:** When the **Risk check** and **Implementation plan** actions are configured to run asynchronously, there is no action button for these actions, and this field specifies whether asynchronous computation should begin when the change request reaches the source status of the action (regardless of the current user). This is the default configuration.

Action condition syntax

In order to specify a condition under which a change request will transition to a new status when an action is performed, you must compose an XQL query. The XQL query can include the following:

Elements	An element may be any node in the XML of a change request, called a *flat ticket*. A flat ticket's root node is `<Ticket>`, which is written in an XQL query as `Ticket`.
	In order to specify a sub-node, use "/". For example, to specify a flat ticket's `<Firewall>` node, write:
	`Ticket/Firewall`
	You can use an asterisk "*" to specify a wildcard. For example, to specify any sub-node of `Firewall`, write:
	`Ticket/Firewall/*`

Filters	In order to apply a condition to an element, use square brackets "[ ]" in the following format:
	`Element[condition]`
	Where `condition` is a sub-query specifying the desired condition.
	For example, to specify that the device brand must be Juniper Netscreen, write the following:
	`Ticket/Firewall[Brand = "Juniper Netscreen"]`

Comparison operators	Elements in a sub-query may be compared via comparison operators in the following format:
	`element operator "value"`
	Where `operator` is a supported comparison operator, and `value` is the element's desired value.
	In the previous example, the sub-query used the = operator as follows:
	`Brand = "Juniper Netscreen"`

Boolean operators	It is possible to use Boolean operators inside a sub-query. For example, the following query specifies that the change request must be assigned to the Standard workflow, and the status must be "new":
	`Ticket[Workflow = "Standard" $and$ Status = "new"]`
	For more intricate queries, you can use parentheses to group comparisons inside a sub-query. For example, the following query specifies that the change request must be assigned to the Standard workflow, and the change request status must be "new" or "plan".
	`Ticket[Workflow = "Standard" $and$ (Status = 'new' $or$ Status = 'plan')]`

Flat Ticket Nodes

The following table lists the standard flat ticket nodes in alphabetical order.

Note: These nodes represent the various change request fields.

If you configured custom fields, there will also be a node for each custom field, and those nodes can be used as elements in XQL queries.

Flat Ticket Node reference

Node	Description	Sub-nodes
Action	The action to perform for the connection. Sub-node of `PlannedTraffic` and `RequestedTraffic`.	If inclusion of user-defined custom traffic fields in flat tickets is enabled, then this node will have the following sub-nodes: • Value. • A node for each custom field. Each such node will have its own Value sub-node. See Enabling/Disabling Inclusion of User-Defined Custom Traffic Fields in Flat Tickets (see Enable / disable inclusion of user-defined custom traffic fields in flat tickets).
AffectedRulesResult	The device rules that will be affected by the requested change. Sub-node of `Ticket`. **Note:** Relevant for object change requests only.	None

Node	Description	Sub-nodes
AlreadyWorksFirewalls	The names of devices on which the requested change already works. Sub-node of `Ticket`. **Note:** Relevant for traffic change requests only.	None
AutomaticallyImplemented	Indicates whether the requested change should be automatically implemented. Sub-node of `Ticket`. **Note:** Relevant for traffic change requests only.	None
Brand	The device vendor. Sub-node of `Firewall`.	None

Node	Description	Sub-nodes
Cc	Email addresses to which the FireFlow system will send copies of all email messages regarding this request. Sub-node of `Ticket`.	None
ChangeFullData	The change description. Sub-node of `Ticket`.	None
ChangeImplementationNotes	The change request's implementation notes, if the change request has completed the Implement stage. Sub-node of `Ticket`. **Note:** Relevant for traffic change requests only.	None

Node	Description	Sub-nodes
City	The city in which the change request owner or requestor is located, depending on the parent node. Sub-node of `Owner` and `Requestor`.	None
ClosedAt	The date and time when the change request was closed. Sub-node of `Ticket`.	None
CMSticketid	The ID number of a related change request in an external change management system that is integrated with FireFlow. Sub-node of `Ticket`.	None

Node	Description	Sub-nodes
code	The code number of a risk. Sub-Node of `Risk`. **Note:** Relevant for traffic change requests only.	None
Country	The country in which the change request owner or requestor is located, depending on the parent node. Sub-node of `Owner` and `Requestor`.	None
Created	The date and time when the change request was created. Sub-node of `Ticket`.	None

Node	Description	Sub-nodes
Createticketsfromattachment	Indicates whether the change request was created from a file. Sub-node of `Ticket`.	None
Description	The description of the change request. Sub-node of `Ticket`.	None
description	The description of a risk. Sub-Node of `Risk`. **Note:** Relevant for traffic change requests only.	None

Node	Description	Sub-nodes
Destination	The IP address, IP range, network, or device object. Sub-node of `PlannedTraffic` and `RequestedTraffic`. **Note:** Relevant for traffic change requests only.	If inclusion of user-defined custom traffic fields in flat tickets is enabled, then this node will have the following sub-nodes: • Value. • A node for each custom field. Each such node will have its own Value sub-node. See Enabling/Disabling Inclusion of User-Defined Custom Traffic Fields in Flat Tickets (see Enable / disable inclusion of user-defined custom traffic fields in flat tickets).
Due	The date by which this change request should be resolved. Sub-node of `Ticket`.	None
EmailAddress	The email address of the change request owner or requestor, depending on the parent node. Sub-node of `Owner` and `Requestor`.	None

Node	Description	Sub-nodes
Expires	The date on which this change request will expire. Sub-node of `Ticket`.	None
Firewall	Information about the device on which the change will be implemented, if the change request has completed the Plan stage. Sub-node of `Ticket`.	• Brand • IPAddress • LastReport • LastReportDate • ManagementServer • Name • Policy
FormType	The change request's form type (Traffic Change / Object Change / Generic Change). Sub-node of `Ticket`.	None

Node	Description	Sub-nodes
HomePhone	The home telephone number of the change request owner or requestor, depending on the parent node. Sub-node of `Owner` and `Requestor`.	None
Id	The ID number of the change request or the change request owner, depending on the parent node. Sub-node of `Ticket` and `Owner`.	None
ImplementaionDate	The date on which the change request was implemented. Sub-node of `Ticket`.	None

Node	Description	Sub-nodes
InitialPlanStartTime	The amount of time that has elapsed since initial planning, in UNIX time. Sub-node of `Ticket`.	None
IPAddress	The IP address of the device. Sub-node of `Firewall`.	None
IsActiveChangeApplicable	Indicates whether ActiveChange can be used to automatically implement the requested change. Sub-node of `Ticket`. **Note:** Relevant for traffic change requests only.	None
IsWorkOrderEditable	Indicates whether the work order is editable. Sub-node of `Ticket`.	None

Node	Description	Sub-nodes
LastReport	The last report generated for the device. Sub-node of `Firewall`.	None
LastReportDate	The date and time at which the last report for this device was generated. Sub-node of `Firewall`.	None
LastUpdated	The date and time when the change request was last updated. Sub-node of `Ticket`.	None
LastUpdatedBy	The username of the person who last updated the change request. Sub-node of `Ticket`.	None
ManagementServer	The name of the device's management server. Sub-node of `Firewall`.	None

Node	Description	Sub-nodes
Name	The name of the device. Sub-node of `Firewall`.	None
name	The name of a risk. Sub-Node of `Risk`. **Note:** Relevant for traffic change requests only.	None
New	Indicates whether the change request is new. Sub-node of `Ticket`.	None

Node	Description	Sub-nodes
NewValues	The IP addresses or protocols to add to the device object. Sub-node of `PlannedTraffic` and `RequestedTraffic`. **Note:** Relevant for object change requests only.	None
ObjectChangeValidationResult	The results of object change validation. Sub-node of `Ticket`. **Note:** Relevant for object change requests only.	None

Node	Description	Sub-nodes
ObjectName	The name of the device object. Sub-node of `PlannedTraffic` and `RequestedTraffic`. **Note:** Relevant for object change requests only.	None
Organization	The organization to which the change request owner or requestor belongs, depending on the parent node. Sub-node of `Owner` and `Requestor`.	None
Owner	The change request owner's username and email address. Sub-node of `Ticket`.	• City • Country • EmailAddress • HomePhone • Id • Organization • RealName

Node	Description	Sub-nodes
OwningGroup	The name of the user role that currently owns the change request. Sub-node of `Ticket`.	None
PlannedTraffic	The changes planned during the Plan stage. Sub-node of `Ticket`.	• Action • Destination • NewValues • ObjectName • Requestedaction • RuleDisplayId • RuleId • RuleRemovalRelatedTickets • RuleRemovalRelatedTickets Requestors • RuleRemovalRuleAction • RuleRemovalUserstoNotify • Scope • Service • Source • ValuesToRemove
Policy	The device security policy. Sub-node of `Firewall`.	None

Node	Description	Sub-nodes
Priority	A number indicating this request's priority, where 0 indicates lowest priority. Sub-node of `Ticket`.	None.
RealName	The full names of the change request owner or requestor, depending on the parent node. Sub-node of `Owner` and `Requestor`.	None
Requestedaction	The action the user selected to perform on the rule (remove or disable). Sub-node of `PlannedTraffic` and `RequestedTraffic`. **Note:** Relevant for rule removal requests only.	None

Node	Description	Sub-nodes
RequestedTraffic	The changes requested during the Request stage. Sub-node of `Ticket`.	• Action • Destination • NewValues • ObjectName • Requestedaction • RuleDisplayId • RuleId • RuleRemovalRelatedTickets • RuleRemovalRelatedTickets Requestors • RuleRemovalRuleAction • RuleRemovalUserstoNotify • Scope • Service • Source • ValuesToRemove
Requestor	Information about the requestor. Sub-node of `Ticket`.	• City • Country • EmailAddress • HomePhone • Organization • RealName

Node	Description	Sub-nodes
Risk	A risk that implementation of the planned change would entail. Sub-node of `RiskDetails`. **Note:** Relevant for traffic change requests only.	• code • description • name • severity
RisksDetails	The results of the risk check, if the change request has completed the Check stage. Sub-node of `Ticket`. **Note:** Relevant for traffic change requests only.	• Risk

Node	Description	Sub-nodes
RisksNumber	The total number of risks that implementation of the planned change would entail. Sub-node of `Ticket`. **Note:** Relevant for traffic change requests only.	None
RuleDisplayId	The rule ID as displayed to users. Sub-node of `PlannedTraffic` and `RequestedTraffic`. **Note:** Relevant for rule removal requests only.	None

Node	Description	Sub-nodes
RuleId	The rule ID as displayed in reports. Sub-node of `PlannedTraffic` and `RequestedTraffic`. **Note:** Relevant for rule removal requests only.	None
RuleRemovalRelatedTickets	FireFlow change requests with traffic that intersects that of the rule slated to be removed/disabled. Sub-node of `PlannedTraffic` and `RequestedTraffic`. **Note:** Relevant for rule removal requests only.	None

Node	Description	Sub-nodes
RuleRemovalRelatedTickets Requestors	The requestors of FireFlow change requests with traffic that intersects that of the rule slated to be removed/disabled. Sub-node of `PlannedTraffic` and `RequestedTraffic`. **Note:** Relevant for rule removal requests only.	None

Node	Description	Sub-nodes
RuleRemovalRuleAction	The action to perform on the rule in the device policy (for example, allow or drop). Sub-node of `PlannedTraffic` and `RequestedTraffic`. **Note:** Relevant for rule removal requests only.	None
RuleRemovalUserstoNotify	FireFlow users to notify regarding the rule's upcoming removal/disablement. Sub-node of `PlannedTraffic` and `RequestedTraffic`. **Note:** Relevant for rule removal requests only.	None

Node	Description	Sub-nodes
Scope	The scope of the change (Local / Global). Sub-node of `PlannedTraffic` and `RequestedTraffic`. **Note:** Relevant for object change requests only.	None
Service	The device service or port for the connection. Sub-node of `PlannedTraffic` and `RequestedTraffic`. **Note:** Relevant for traffic change requests only.	If inclusion of user-defined custom traffic fields in flat tickets is enabled, then this node will have the following sub-nodes: • Value. • A node for each custom field. Each such node will have its own Value sub-node. See Enabling/Disabling Inclusion of User-Defined Custom Traffic Fields in Flat Tickets (see Enable / disable inclusion of user-defined custom traffic fields in flat tickets).

Node	Description	Sub-nodes
severity	The severity of a risk. Sub-Node of `Risk`. **Note:** Relevant for traffic change requests only.	None
Source	The IP address, IP range, network, or device object. Sub-node of `PlannedTraffic` and `RequestedTraffic`. **Note:** Relevant for traffic change requests only.	If inclusion of user-defined custom traffic fields in flat tickets is enabled, then this node will have the following sub-nodes: • Value. • A node for each custom field. Each such node will have its own Value sub-node. See Enabling/Disabling Inclusion of User-Defined Custom Traffic Fields in Flat Tickets (see Enable / disable inclusion of user-defined custom traffic fields in flat tickets).
Status	The change request's status. Sub-node of `Ticket`.	None

Node	Description	Sub-nodes
Subject	The change request's subject. Sub-node of `Ticket`.	None

Node	Description	Sub-nodes
Ticket	The root node of a flat ticket.	• AffectedRulesResult • AlreadyWorksFirewalls • AutomaticallyImplemented • Cc • ChangeFullData • ChangeImplementationNotes • ClosedAt • CMSticketid • Createticketsfromattachment • Description • Due • Expires • Firewall • FormType • Id • ImplementaionDate • InitialPlanStartTime • IsActiveChangeApplicable • IsWorkOrderEditable • LastUpdated • LastUpdatedBy • New • ObjectChangeValidationResult • Owner • OwningGroup • Planned Traffic • Priority • RequestedTraffic • Requestor • RiskDetails

Node	Description	Sub-nodes
		• RisksNumber • Status • Subject • TicketTemplateName • TrafficChangeTime • TranslatedDestination • TranslatedService • TranslatedSource • Workflow
TicketTemplateName	The name of the change request's template. Sub-node of `Ticket`.	None
TrafficChangeTime	The amount of time that has elapsed since the traffic was changed, in UNIX time. Sub-node of `Ticket`. Relevant for traffic change requests only.	None

Node	Description	Sub-nodes
TranslatedDestination	The change request's destination, as translated to IP addresses. Sub-node of `Ticket`. **Note:** Relevant for traffic change requests only.	None
TranslatedService	The change request's destination, as translated to ports. Sub-node of `Ticket`. **Note:** Relevant for traffic change requests only.	None

Node	Description	Sub-nodes
TranslatedSource	The change request's source, as translated to IP addresses. Sub-node of `Ticket`. **Note:** Relevant for traffic change requests only.	None

Node	Description	Sub-nodes
Value	The value of this node's parent node. Sub-node of `Action`, `Destination`, `Service`, and `Source`. **Note:** Relevant only when inclusion of user-defined custom traffic fields in flat tickets is enabled. See Enabling/Disabling Inclusion of User-Defined Custom Traffic Fields in Flat Tickets (see Enable / disable inclusion of user-defined custom traffic fields in flat tickets).	None

Node	Description	Sub-nodes
ValuesToRemove	The IP addresses or protocols to remove from the device object. Sub-node of `PlannedTraffic` and `RequestedTraffic`. **Note:** Relevant for object change requests only.	None
Workflow	The change request's assigned workflow. Sub-node of `Ticket`.	None

Flat Ticket Examples

A *flat ticket* is a change request in XML format. For full XML examples, see our online Tech Docs.

Supported Comparison Operators

Supported Comparison Operators

Operator	Description
=	Equal

Operator	Description
!=	Not equal
=~	Contains
!~	Does not contain
<	Less than
>	Greater than

Supported Boolean Operators

Supported boolean operators include:

Operator	Description
and	Both of the comparisons in the sub-query must be true. In the following example, the condition is only met for new change requests with the Standard workflow: `Ticket[Workflow = "Standard" $and$ Status = "new"]`
or	One or both of the sub-queries pairs joined by this operator must be true. In the following example, the condition is met for change requests that are new, change requests owned by John Smith, and new change requests owned by John Smith: `Ticket[Status = "new" $or$ Owner/RealName = "John Smith"]`

Comprehensive Examples

Example 1

The following XQL query specifies that one of the following must be true, in order for the condition to be satisfied.

- The change request's priority is greater than 7.
- The requestor's email address includes the string "company.com".
- The value of the custom field called "Project" is "Infrastructure".

```
Ticket[Priority > 7 $or$ Requestor/EmailAddress =~ "company.com" $or$
Project = "Infrastructure"]
```

Example 2

The following discrete XQL queries,when used in the sequence shown, specify the following:

- If the change request's most severe risk is high, the first condition will be satisfied.
- If the change request's most severe risk is suspected high, the second condition will be satisfied.
- If the change request's most severe risk is medium, the third condition will be satisfied.
- If the change request's most severe risk is low, the fourth condition will be satisfied.

Note: In this example, each query is the condition for a discrete **conditional target status**. Each condition would have its own **target status** specified.

```
Ticket/RisksDetails/Risk[severity = "high" ]

Ticket/RisksDetails/Risk[severity = "suspected high" ]

Ticket/RisksDetails/Risk[severity = "medium" ]

Ticket/RisksDetails/Risk[severity = "low" ]
```

This would be relevant, for example, if an approval stage is only required if there are certain risks.

Note: When multiple items are expected in the XML, such as risks found by Risk Check, XQL conditions should only include equality (=) or containment (= ~), and not include inequality (! =) or exclusion (! ~). This is because the condition is true if found at least once in XML.

Add parallel action logic

By default, FireFlow allows you to specify whether an action will be performed in parallel to a second, identical action.

If desired, you can add more logic for parallel actions. For example, you can add the following parallel action logic:

- 50% of the responsible roles must meet certain criteria, in order to trigger this action.
- The "Managers" user role must meet certain criteria in order to trigger this action.

Do the following:

1. Log in to the FireFlow server using the username "root" and the related password.
2. Under the directory `/usr/share/fireflow/local/etc/site/lib/`, open the file `ParallelSiteLogic.pm`.
3. For each parallel logic you want to configure, add the following lines to the file:

   ```
   sub parallel_ logicName
   {      my $additionalGroups = shift;      my $pendingGroups = shift;}
   ```

   Where *logicName* is the name of the parallel logic. This can be any string.

   The function will receive the following parameters as input:

   - `$additionalGroups` - The additional responsible roles field after update
   - `$pendingGroups` - The pending responsible roles field after update

   The function will return a Boolean value:

   - 1 - The logic is satisfied, and the action will be triggered.
   - 0 - The logic is not satisfied, and the action is still in parallel status.
4. Save the file.
5. Restart FireFlow. For details, see Restart FireFlow.

Edit actions

Editing an action will modify the action's default settings throughout all statuses in the workflow.

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

   The **List of Workflows** page is displayed.

2. Do one of the following:

   - Click on the desired workflow's name.
   - Next to the desired workflow, click **Edit**.

   The **Edit Workflow** page opens with the workflow's details.

3. Do one of the following:

   - In the VisualFlow main menu, click **Actions**.

     The **Available actions** page is displayed with a list of actions used in the workflow.

   - In the workflow layout, click on a status that uses the desired action as an inbound or outbound action.

     The **Edit Status** page is displayed with a list of inbound and outbound actions for the status.

4. Click **Edit** next to the desired action.

   The **Edit Action** page is displayed.

5. Complete the fields using the information in Action Fields (see Action Fields).

   If you expanded the **Advanced** area, additional fields appear.

6. If you set the **Parallel** field to all, set the action's responsible roles by doing the following:

a. Click the **Click here to set the action's responsible roles** link.

   The **Responsible roles** dialog box appears.

   The **Responsible role** field displays the user role responsible for change requests in this status.

b. In the **Additional responsible roles** list, select the additional user roles responsible for change requests in this status.

   To select multiple user roles, press **Ctrl** while you click on the desired user roles.

c. Click **OK**.

7. Click **Save Draft**.

Reorder actions

You can control the order in which actions appear in a workflow's list of actions.

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

   The **List of Workflows** page is displayed.

2. Do one of the following:

   - Click on the desired workflow's name.
   - Next to the desired workflow, click **Edit**.

   The **Edit Workflow** page opens with the workflow's details.

3. In the VisualFlow main menu, click **Actions**.

   The **Available actions** page is displayed.

4. In the list of actions, click  next to an action you want to move, and drag it to the desired location in the list.

Delete actions

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

   The **List of Workflows** page is displayed.

2. Do one of the following:

   - Click on the desired workflow's name.
   - Next to the desired workflow, click **Edit**.

   The **Edit Workflow** page opens with the workflow's details.

3. Do one of the following:

   - In the VisualFlow main menu, click **Actions**.

     The **Available actions** page is displayed with a list of actions used in the workflow.

   - In the workflow layout, click on a status that uses the desired action as an inbound or outbound action.

     The **Edit Status** page appears with a list of inbound and outbound actions for the status.

4. Next to the desired action, click **Delete**.

   A confirmation message appears.

5. Click **OK**.

The action is deleted from the list.

Working with SLAs

FireFlow enables you to configure a Service Level Agreement (SLA) per workflow. An SLA is a formal definition of the logical workflow stages that comprise a change request's lifecycle and, optionally, the amount of time allotted for completing each of

these stages and the change request lifecycle as a whole. Hence, a separate SLA must be defined for each workflow.

Workflow stages in SLAs

In an SLA, each of the workflow stages is represented by a Service Level Objectives (SLO). An SLO specifies the following:

- The stage's starting point, which is when the change request enters a certain status
- The stage's ending point, which is when the change request leaves a certain status
- The stage's name

If you configure a time limit to an SLO, you can optionally configure the SLA to transition to the next status once the SLO expires. For example, after a traffic change request is implemented and the requestor has been notified, the change request waits for the requestor to approve the change request. If you create an SLO on the "user accept" status and configure a time limit for it, you can configure the SLA such that if the SLO expires and the request is still in the "user accept" status (meaning the requestor has not yet responded), the change request automatically transitions to the next status.

FireFlow uses the information specified in an SLO to measure the amount of time spent on the relevant stage; and once the change request has completed its lifecycle, FireFlow can use all of the SLA's SLOs together to calculate the amount of time spent on the entire lifecycle.

FireFlow then uses the calculated SLA information to generate reports on change requests that meet certain criteria (for example, change requests which have spent more than a certain number of days in a particular stage), and display those reports in searches, charts, and dashboards. For information on configuring SLA notifications, see Working with SLA Notifications (see Manage SLA notifications).

Note: You can optionally configure SLO time to be measured in business hours. See Configuring FireFlow to Measure SLO Time in Business Hours (see Configuring FireFlow to Measure SLO Time in Business Hours).

Add SLOs

This procedure describes how to add SLOs to a worfklow's SLA.

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

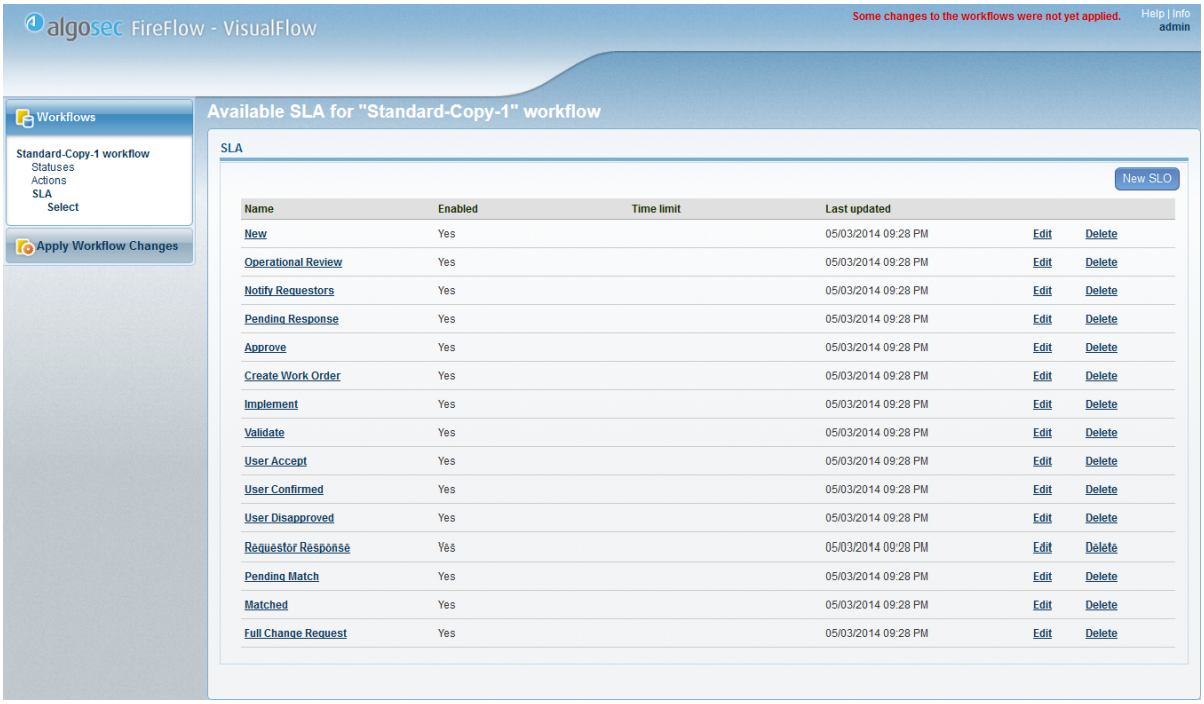
   The **List of Workflows** page is displayed.

2. Next to the desired workflow, click **Edit**.

   The **Edit Workflow** page opens with the workflow's details.

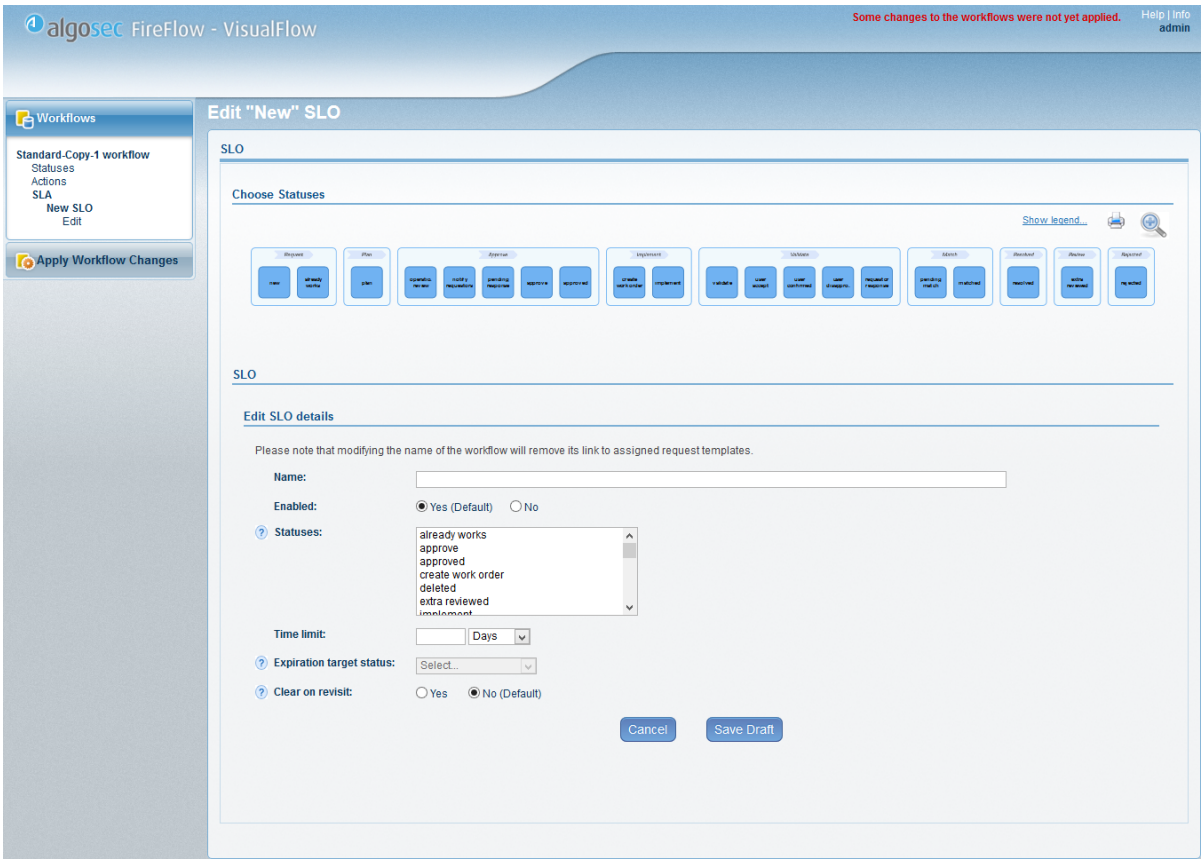
3. In the VisualFlow main menu, click **SLA**.

   The **Available SLA** page is displayed with all of the SLOs comprising the workflow's SLA.



4. Click **New SLO**.

   The **Edit SLO** page is displayed.



5. Complete the fields using the information in SLO Fields (see SLO Fields).
6. Click **Save Draft**.

The new SLO is added to the workflow's SLA.

SLO Fields

In this field...	Do this...
Name	Type the name of the SLO. This field is mandatory.

In this field...	Do this...
Enabled	Specify whether this SLO should be enabled, by choosing one of the following: • **Yes:** The SLO is enabled and will be used for SLA calculations. • **No:** The SLO is disabled. It will not be used for SLA calculations. The default value is **Yes**.
Statuses	Select one or more statuses that represent the starting point for the workflow stage represented by this SLO. To select multiple statuses, hold down the **Ctrl** key while clicking on the desired statuses. The selected statuses are highlighted in the diagram at the top of the workspace. Alternatively, click **Enable visual edit**, and then click on the desired statuses in the diagram at the top of the workspace. The selected statuses appear in green. When finished, click **Finish visual edit**.
Time limit	To configure a time limit for the workflow stage represented by this SLO, type in the number of time units in the field provided, and select the type of time unit in the drop-down list.
Expiration target status	Select the status to which the change request should transition, when the specified time limit has been exceeded. This field is only enabled, if you configured a time limit for the SLO.
Clear on revisit	Specify whether when re-visiting the SLO or one of its statuses, the time counter should be reset to zero, by choosing one of the following: • **Yes:** Reset the time counter, then begin timing from zero. • **No:** Resume timing, without resetting the time counter. The default value is **No**.

In this field...	Do this...
End trigger	Specify what event should trigger the end of the SLO, by choosing one of the following: • **Change request leaves the status:** End the SLO, when the change request leaves the status. • **Parallel action done by role:** End the SLO, when a parallel action is performed by a certain responsible role. You must select the desired responsible role in the drop-down list provided. This field appears only for SLOs that contain a status with a parallel action.

Edit SLOs

This procedure describes how to edit SLOs in a workflow's SLA.

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

   The **List of Workflows** page is displayed.

2. Next to the desired workflow, click **Edit**.

   The **Edit Workflow** page opens with the workflow's details.

3. In the VisualFlow main menu, click **SLA**.

   The **Available SLA** page appears with all of the SLOs comprising the workflow's SLA.

4. Next to the desired SLO, click **Edit**.

   The **Edit SLO** page is displayed.

5. Complete the fields as needed. For details, see SLO Fields .

6. Click **Save Draft**.

Delete SLOs

This procedure describes how to delete SLOs from a workflow's SLA.

Do the following:

1. In the VisualFlow main menu, click **Workflows**.

   The **List of Workflows** page is displayed.
2. Next to the desired workflow, click **Edit**.

   The **Edit Workflow** page opens with the workflow's details.
3. In the VisualFlow main menu, click **SLA**.

   The **Available SLA** page is displayed with all of the SLOs comprising the workflow's SLA.
4. Next to the desired SLO, click **Delete**.

   A confirmation message appears.
5. Click **OK**.

The SLO is deleted.

Apply / discard workflow changes

This topic describes how to apply or discard workflow changes in FireFlow.

Apply workflow changes

Applying workflow changes imports all workflow changes into FireFlow. No changes to workflows will take affect unless they are applied.

Do the following:

1. Do one of the following:
   - In the VisualFlow main menu, click **Workflows**.

     The **List of Workflows** page is displayed.
   - In the VisualFlow main menu, click **Apply Workflow Changes**.

   The **Apply Changes** page is displayed.

2. Click **Apply changes to all workflows**.

   A confirmation message appears.

3. Click **OK**.

   A backup of the previous workflows configuration is saved to `/usr/share/fireflow/local/etc/site/backup/YYYY_MM_DD_hh-mm-ss`, where `YYYY_MM_DD_hh-mm-ss` is a timestamp.

   For example: **2011_01_21_10-30-00**

   All workflow changes are imported into FireFlow and a success message appears.

4. Click **OK**.

   The message informing you that changes have been made to the workflows disappears.

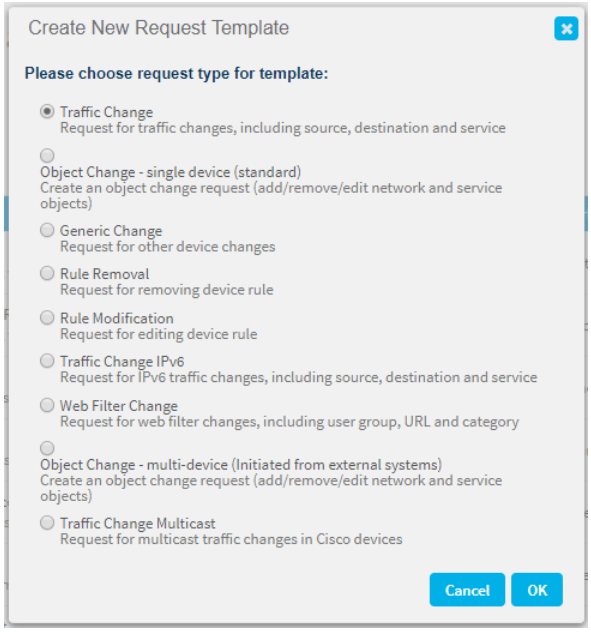
   Note: You do not need to restart FireFlow to see workflow changes.

5. (Optional) To finish enabling the workflow by adding or editing the relevant request template, do the following:

a. If you are viewing the **List of Workflows** page, click **Apply Workflow Changes** in the VisualFlow main menu.

b. In the **Apply changes to workflows** area, click **Define Request Templates**.

   The **Request Templates** page is displayed.



For more details, see Manage request templates.

Discard workflow changes

You can discard all workflow changes that have not yet been applied. This will reload the XML workflow files that are currently in use by FireFlow into VisualFlow.

Do the following:

1. In the VisualFlow main menu, click **Apply Workflow Changes**.

   The **Apply Changes** page is displayed.

2. Click **Discard all changes**.

   A confirmation message appears.

3. Click **OK**.

All workflow changes are discarded, and a success message is displayed.

4. Click **OK**.

   The message informing you that changes have been made to the workflows disappears.

Examples using VisualFlow

This topic describes several sample use cases for VisualFlow.

Remove the Notify Requestor stage

The following comprehensive example describes how to modify a copy of the Standard workflow, so that FireFlow does not wait for user acceptance after implementing a change request.

Once implementation is complete, the Network user can simply resolve the change request (or re-implement it, if an error was detected). Notification is sent to the user only upon the resolve action.

Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. Access VisualFlow. For details, see Get started in VisualFlow.
3. Add a new workflow based on the Standard workflow.

   The workflow "Standard-Copy-*#*" is created, where *#* represents the copy's number.

4. Edit the new workflow as follows:
   - Set the **Name** field to the workflow's name. For example, "MyStandard".
   - Set the **Configuration File** field to the workflow's configuration file. For example, "MyStandard".
   - Set the **Default** field to **yes**.
5. Delete the workflow's "Notify Requestor" action.

6. Edit the workflow's "Resolve" action as follows:
    - Set the **Type** field's to **Reply to user**, so that mail can be sent to the requestor.
    - Set the **Mail content** field to "Your request has been implemented. It will be closed now.".
7. Add a "resolve" outbound action to the workflow's "Validate" status as follows:
    - Set the **Display action button** field to **Yes**, so that the "Resolve" button will appear for change requests in the "Validate" stage.
    - Set the **Display in workflow layout** field to **Yes**, so that the outbound action will appear as an arrow in the workflow layout.
8. Install the workflow.
9. Log in to the FireFlow server via SSH, using the username "root" and the related password.
10. Restart FireFlow. For details, see Restart FireFlow.

Allowe the Network Role to approve change requests

The following comprehensive example describes how to modify a copy of the Standard workflow, to allow Network users to approve change requests.

After initial planning, the change request achieves the new status "pre-check". Network users can then decide whether to approve the change request, not approve it, or send it to a Security user.

Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. Access VisualFlow. For details, see Get started in VisualFlow.
3. Add a new workflow based on the Standard workflow.

    The workflow "Standard-Copy-#" is created, where # represents the copy's number.

4. Edit the new workflow as follows:
    - Set the **Name** field to the workflow's name. For example, "MyStandard".
    - Set the **Configuration File** field to the workflow's configuration file. For example, "MyStandard".
    - Set the **Default** field to **yes**.
5. Add a new status to the workflow as follows:
    - Set the **Name** field to "pre-check".
    - Set the **Stage** field to **approve**.
    - Set the **Responsible role** field to **Network**.
    - Set the **Allow editing traffic fields** field to **yes**.
    - Set the **Stage still incomplete** field to **yes**.
6. Reorder the statuses so that the new "pre-check" status appears immediately before the "approve" status.
7. Add a new action to the workflow as follows:
    - Set the **Name** field to "send_to_security".
    - Set the **Type** field to **Change status**.
    - Set the **Display Name** field to "Send to Security".
    - Set the **Target status** field to **approve**.
    - Set the **Required action permission** field to **UserDefinedRight01**.
    - Set the **Applies to change requests of type** field to **Parent** and **Regular**.
    - Set the **Traffic fields required** field to **yes**.
8. Reorder the actions so that the new "Send to Security" action appears immediately after the "Risk Check" action.
9. Edit the "Initial Plan" action to transition the change request to the new "pre-check" status as follows:

Set the **Target status** field to **pre-check**.

10. Edit the "Risk Check" action to transition the change request to the new "pre-check" status as follows:

    Set the **Target status** field to **pre-check**.

11. Add a "risk_check" outbound action to the "pre-check" status as follows:
    - Set the **Display action button when field is empty** field to **Request Risk Check Result**, so that the "Risk Check" button will appear for change requests in the "pre-check" stage when this field is empty.
    - Set the **Display in workflow layout** field to **Yes**, so that the outbound action will appear as an arrow in the workflow layout.
12. Add a "send_to_security" outbound action to the "pre-check" status as follows:
    - Set the **Display action button** field to **Yes**, so that the "Send to Security" button will appear for change requests in the "pre-check" stage.
    - Set the **Display in workflow layout** field to **Yes**, so that the outbound action will appear as an arrow in the workflow layout.
13. Add an "approve" outbound action to the "pre-check" status as follows:
    - Set the **Display action button** field to **Yes**, so that the "Approve" button will appear for change requests in the "pre-check" stage.
    - Set the **Display in workflow layout** field to **Yes**, so that the outbound action will appear as an arrow in the workflow layout.
14. Add a "re_plan" outbound action to the "pre-check" status as follows:
    - Set the **Display Name** field to "Not Approve", so that this button's name will appear for change requests in the "pre-check" stage.
    - Set the **Display action button** field to **Yes**, so that the "Not Approve" button will appear for change requests in the "pre-check" stage.

- Set the **Display in workflow layout** field to **Yes**, so that the outbound action will appear as an arrow in the workflow layout.
- Set the **User confirmation needed** field to **No**, so that this action will not trigger an "Are you sure?" pop-up for change requests in "pre-check" stage.
- Set the **Mail content** field to "Your request has not been approved and needs to be re-planned", so that this text will appear in emails sent to the requestor for change requests in "pre-check" stage.

15. Add a "re_implement" outbound action to the "pre-check" status as follows:

    Set the **User confirmation needed** field to **No**, so that this action will not trigger an "Are you sure?" pop-up for change requests in the "pre-check" stage.

16. Delete the "Risk Check" outbound action from the "approve" status, so that the risk check button will not appear for change requests in the "Approve" stage.
17. Assign the **UserDefinedRight01** permission to the Network user role.

    Members of the Network role can now perform the "Send to Security" action.

18. Install the workflow.
19. Log in to the FireFlow server via SSH, using the username "root" and the related password.
20. Restart FireFlow.

Add another Approve stage

The following comprehensive example describes how to modify a copy of the Standard workflow, by adding a second Approve stage to the lifecycle.

A new status, "second check", will be achieved after the first approve action. The second approve must then be performed by the new "High Level Security" user role.

Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. Add a user role as follows:
   - Set the **Name** field to "High Level Security".
   - Set the **Description** field to "High Level Security".
3. Set the user role to inherit permissions from the security role.
4. Access VisualFlow.
5. Add a new workflow based on the Standard workflow.

   The workflow "Standard-Copy-*#*" is created, where *#* represents the copy's number.
6. Edit the new workflow as follows:
   - Set the **Name** field to the workflow's name. For example, "MyStandard".
   - Set the **Configuration File** field to workflow's configuration file. For example, "MyStandard".
   - Set the **Default** field to **yes**.
7. Add a new status for the workflow as follows:
   - Set the **Name** field to "second check".
   - Set the **Stage** field to **approve**.
   - Set the **Responsible role** field to **High Level Security**.
   - Set the **Allow editing traffic fields** field to yes.
   - Set the **Stage still incomplete** field to yes.
8. Reorder the statuses so that the new "second check" status appears immediately after the "approve" status.
9. Add an "approve" outbound action to the "second check" status as follows:

- Set the **Display action button** field to **Yes**, so that the "Approve" button will appear for change requests in the "second check" stage.
- Set the **Display in workflow layout** field to **Yes**, so that the outbound action will appear as an arrow in the workflow layout.

10. Add a "re-plan" outbound action to the "second check" status as follows:
    - Set the **Display Name** field to "Reject", so that this button's name will appear for change requests in the "second check" stage.
    - Set the **Display action button** field to **Yes**, so that the "Reject" button will appear for change requests in the "second check" stage.
    - Set the **Display in workflow layout** field to **Yes**, so that the outbound action will appear as an arrow in the workflow layout.
    - Set the **User confirmation needed** field to **No**, so that this action will not trigger an "Are you sure?" pop-up for change requests in the "second check" stage.
    - Set the **Mail content** field to "Your request has been rejected and needs to be re-planned", so that this text will appear in emails sent to the requestor for change requests in the "second check" stage.
11. Add a "re-implement" outbound action to the "second check" status as follows:

    Set the **User confirmation needed** field to **No**, so that this action will not trigger an "Are you sure?" pop-up for change requests in "second check" stage
12. Add a new action to the workflow as follows:
    - Set the **Name** field to "first_approve".
    - Set the **Type** field to **Internal comment**.
    - Set the **Display Name** field to "First Approve".
    - Set the **Target status** field to **second check**.
    - Set the **Required action permission** field to **UserDefinedRight02**.

- Set the **Applies to change requests of type** field to **Parent** and **Regular**.
- Set the **Traffic fields required** field to **yes**.

13. Reorder the workflow's actions, so that the new "First Approve" action immediately after the "Risk Check" action.
14. Edit the "Approve" action as follows:

    Set the **Display Name** field to "Final Approve".
15. Add a "first_approve" outbound action to the "approve" status as follows:
    - Set the **Display action button** field to **Yes**, so that the "First Approve" button will appear for change requests in the "approve" stage.
    - Set the **Display in workflow layout** field to **Yes**, so that the outbound action will appear as an arrow in the workflow layout.
16. Delete the "Final Approve" outbound action from the approve status.
17. Assign the **UserDefinedRight02** permission to the Security user role.

    Members of the Security role can now perform the "First Approve" action.
18. Install the workflow.
19. Log in to the FireFlow server via SSH, using the username "root" and the related password.
20. Restart FireFlow.

Manage workflow options

A change request's workflow determines which lifecycle stages it will pass through. You can customize change request lifecycles, by creating new workflows, and by disabling or deleting the built-in workflows. Furthermore, you can modify the set of conditions determining when each workflow should be assigned.

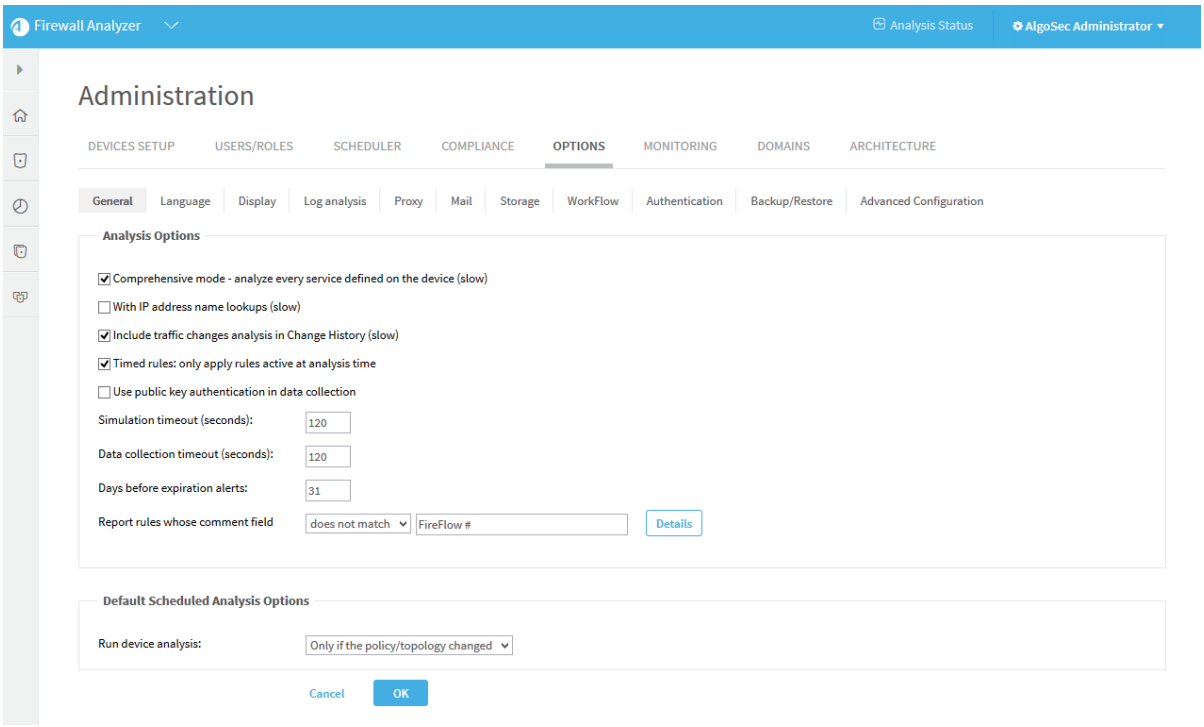
You must define the parameters for integration with your external corporate Change Management System (CMS). AFA can connect to AlgoSec FireFlow, BMC Remedy, HP

Service Center and Service Manager (formerly Peregrine), or any other system supporting Web-based access.

When implementing a requested change in the device, many organizations choose to specify a CMS change request ID in the relevant rule comment. AFA will automatically detect such CMS change request IDs in rule comments. Wherever a rule is displayed in the AFA report, its comment will include a link to the CMS system, pointing at the relevant change request. By a simple click on the link, a browser window with the relevant CMS change request will open, to allow further examination of the change (who requested it, who authorized it and when, etc.).

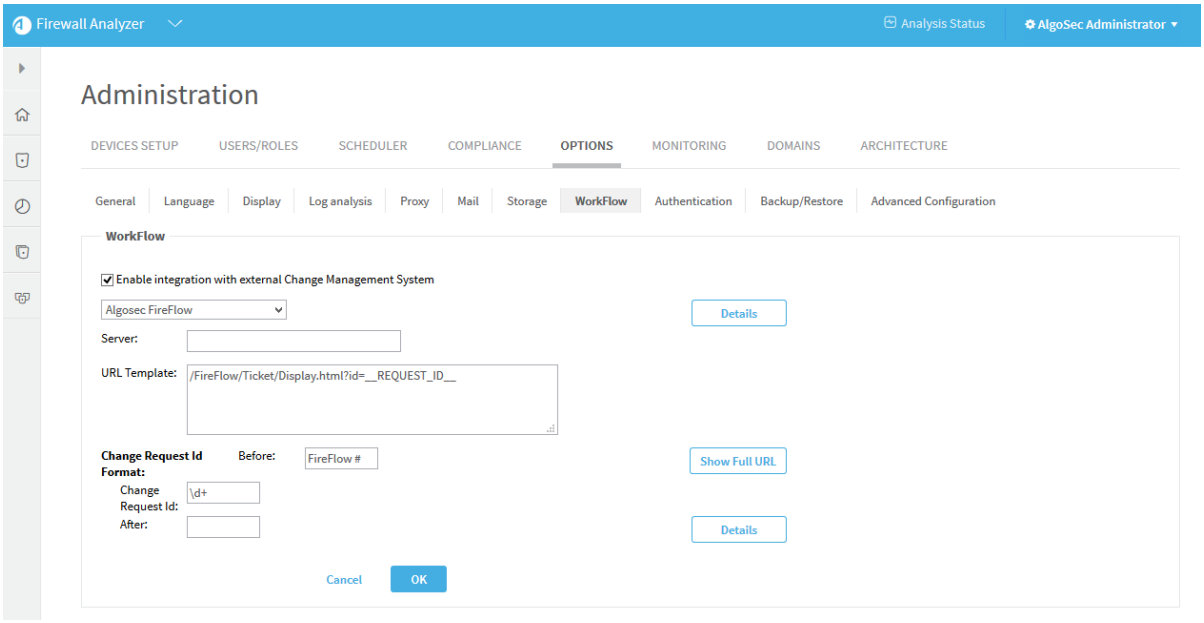
Do the following:

1. In AFA, access the AFA**Administration** area > **Options** tab.



2. In the **Options Menu** area, click **Workflow**.

   The **Workflow** page appears.



3. Select the **Enable integration with external Change Management System** check box.
4. Do **one** of the following:

   To specify FireFlow as the CMS:

   a. In the drop-down list, select **Algosec FireFlow**.

   b. In the **Server** field, type the name of the AlgoSec FireFlow server to be accessed (usually the AFA server).

   c. In the **URL Template** field, specify the structure of the URL that will be created for change request ID links in AFA reports.

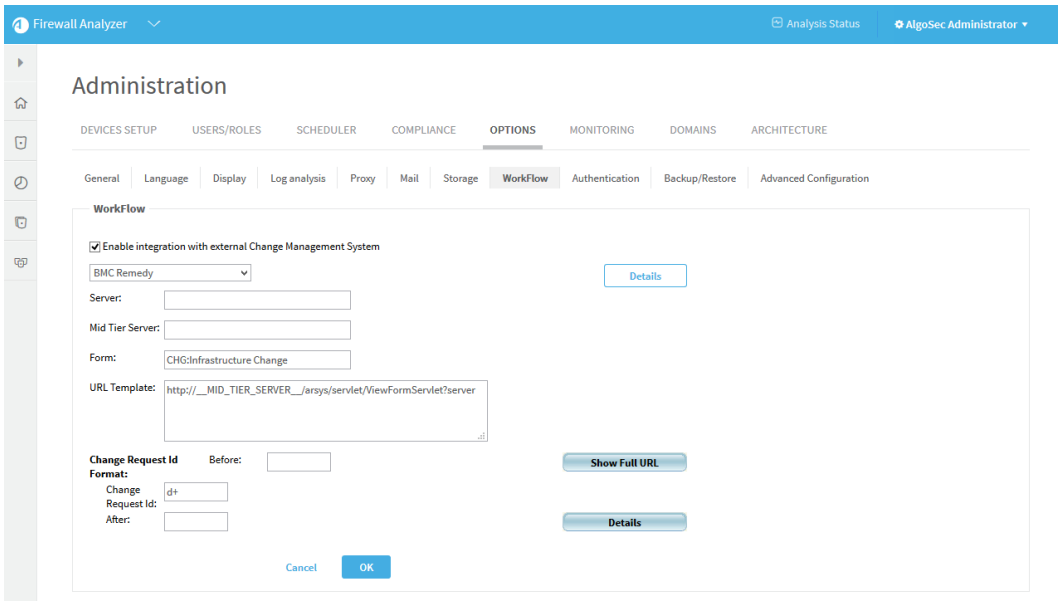
   The following keywords will be replaced by the relevant values: **__SERVER_NAME__ and _REQUEST_ID__.**

   d. Click the **Show Full URL** button to see the resulting URL string.

   To specify BMC Remedy as the CMS:

a. In the drop-down list, select **BMC Remedy**.

The fields change:



b. Fill in the different fields, in order to allow AFA to create the correct links.

The format of a typical URL to a Remedy change request is as follows:

```
<protocol>://<mid_tier_server>/arsys/servlet/ViewFormServlet?
server=<server_name>&form=<form_name>&qual=<query>
```

Where:

- `<protocol>:` may be either `http` or `https`
- `<mid_tier_server>:` (required) - the server name or IP where the Mid Tier is installed. May contain an optional port number, format: 192.168.2.60:8080
- `<server_name>:` (required) - Name of the AR System server to be accessed.
- `<form>:` (required) - Name of the AR System form to be accessed.

For example, if the parameters are:

- Mid Tier Server: 192.168.2.60:8080 (Host: 192.168.2.60, Port: 8080),
- Server: remedy (this is its DNS name)
- Form: Sample
- URL Template: kept at the AlgoSec default

Then the fully formatted URL for change request id 12345 would look like this (all on one row):

```
http://192.168.2.60:8080/arsys/servlet/ViewFormServlet?
server=remedy&form=Sample&qual=%27Change%20ID%2A%2B%27%
3D%2212345%22
```

The URL template that AFA uses can be viewed and edited in the **URL Template** field. It contains the structure of the URL that will be created for change request ID links in AFA reports. You may change this field to specify the URL format explicitly (over-ride the defaults).

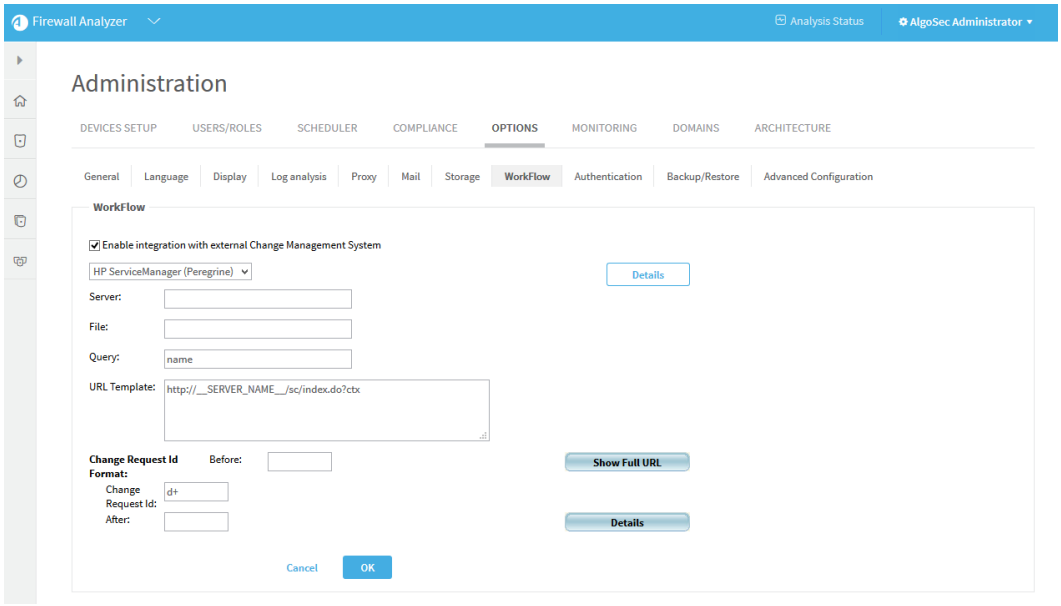
The following keywords will be replaced by the relevant values: __SERVER_NAME__, __MID_TIER_SERVER__, __FORM_NAME__, __REQUEST_ID__.

c. Click **Show Full URL** to see the resulting URL string.

To specify HP Service Center and Service Manager (formerly Peregrine) as the CMS:

a. In the drop-down list, select **HP ServiceCenter (Peregrine).**

The fields change:



b. Fill in the different fields, in order to allow AFA to create the correct links. The format of a typical URL to an HP ServiceCenter change request is as follows:

```
protocol://<server>/sc/index.do?ctx=docEngine&file
=<file>&query=<query>&action=&title=Ticket%20Information
```

Where:

- <protocol>: may be either http or https
- <server>: The HP ServiceCenter (Peregrine) server (name or IP address)
- <file>: The table name
- <query>: Format of the actual query string, e.g. number="__REQUEST_ID__" or incident.id="__REQUEST_ID__"

The string "__REQUEST_ID__" must appear in the query, and will be replaced by the actual request ID in the final link URL.

The URL template that AFA uses can be viewed and edited in the URL Template field. It contains the structure of the URL that will be created for change request ID links in AFA reports. You may change this field to specify the URL format explicitly (over-ride the defaults). The following keywords will be replaced by the relevant values: __SERVER_NAME__, __FILE_NAME__, __QUERY__.

c. Click **Show Full URL** to see the resulting URL string.

Note: Some versions of HP ServiceCenter may require the URL to contain a hash value in addition to the query itself. In order to integrate with AFA, this option should be disabled. In order to configure ServiceCenter Web application to ignore this hash value:

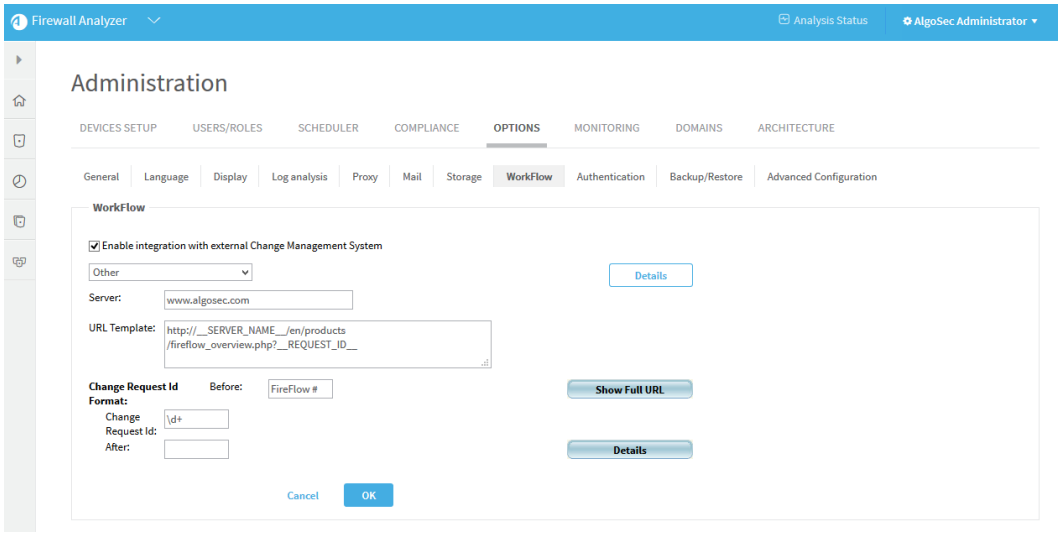
d. Add the following lines to the Web application's web.xml file:

```
<init-param>  <param-name>sc.querysecurity</param-name>
<param-value>false</param-value></init-param>
```

To specify any other CMS system:

a. In the drop-down list, select **Other**.

The fields change:



b. In the Server field, type the name of the HP ServiceCenter server to be accessed.

c. In the **URL Template** area, specify the structure of the URL that will be created for change request ID links in AFA reports.

   The following keywords will be replaced by the relevant values: __SERVER_NAME__, __REQUEST_ID__.

d. Click the **Show Full URL** button to see the resulting URL string.

5. In the **Change Request ID Format** area, define a format to which the device rule comments must comply, so AlgoSec recognizes them as containing a change request ID.

   Only properly formatted rule comments will be linked to the CMS change request. This is relevant for all the Work Flow systems. AFA will look for the following format in the rule comments:

   ```
   <Before><Ticket_id><After>
   ```

   Where <Before> and <After> are fixed strings, and <Ticket_id> is a Perl regular expression (see note below).

For example, if: Before = 'Ticket #', Ticket id = '\d+', and After = '#'

Then this comment will become a link: 'Ticket #1234#' but this comment will not: 'Ticket 1234#' , because <Before> is not equal to 'Ticket #'.

Note: The required Ticket_id format should be specified as a Perl regular expression. You can find tutorials on writing regular expressions on the Internet. Here are some examples for the type of things you can accomplish:

\d represents a digit, \s represents a space, \w - an alphanumeric character.

Examples:

- \d\d\d\d-\d\d- comments must contain a ticket number like 1234-56
- \d\d-\d\d-\d\d\d\d- comments must contain a date like 01-01-2007
- [A-Z]{2}\s*\d+- comments must contain two capital letters, then zero or more spaces, then one or more digits (e.g. “AK 123”)

6. Click **OK**.

Manage request templates

When a user submits a request or creates a change request, they must choose a template on which to base the request. The template determines which fields and pre-set values appear in the change request form, as well as which workflow is used for the change request.

FireFlow provides a set of built-in templates. If desired, you can add, edit, disable and delete templates. You can also specify which templates should be used in specific situations. Both administrators and network operations users can perform these tasks.

For details, see:

- Add and edit request templates
- Modify fields in request templates
- Define request templates for specific scenarios
- Disable / enable request templates
- Configure initial plan device group conditions
- Configure field input validation
- Customize change request wizards
- Add rule documentation for allowing rules
- Configure change request creation from file

Creating Change Request Templates: Watch to learn how to create a new, custom change request template.

Add and edit request templates

This topic describes how to add new request templates to FireFlow, from scratch or based on an existing template, as well as how to edit existing templates.

Add IPv4 traffic, multicast, or multiple-device templates

This procedure describes how to add a new IPv4 traffic, multicast or multiple-device object change request template from scratch.

Note: For other types, see Add other types of request templates.

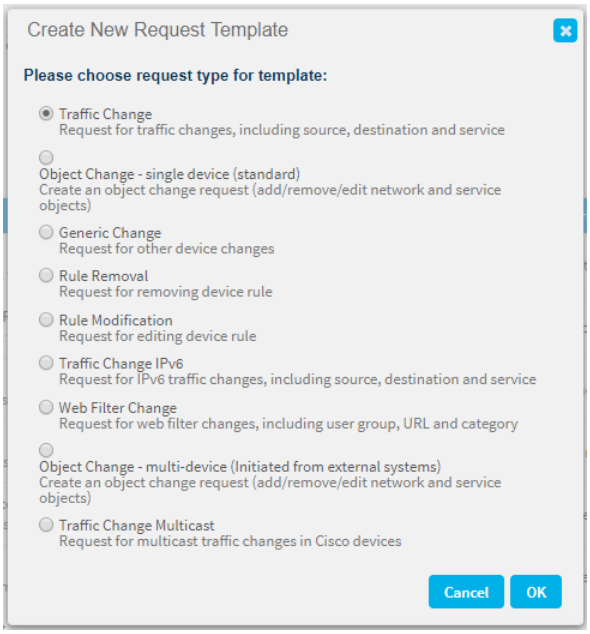
Do the following:

1. In the main menu, click **Request Templates**.

   The **Request Templates** page appears with a list of templates.

2. Click **New Request Template**.

   The **Create New Request Template** dialog box appears.

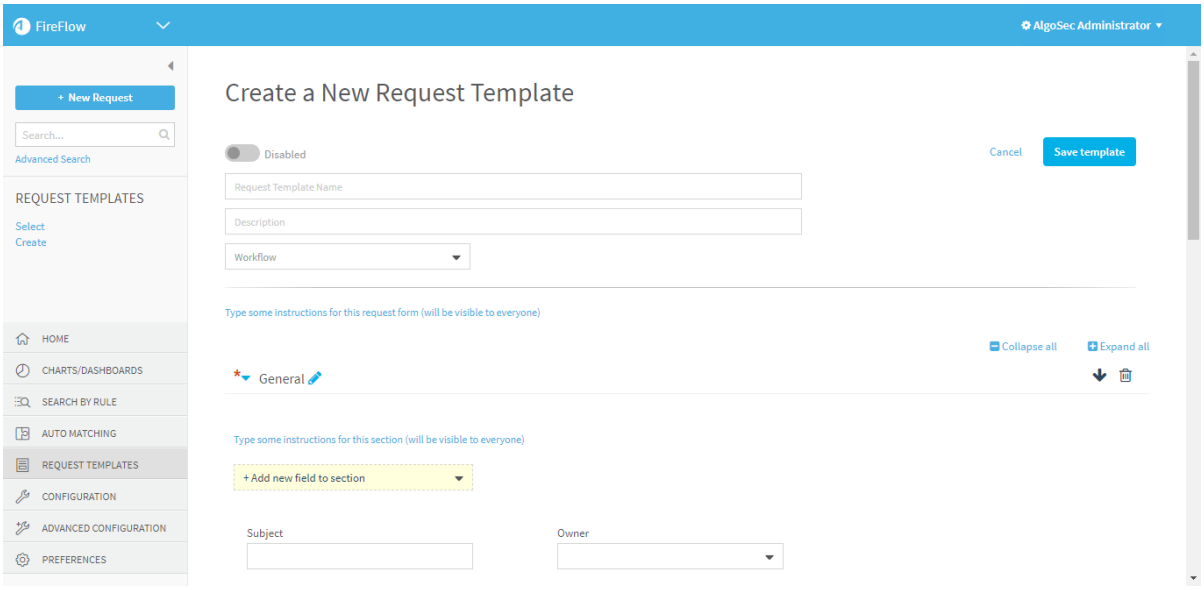


3. Select the request type for the template using the following information:
   - Select **Traffic Change** for a template that includes IPv4 traffic fields.
   - Select **Object Change-single device** for a template that includes object fields for a single device.
   - Select **Generic Change** for a template that does not involves any of the above.

- Select **Rule Removal** for a template that involves device rule removal/disablement.
- Select **Rule Modification** for a template that involves device rule modification.
- Select **Traffic Change IPv6** for a template that involves IPv6 traffic changes.
- Select **Web Filter Change** for a template that involves filtering Web connections for Symantec Blue Coat devices.
- Select **Object Change-multi device** for a template that includes object fields for multiple devices.
- Select **Traffic Change Multicast** for a template that involves multicast traffic changes in Cisco devices.

Click **OK**.

The **Create a New Request Template** page appears for the specified template type.



4. Complete the template fields as needed.

   Any values you enter in the template will appear in all change request forms based on the template.

   For more details, see:

- Traffic change, multicast, and multi-device object template fields
- Object change template fields
- Generic change template fields
- Rule modification template fields
- Rule removal template fields
- Traffic change IPv6 template fields
- Web filter change template fields

5. Click **Save template**.

The new template is created.

Add other types of request templates

This procedure describes how to add request templates for types other than IPv4 traffic, multicast, or multiple-device change requests.

Note: For more details, see Traffic change, multicast, and multi-device object template fields.

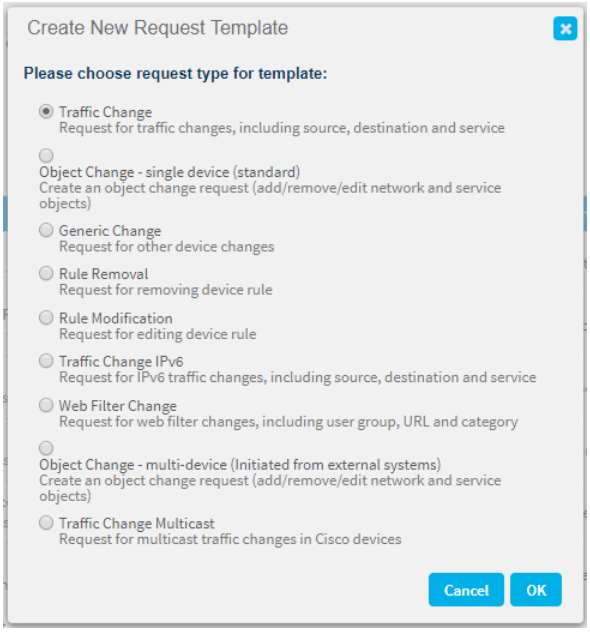
Do the following:

1. In the main menu, click **Request Templates**.

   The **Request Templates** page appears with a list of templates.

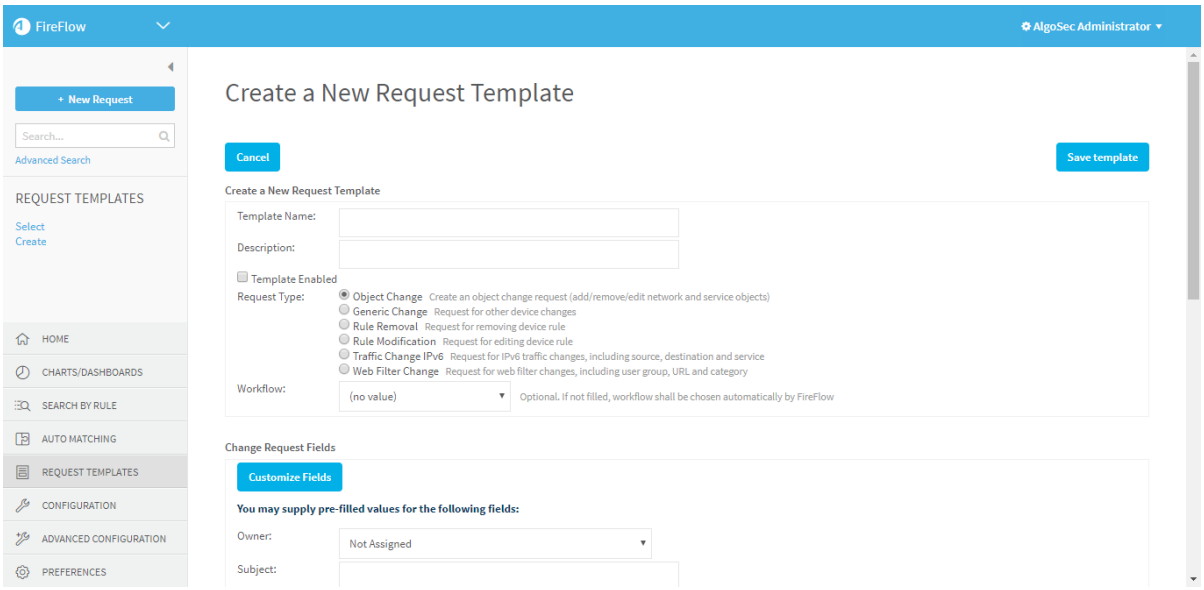
2. Click **New Request Template**.

   The **Create New Request Template** dialog box appears.



3. Select the request type for the template, using the following information:
    - Select **Traffic Change** for a template that includes IPv4 traffic fields.
    - Select **Object Change-single device** for a template that includes object fields for a single device.
    - Select **Generic Change** for a template that does not involves any of the above.
    - Select **Rule Removal** for a template that involves device rule removal/disablement.
    - Select **Rule Modification** for a template that involves device rule modification.
    - Select **Traffic Change IPv6** for a template that involves IPv6 traffic changes.
    - Select **Web Filter Change** for a template that involves filtering Web connections for Symantec Blue Coat devices.
    - Select **Object Change-multi device** for a template that includes object fields for multiple devices.
    - Select **Traffic Change Multicast** for a template that involves multicast traffic changes in Cisco devices.
4. Click **OK**.

The **Create a New Request Template** page appears for the specified template type.



By default, the new template is disabled.

5. To enable template after creation, click **Template disabled**. The **Template enabled** button appears.
6. In the **Request Template Name** box, type a unique name for the new template.
7. In the **Description** box, type a description for the template.
8. In the **Workflow** list, select a workflow for the template.
9. In the General section, complete the fields as needed for your template.

   For details, see:

   - Traffic change, multicast, and multi-device object template fields
   - Object change template fields
   - Generic change template fields
   - Rule modification template fields
   - Rule removal template fields

- Traffic change IPv6 template fields
- Web filter change template fields

Any values you enter in the template will appear in all change request forms based on the template.

10. To customize the position of the fields in the template, see
11. Click **Save template**.

The new template is created.

Add request templates based on an existing template

This procedure describes how to add a new request template based on an existing template.

Note: Alternately, see Traffic change, multicast, and multi-device object template fields and Add other types of request templates.

Do the following:

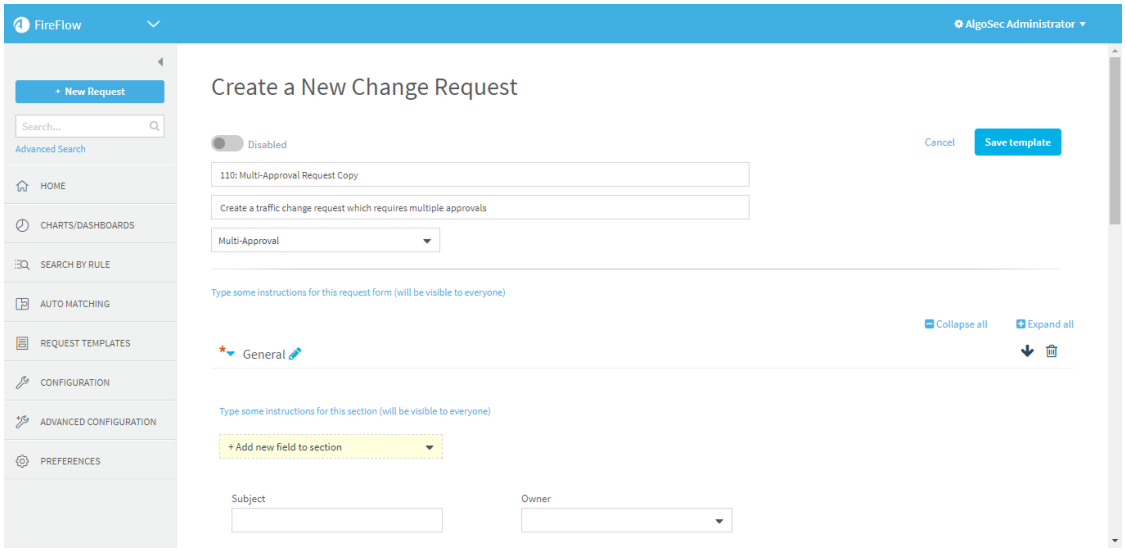
1. In the main menu, click **Request Templates**.

   The **Request Templates** page appears.

2. Do one of the following:

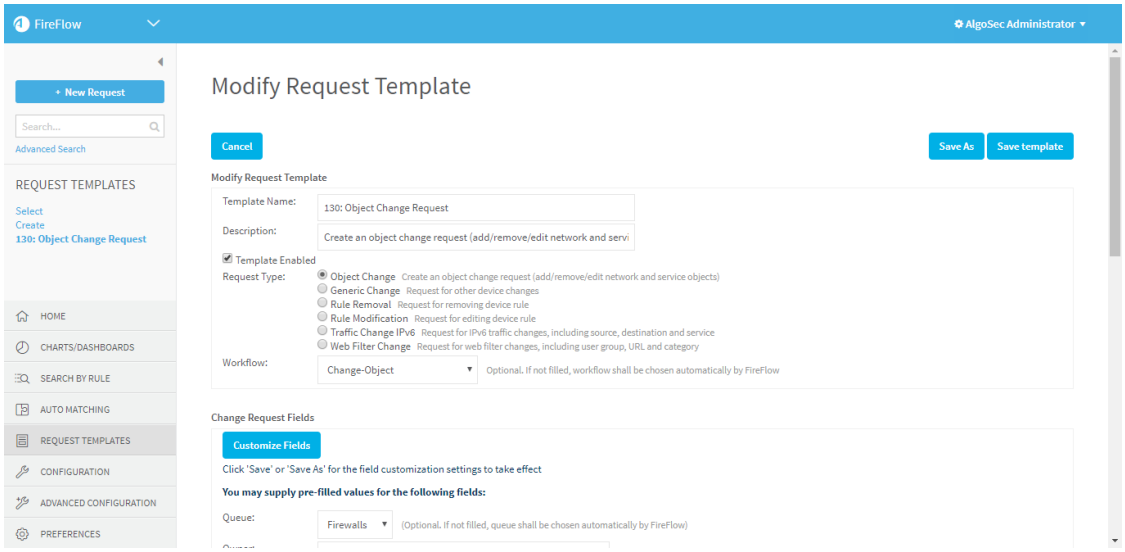
   - For IPv4 traffic, multicast, and multi device object change request templates, hover your mouse over the name of the template, and click  .

     The **Create a New Change Request** page appears.



- For all other templates, click on the name of the template on which you want to base the new template.

  The **Modify Request Template** page appears, displaying the selected template's settings.



Note: Depending on the template, the Web Interface may look different.

3. Modify your fields as needed. For details, see:

- Traffic change, multicast, and multi-device object template fields
- Object change template fields
- Generic change template fields
- Rule modification template fields
- Rule removal template fields
- Traffic change IPv6 template fields
- Web filter change template fields

Any values you enter in the template will appear in all request forms based on the template.

4. Do one of the following:
   - For IPv4 traffic or multicast request templates, click **Save template**.
   - For all other templates, click **Save As**, and enter a new name for the template.

     Click **OK** when you're done.

The new template is created.

Edit request templates

Do the following:

1. In the main menu, click **Request Templates**.

   The **Request Templates** page appears, displaying a list of existing templates.
2. Click on the desired template's name.

   The request template's page appears.
3. Modify the fields as needed. For details, see:
   - Traffic change, multicast, and multi-device object template fields
   - Object change template fields
   - Generic change template fields

- Rule modification template fields
- Rule removal template fields
- Traffic change IPv6 template fields
- Web filter change template fields

Any values you enter in the template will appear in all request forms based on that template.

4. Click **Save template**.

Delete request templates

You can delete any template, including built-in templates.

Do the following:

1. In the main menu, click **Request Templates**.

   The **Request Templates** page appears with a list of existing templates.

2. Hover over the desired template's name with the mouse.
3. To delete, click the  icon on the right.

   A confirmation message appears.

4. Click **OK**.

The template is deleted.

Traffic change, multicast, and multi-device object template fields

In this field...	Do this...
Template disabled	To enable the template, click the widget at the top of the form. The widget turns green () and the label switches to **Enabled**. Disabled templates will not appear as an option in the Create a New Change Request page.

In this field...	Do this...
Request Template Name	Type a name for the template.
Description	Type a description of the template.
Workflow	Select the workflow to assign change requests based on this template.
Type some instructions for this request form (will be visible to everyone)	See Add custom instructions to IPv4, multicast, and multi-device object change templates.
Collapse all Expand all	To collapse or expand all sections, click the relevant link.
General	
Type some instructions for this section (will be visible to everyone)	See Add custom instructions to IPv4, multicast, and multi-device object change templates.
+Add new field to section	To add a pre-defined custom field to the template, click this link and select the field in the drop-down menu. To add a new custom field to the template, or to customize the position of the fields, see Modify fields for IPv4 traffic and multicast request templates.
Traffic	**Note:** This section is not relevant to multi device object change request templates. These request templates have object fields, and the Web Interface does no support customizing these object fields.

In this field...	Do this...
Type some instructions for this section (will be visible to everyone)	See Add custom instructions to IPv4, multicast, and multi-device object change templates.
+ Add or remove traffic fields	Click this link to select traffic fields which should appear for the request template. This includes generic traffic fields (which appear as an additional field in the traffic area) or traffic fields related to an existing traffic field, such as Source, Destination, Service, User or Application. A dialog box opens. Select a field and click **Save**. To add a new traffic field, click **+ New Traffic field**. See New Field for Change Request Fields.
More	
Type some instructions for this section (will be visible to everyone)	See Add custom instructions to IPv4, multicast, and multi-device object change templates.
+Add new field to section	To add a pre-defined custom field to the template, click this link and select the field in the drop-down menu. To add a new custom field to the template, or to customize the position of the fields, see Modify fields for IPv4 traffic and multicast request templates.
+ New Section	To add a new section, click this link. For more information, see Modify fields for IPv4 traffic and multicast request templates.
Hidden Fields	**Note:** Fields added to the Hidden Fields section will not appear in the request form. They are only for internal use. You can drag fields into and out of this section, like all other sections.
+Add new field to section	To add a pre-defined custom field to the template, click this link and select the field in the drop-down menu. To add a new custom field to the template, or to customize the position of the fields, see Modify fields for IPv4 traffic and multicast request templates.

Object change template fields

In this field...	Do this...
Template Name	Type a name for the template.
Description	Type a description of the template.
Template enabled	Check this box to enable the template. Disabled templates will not appear as an option in the Create a New Change Request page.
Request Type	Choose **Object Change**.
Workflow	Select **Change-Object**.
Customize Fields	Click this button to add/remove fields, reorder fields, or reposition fields in the template. See Modify fields in request templates.
Queue	Select the desired queue.
Subject	Type a title for the change request that will be generated. This field is optional.
Priority	Type a number indicating this request's priority, where 0 indicates lowest priority. This field is optional. The default value is 0.
Device Name	Select the device on which the change should be made. The **Request** area and its fields are enabled. This field is optional.

In this field...	Do this...
Action	Choose the desired request action. For non-Check Point devices, the following options are available: • **Add IPs to Object:** Add IP addresses to a host group object on the selected device. • **Remove IPs from Object:** Remove IP addresses from a host group object on the selected device. • **New Object:** Add a host group object to the selected device. • **Delete Object:** Remove a host group object from the selected device. For Check Point devices, the following options are available: • **Add Values to:** Add values to a host group object on the selected device. • **Remove Values from Group:** Remove values from a host group object on the selected device. • **New:** Add an object to the selected device. • **Edit:** Modify an object on the selected device. • **Delete:** Remove an object from the selected device. When using the **New**, **Edit**, and **Delete** actions, you must select the object type. This can be any of the following: • **Host:** An object with a single IP address. • **Group:** An object containing other objects, as well as sub-groups. • **Range:** An object with an IP address range. • **Network:** An object containing a network mask.
Object Name	Do one of the following: • Type the object name. • Use the **Object Wizard**. This field is optional.

In this field...	Do this...
Show	For non-Check Point devices, click this button to translate the object name into an IP address(es). For Check Point devices, click this button to do the following: • If the object is a *host*, click this button to translate the object name into an IP address. • If the object is a *network*, click this button to translate the CIDR/netmask content into an IP address range. • If the object is an *IP address range*, click this button to display the IP address range. • If the object is a *group*, click this button to display a list of objects in the group. All objects that are groups themselves can be expanded by clicking the + icon.
Values To Add / Values To Remove	Do one of the following: • Type the relevant IP address. • Use the **Add IPs** or **Remove IPs** wizard. This field is optional.
Scope	Select the relevant scope. For Check Point devices, **Local** is automatically selected for a CMA and **Global** is automatically selected for MDSM. This field is optional.
Change More Objects	To add more object changes, click this option and complete the fields.
	To remove additional object changes from the request, click this option next to the desired object change.
Create change requests from file	Click **Yes** to enable creating a change request from an attached spreadsheet file.

In this field...	Do this...
External change request id	If a relevant change request has already been opened for this request in an external change management system that is integrated with FireFlow, type the change request's ID number. The FireFlow change request will be linked to the external system change request. This field is optional.
Describe the issue	Type a free text description of the issue. This description will be added to the change request history. This field is optional.

Generic change template fields

In this field...	Do this...
Template Name	Type a name for the template.
Description	Type a description of the template.
Template enabled	Check this box to enable the template. Disabled templates will not appear as an option in the create a new change request page.
Request Type	Choose **Generic Change**.
Workflow	Select **Generic**.
Customize Fields	Click this button to add/remove fields, reorder fields, or reposition fields in the template. See Modify fields in request templates.
Queue	Select the desired queue.
Subject	Type a title for the change request that will be generated. This field is optional.

In this field...	Do this...
Priority	Type a number indicating this request's priority, where 0 indicates lowest priority. This field is optional. The default value is 0.
Create change requests from file	Click **Yes** to enable creating a change request from an attached spreadsheet file.
External change request id	If a relevant change request has already been opened for this request in an external change management system that is integrated with FireFlow, type the change request's ID number. The FireFlow change request will be linked to the external system change request. This field is optional.
Describe the issue	Type a free text description of the issue. This description will be added to the change request history. This field is optional.

Rule removal template fields

In this field...	Do this...
Template Name	Type a name for the template.
Description	Type a description of the template.
Template enabled	Check this box to enable the template. Disabled templates will not appear as an option in the Create a New Change Request page.
Request Type	Choose **Rule Removal**.
Workflow	Select **Rule-Removal**.

In this field...	Do this...
Customize Fields	Click this button to add/remove fields, reorder fields, or reposition fields in the template. For details, see Modify fields in request templates.
Queue	Select the desired queue.
Owner	Select the owner.
Requestor	Type the name of the requestor.
Subject	Type a title for the change request that will be generated. This field is optional.
Due	Click the calendar icon and select the due date.
Expires	Click the calendar icon and select the expiration date.
Priority	Type a number indicating this request's priority, where 0 indicates lowest priority. This field is optional. The default value is 0.
Device Name	Select the device on which the change should be made. This field is optional.
Rule to remove	Click **Select Rules** to open the list of rules for the device. For each rule to remove, select the rule and click **Select**.
Requested action	Choose the action to perform on rules. This can be either of the following: • **Disable rule:** Disable the rule. • **Remove rule:** Remove the rule from the device.
Create change requests from file	Click **Yes** to enable creating a change request from an attached spreadsheet file.

In this field...	Do this...
External change request id	If a relevant change request has already been opened for this request in an external change management system that is integrated with FireFlow, type the change request's ID number. The FireFlow change request will be linked to the external system change request. This field is optional.
From Template	
Describe the issue	Type a free text description of the issue. This description will be added to the change request history. This field is optional.

Rule modification template fields

In this field...	Do this...
Template Name	Type a name for the template.
Description	Type a description of the template.
Template enabled	Check this box to enable the template. Disabled templates will not appear as an option in the Create a New Change Request page.
Request Type	Choose **Rule Modification**.
Workflow	Select **Rule-Modification**.
Customize Fields	Click this button to add/remove fields, reorder fields, or reposition fields in the template. For details, see Modify fields in request templates.
Queue	Select the desired queue. This field is optional.

In this field...	Do this...
Subject	Type a title for the change request that will be generated. This field is optional.
Priority	Type a number indicating this request's priority, where 0 indicates lowest priority. This field is optional. The default value is 0.
Device Name	Select the device on which the change should be made. This field is optional.
Create change requests from file	Click **Yes** to enable creating a change request from an attached spreadsheet file.
External change request id	If a relevant change request has already been opened for this request in an external change management system that is integrated with FireFlow, type the change request's ID number. The FireFlow change request will be linked to the external system change request. This field is optional.
Describe the issue	Type a free text description of the issue. This description will be added to the change request history. This field is optional.

Traffic change IPv6 template fields

In this field...	Do this...
Template Name	Type a name for the template.
Description	Type a description of the template.
Template enabled	Check this box to enable the template. Disabled templates will not appear as an option in the Create a New Change Request page.

In this field...	Do this...
Request Type	Choose **Traffic Change IPv6**.
Workflow	Select **IPv6-Traffic**.
Customize Fields	Click this button to add/remove fields, reorder fields, or reposition fields in the template. For details, see Modify fields in request templates.
Queue	Select the desired queue. This field is optional.
Subject	Type a title for the change request that will be generated. This field is optional.
Priority	Type a number indicating this request's priority, where 0 indicates lowest priority. This field is optional. The default value is 0.
Source	Do one of the following: • Type the IP address, IP range, network, or device object • Use the **Choose Source** wizard. This field is optional.
Destination	Do one of the following: • Type the IP address, IP range, network, or device object. • Use the **Choose Destination** wizard. This field is optional.
Service	Do one of the following: • Type the device service or port for the connection (for example "http" or "tcp/123"). • Use the **Choose Service Wizard**. This field is optional.

In this field...	Do this...
Action	Choose the device action to perform for the connection. This can be either of the following: • **Allow:** Allow the connection. • **Drop:** Block the connection. This field is optional.
NAT settings	Click this option to display Network Address Translation (NAT) and Port Address Translation (PAT) for the defined traffic. The **Source NAT**, **Destination NAT**, **Port Translation**, and **NAT Type** fields appear. Depending on system customizations, the **Source after NAT**, **Destination after NAT**, and **Port after Translation** fields may appear as well. Click NAT settings again to hide the NAT fields.
Source NAT	Type the source NAT value, if the connection's source should be translated. **Note:** If the **Source after NAT** field appears below this field, then you must type the source NAT value *before* translation. This field is optional.
Source after NAT	Type the source NAT value after translation, if the connection's source should be translated. This field is optional.
Destination NAT	Type the destination NAT value, if the connection's destination should be translated. **Note:** If the **Destination after NAT** field appears below this field, then you must type the destination NAT value *before* translation. This field is optional.

In this field...	Do this...
Destination after NAT	Type the destination NAT value after translation, if the connection's destination should be translated. This field is optional.
Port Translation	Type the port value, if the connection's port should be translated. **Note:** If the **Port after Translation** field appears below this field, then you must type the port value *before* translation. This field is optional.
Port after Translation	Type the port value after translation, if the connection's port should be translated. This field is optional.
NAT Type	Specify the type of NAT (**Static** or **Dynamic**). **Note:** If you filled in the **Source NAT**, **Destination NAT**, and/or **Port Translation** fields, then you must specify the NAT type. This field is optional.
Add More Traffic	To add more traffic to the request, click this option and complete the fields.
	To remove additional traffic from the request, click this option next to the desired traffic.
Create change requests from file	Click **Yes** to enable creating a change request from an attached spreadsheet file.

In this field...	Do this...
External change request id	If a relevant change request has already been opened for this request in an external change management system that is integrated with FireFlow, type the change request's ID number. The FireFlow change request will be linked to the external system change request. This field is optional.
Device Name	Select the device on which the change should be made. This field is optional.
Describe the issue	Type a free text description of the issue. This description will be added to the change request history. This field is optional.

Web filter change template fields

In this field...	Do this...
Template Name	Type a name for the template.
Description	Type a description of the template.
Template enabled	Check this box to enable the template. Disabled templates will not appear as an option in the Create a New Change Request page.
Request Type	Choose **Web Filter Change**.
Workflow	Select **Web-Filter**.
Customize Fields	Click this button to add/remove fields, reorder fields, or reposition fields in the template. For details, see Modify fields in request templates.
Queue	Select the desired queue.
Subject	Type a title for the change request that will be generated. This field is optional.

In this field...	Do this...
Priority	Type a number indicating this request's priority, where 0 indicates lowest priority. This field is optional. The default value is 0.
User Group	Do one of the following: • Type the name of the user or user group that should be allowed/denied access to a URL. • Use the **Choose User Group** wizard.
URL	Type the URL to which to allow/deny access.
Category	Do one of the following: • Type URL's Web filtering category. • Use the **Choose Category** wizard. **Note:** When creating a change request via the Blue Coat **Blocked** page, this field is automatically filled in.
Action	Select the device action to perform for the connection. This can be any of the following: • **Allow:** Allow the connection. • **Block:** Block the connection.
Add More Web Filtering	To add more connections to the request, click this option and complete the fields.
	To remove additional traffic from the request, click this option next to the desired traffic.
Create change requests from file	Click **Yes** to enable creating a change request from an attached spreadsheet file.

In this field...	Do this...
External change request id	If a relevant change request has already been opened for this request in an external change management system that is integrated with FireFlow, type the change request's ID number. The FireFlow change request will be linked to the external system change request. This field is optional.
Describe the issue	Type a free text description of the issue. This description will be added to the change request history. This field is optional.

Modify fields in request templates

This topic describes how to modify the fields in specific change request templates.

Modify fields for IPv4 traffic and multicast request templates

When adding or editing IPv4 traffic, multicast traffic, or multi device object change request templates, you can modify the content and layout for the template's fields and sections.

Default template sections

The following table describes the default template sections , and their supported customizations.

Section Name	Can Remove Section?	Rename?	Customize Fields?
General	Yes (The fields in this section will become options when adding a new field to another section.)	Yes	Yes

Section Name	Can Remove Section?	Rename?	Customize Fields?
Traffic **Note:** This section is only for IPv4 and multicast request templates.	No	Yes	Yes
Objects **Note:** This section is only for multi device object change request templates.	No	No	No
More	Yes (The fields in this section will become options when adding a new field to another section.)	Yes	Yes
Hidden Fields	No	No	Yes

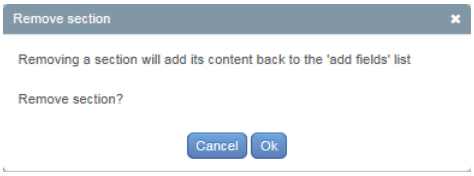
For more details, see:

- Modify sections
- Add a general (non-traffic) change request field
- Add a traffic field

Modify sections

Do any of the following:

Rename a section	Do the following: 1. Click in the section's heading. A text box appears.  2. Edit the name as desired. 3. Click outside the text box. The text box closes.
Add a new section	Do the following: 1. Click **+New Section**. A new section appears with the section's name text box open. 2. Edit the section's name as desired. 3. Click outside the text box. The text box closes. 4. Modify the new section and its fields as desired.
Reposition a section	Do one of the following: • To move the section up, click in the section's heading. • To move the section down, click in the section's heading.

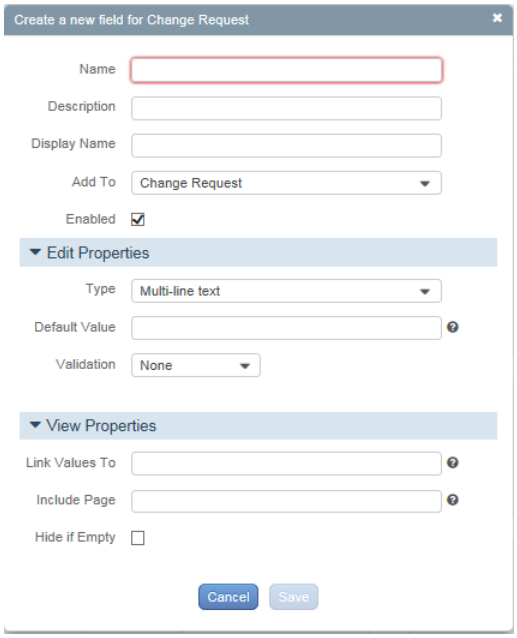
Remove a section	Do the following: Click  in the section's heading. The **Remove section** confirmation message appears.  **Note:** Removing a section will cause it's fields to appear as options when adding a new field to other sections. 1. Click **Ok**. The section is deleted.
Add custom instructions to a section	See Add custom instructions to IPv4, multicast, and multi-device object change templates.

Add a general (non-traffic) change request field

Do the following:

1. Click **+ Add new field to section**, and either select a pre-defined field or the **Create a new field** option.

   Either the field appears at the bottom of the screen, or the **Create a new field for Change Request** dialog box appears.



2. Complete the fields as needed. For details, see New Field for Change Request Fields.

   When you're done, click **Save**.

Add a traffic field

Note: This is only relevant for IPv4 and multicast traffic request templates (not mult device object change request templates).

Do the following:

1. In the **Traffic** section, click **+ Add or remove traffic fields**.

   The **Add or remove traffic fields** dialog box appears.

2. To create a new traffic field, click **+ New traffic field**.

   The **Create a new field for Change Request** dialog box appears.

   Complete the fields using the information in New Field for Change Request Fields (see New Field for Change Request Fields).

   Click **Save**.

The field is defined, and ready to be assigned to a template.

3. To assign a pre-defined field to the template, select the check box for the desired field, and then click **Save**.

   The field(s) appear in the template.

4. To create a space between fields, click **+ Add new field to section**, and then select **Add field spacer**.

   An **Empty space** place holder appears at the bottom of the section.

   Reposition the place holder like any field.

5. To remove a field, hover over the field and click  .

6. To reposition a field, hover over the field, and click and hold  , and drag and drop the field to the desired position.

   As you drag the field, the other fields re-arrange, and a **Drag here** target appears in suitable locations.

   Note: Fields can be moved between sections, as well as within sections. For example, fields added to the **Hidden section** can be moved to a visible section.

Add custom instructions to IPv4, multicast, and multi-device object change templates

You can add custom instructions for a template, or for a specific section of the template.

Note: Custom instructions are not supported for the **Hidden Fields** section.

Do the following:

1. Do one of the following:
   - To add custom instructions for the whole request form, at the top of the page, click **Type some instructions for this request form (will be visible to everyone)**.
   - To add custom instructions for a section of the request form, at the top of the section, click **Type some instructions for this section (will be visible to everyone)**.

   A text box appears.
2. Type the desired instructions in the box.
3. Click outside the text box to save your text and close the text box.
4. To remove the instructions, click  .

New Field for Change Request Fields

In this field...	Do this...
Name	Type the name of field.
Description	Type a description of field.
Display Name	Type the display name of the field. (The name that will appear for the field in the request form.)
Add To	Select the field type in the drop-down menu. The options in the menu depend on how/where you are creating the new field. • To create a general change request field that you can use in any section of the template, select **Change Request**. • To create a traffic field that appears at the bottom of each traffic line, select **Traffic**. • To create a traffic field that appears with the Source, Destination, Service, Application or User fields, select the relevant traffic item.

In this field...	Do this...
Enabled	Select the check box to enable the field (Default). Clear the check box to disable the field. Disabled fields cannot be included in request templates.
Type	Select the type of field in the drop-down menu.
Default Value	Type a default value for the field, if desired.
Validation	Select a validation method. Possible values are: • None. No validation for the field. (default) • Mandatory field. The field must be completed. • Custom. The field will be validated, according to the criteria you define. Type a regular expression in the text box. This field is only relevant for general change request fields (not traffic fields).
Link Values To	Type the location of the view properties to which to link.
Include Page	Type the location of the page to include.
Hide if Empty	Select the check box to hide the field if it is empty.

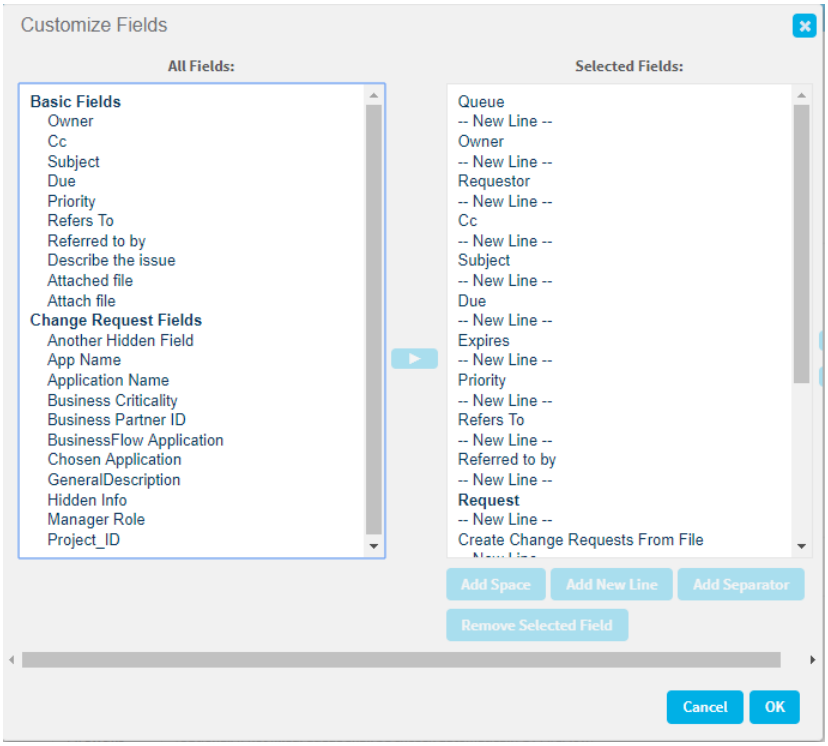
Modify fields for other request template types

When adding or editing request templates of any type other than IPv4 traffic and multicast, follow this procedure to add, remove, reorder, or reposition fields.

Do the following:

1. In the **Change Requests Fields** area, click **Customize Fields**.

   The **Customize Fields** dialog box appears.



2. Do any of the following:

   - To **add** a field, select it in the **All Fields** list box and click  .

     All custom fields defined in the system appear.

   - To **remove** a field, select it in the **Selected Fields** list box and click **Remove Selected Field**.

   - To **reorder** fields, do the following:

     - To move a field up, select it in the **Selected Fields** list box and click  .
     - To move a field down, select it in the **Selected Fields** list box and click  .

     Note: This controls the order of change request user defined custom fields only. The order of user defined custom fields for traffic fields or object fields are defined globally, not per template.

- To reposition fields, do the following:
  - To move the next field to a new line, click **Add New Line**.

    All fields listed between any two **--New Line--** actions will appear on one line. For example, you can use **Add New Line** to create a two-column request form.

    You can put user defined custom fields on one line together with FireFlow fields.
  - To move the next field a space to the right, click **Add Space**.

    The **--Space--** action serves as an empty field place holder. You can use **Add Space** to align the fields horizontally, as you desire.

Example

The following example shows how to use the **Add New Line** and **Add Space** actions to create a custom layout.

To create a form that looks like the following:

Subject	
Requestor	Cc
Due	Expires
	Application
	Business Unit

Configure the **Selected Fields** area as follows:

```
Subject
-- New Line --
Request
Cc
-- New Line –
Due
```

```
Expires
-- New Line –
-- Space –
Application
-- New Line --
-- Space –
Business Unit
```

Note: Application and **Business Unit** are user defined custom fields.

The custom fields appear in the template, in the position you specified.

Define request templates for specific scenarios

This topic describes how to define FireFlow to use specific templates in specific situations.

Specify a request template to use for disabling rules via Optimization reports

Do the following:

1. In the main menu, click **Request Templates**.

   The **Request Template** page appears with a list of existing templates.

2. In the **Templates for Requests from AlgoSec Firewall Analyzer** area, in the **Rules Cleanup Requests** field, select the desired rule removal template.

3. Click **Update**.

Specify a request template to use for removing objects via Optimization reports

Do the following:

1. In the main menu, click **Request Templates**.

   The **Request Template** page appears with a list of existing templates.

2. In the **Templates for Requests from AlgoSec Firewall Analyzer** area, in the **Objects Cleanup Requests** field, select the desired object change template.

3. Click **Update**.

Specify a request template to use for traffic change requests via a traffic simulation query

Do the following:

1. In the main menu, click **Request Templates**.

   The **Request Template** page appears with a list of existing templates.

2. In the **Templates for Requests from AlgoSec Firewall Analyzer** area, in the **Traffic Change Requests** field, select the desired traffic change template.

3. Click **Update**.

Specify a request template to use for requests submitted via the Blue Coat **Blocked** page

Do the following:

1. In the main menu, click **Request Templates**.

   The **Request Template** page appears with a list of existing templates.

2. In the **Templates for Requests From External Locations** area, in the **Blue Coat Requests** field, select the desired web-filter template.

3. Click **Update**.

Disable / enable request templates

You can disable any template, including built-in templates. Disabled templates do not appear in the **Create a New Change Request** page. Disabled templates can easily be re-enabled when desired.

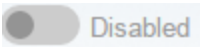
Disable a request template

Do the following:

1. In the main menu, click **Request Templates**.

   The **Request Template** page appears with a list of existing templates.
2. Click on the name of the template which you want to disable.

   The template's page appears.
3. Do one of the following:
   - For IPv4 traffic and multicast request templates, click  .

     The icon changes to 

.
   - For other templates, clear the **Template Enabled** check box.
4. Click **Save template**.

The template is disabled.

Enable a request template

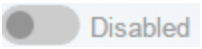
Do the following:

1. In the main menu, click **Request Templates**.

   The **Request Templates** page appears with a list of existing templates.
2. Click the **Show Disabled** link.

   All disable request templates appear in the list.
3. Click on the name of the template which you want to enable.

The template's page appears.

4. Do one of the following:
   - For IPv4 traffic and multicast request templates, click 

.

     The icon changes to  .
   - For other templates, check the **Template Enabled** check box.
5. Click **Save template**.

The template is enabled.

Configure initial plan device group conditions

This topic explains how to configure custom conditions for which device group to query during initial planning.

Create new initial plan conditions

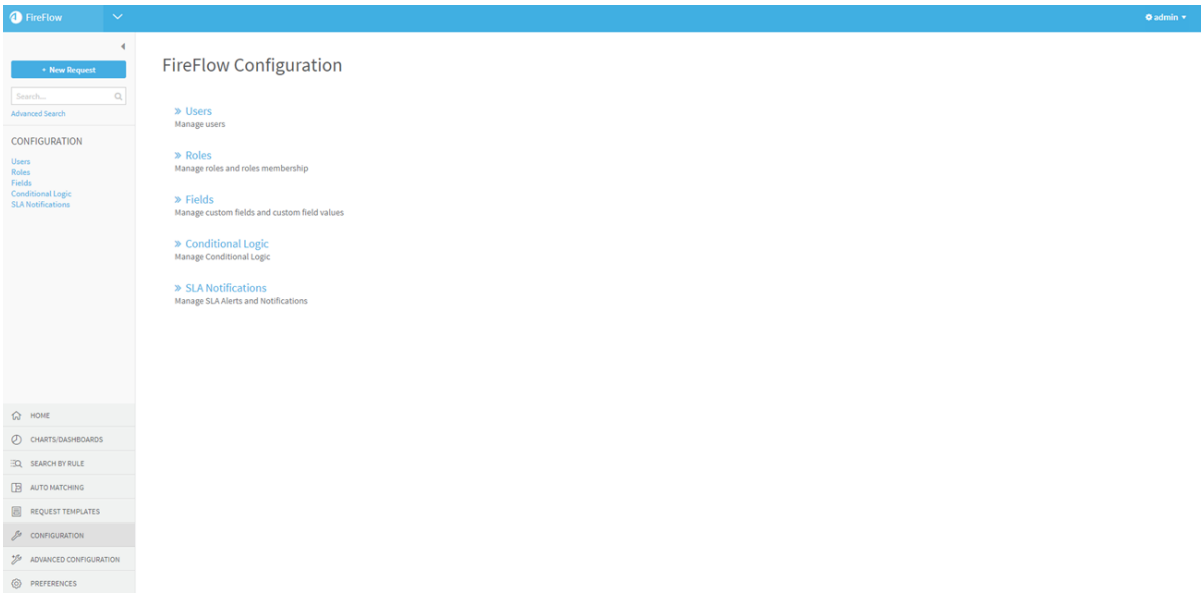
When a traffic change request enters the Initial Plan stage, FireFlow determines which devices are relevant for the change request with an AFA traffic simulation query on a group of devices. By default, the traffic simulation query is always run on the ALL_FIREWALLS group. If desired, you can specify conditions for when the query should run on a different AFA defined device group.

Note: Conditions configured for the initial plan device group in the FireFlow web interface take precedence over any conditions specified with the **GetFirewallGroupName** (see GetFirewallGroupName) hook.

Do the following:

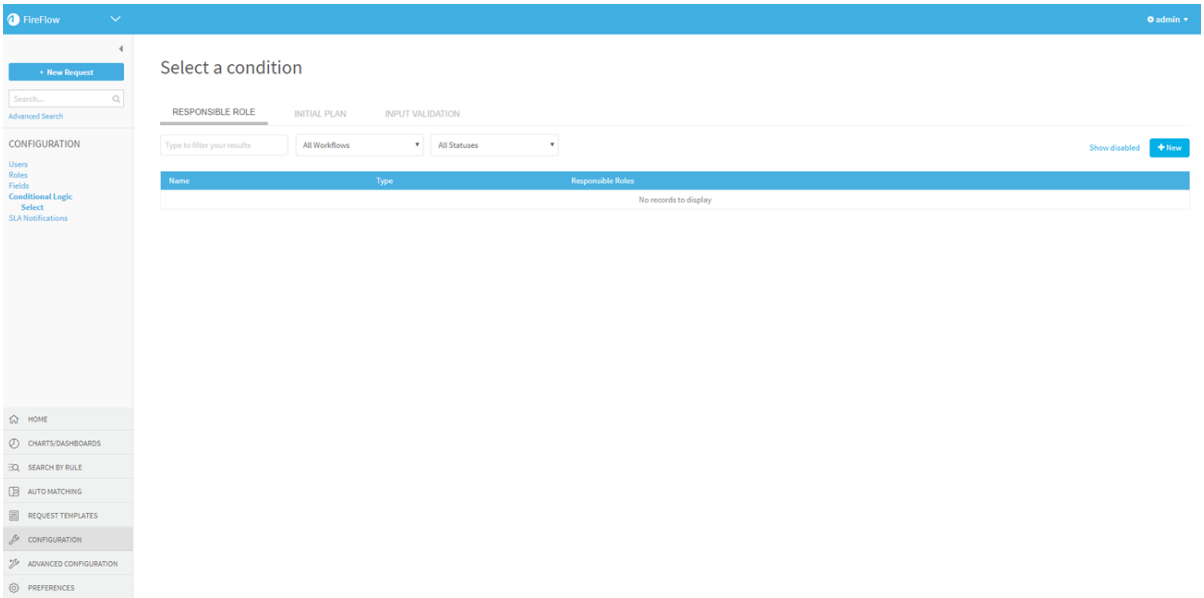
1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

The **FireFlow Configuration** page appears.



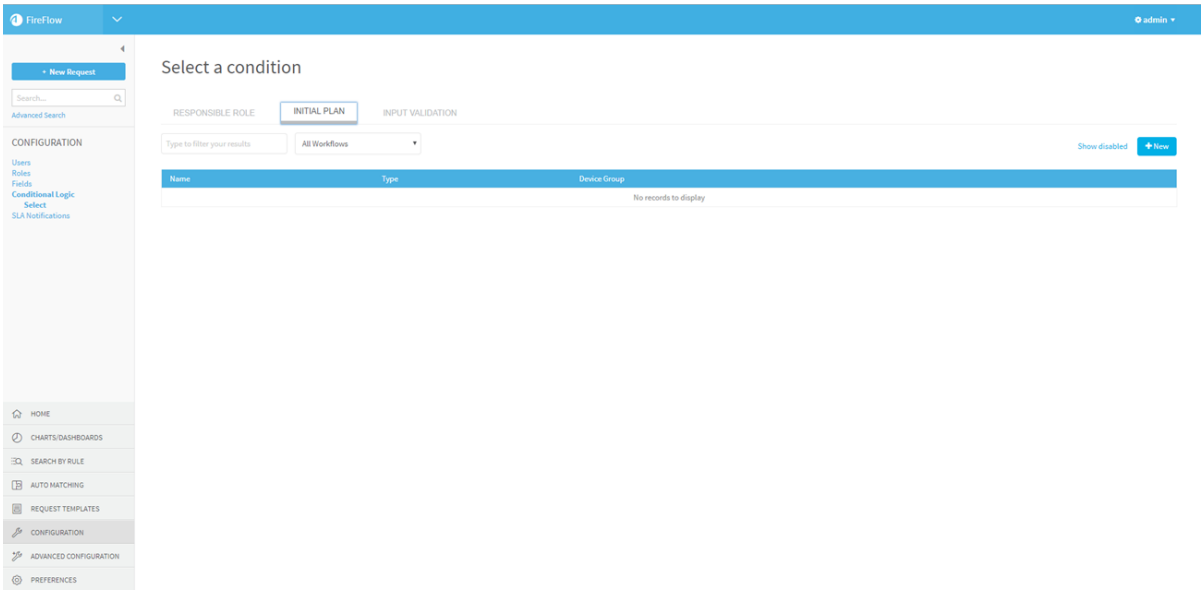
3. Click **Conditional Logic**.

   The **Select a condition** page appears.



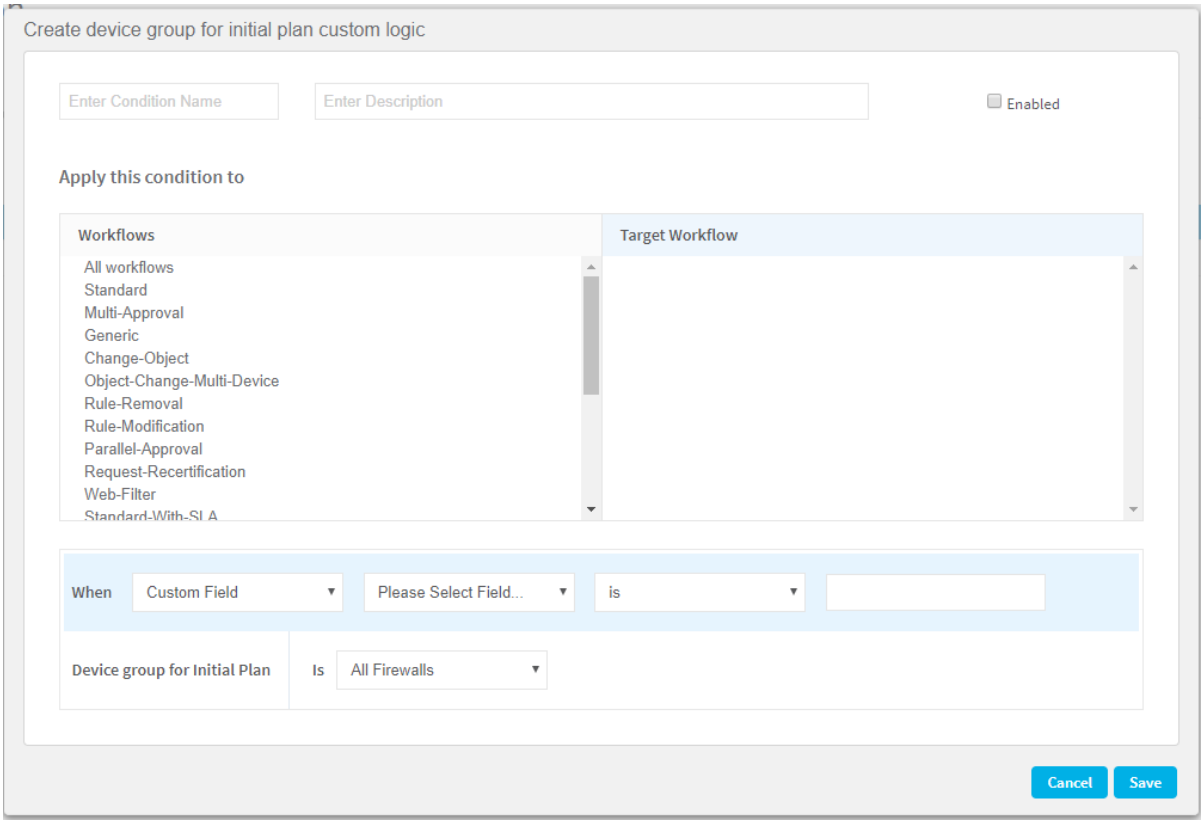
4. Click the **Initial Plan** tab.

   The **Initial Plan** tab appears.



5. Click **+ New**.

The **Create device group for initial plan custom logic** window appears.



6. Complete the fields using the relevant information in Initial Plan Custom Logic Fields (see Initial Plan Custom Logic Fields).
7. Click **Save**.

Initial Plan Custom Logic Fields

In this field...	Do this...
Enter Condition Name	Type a name to represent the condition.
Enter Description	Type the description of the condition.
Enabled	Select this check box to enable the condition.
Apply this condition to	Select the relevant workflows. The selected workflows appear in the **Target Workflow** list. To remove a status, click the status in the **Target Workflow** list.
When	Define the condition by selecting the condition type in the drop down menu and completing the relevant fields. • For the **Custom Field** condition type, select the field, select the boolean operator, and type the value for the field. • For the **Traffic** condition type, select the relevant endpoint(s), select the boolean operator, and type the IP address, range or CIDR for the field. **Note:** The **Traffic** condition type is only for traffic change request workflows.
Device group for Initial Plan is	In the drop-down list, select the device group which should be used for the Initial Planning traffic simulation query for change requests which meet the defined conditions.

Configure field input validation

This topic explains how to configure input validation for change request fields.

Create new conditions for change request fields

If desired, you can define specific conditions for the values provided for certain change request fields in the request template. FireFlow will enforce these custom conditions by validating these fields when the change request is created and anytime the field is edited. You can additionally configure custom error messages to accompany each field condition.

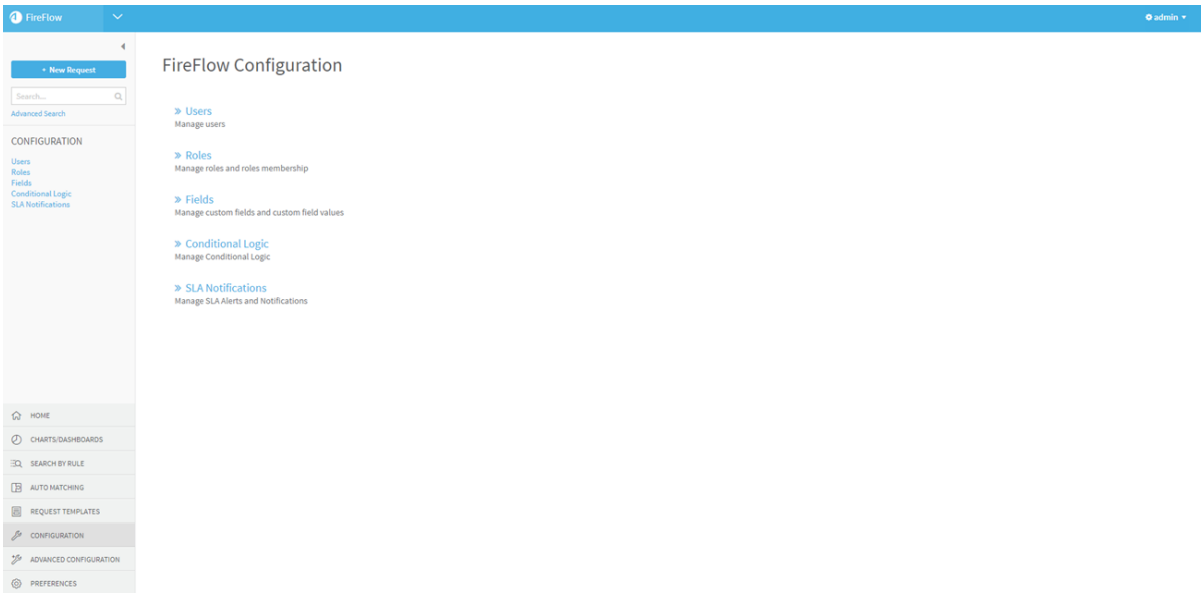
Note: Any conditions configured for change request validation with the **ValidateTicket** (see ValidateTicket) hook will additionally cause validation to fail.

Note: Input validation for change request fields is only supported for traffic change request templates (IPv4 only).

Do the following:

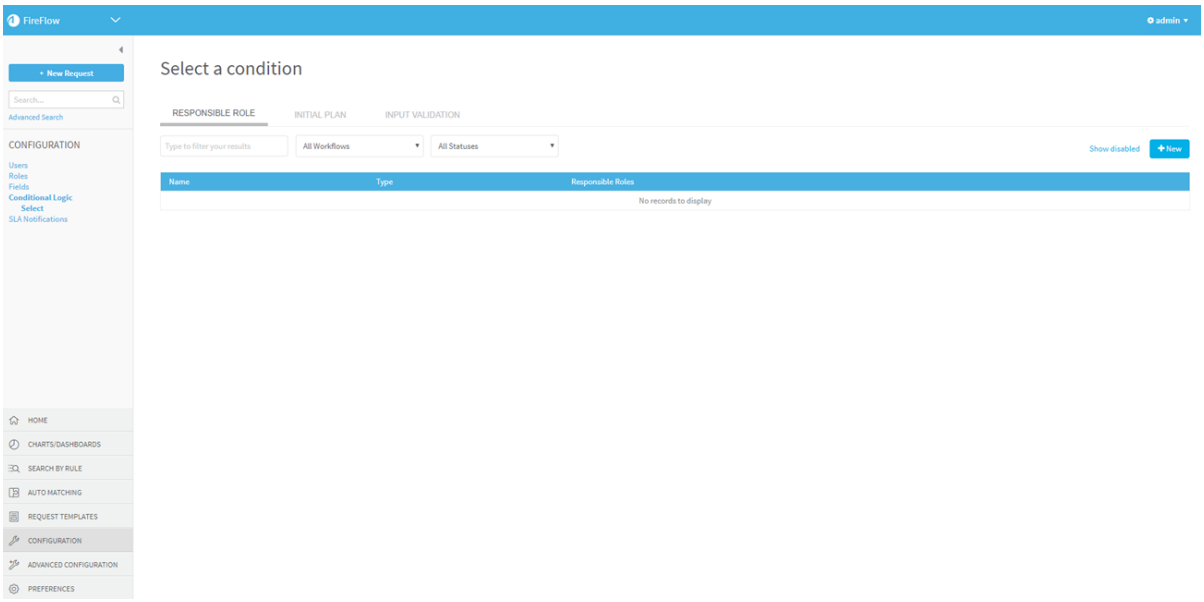
1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page appears.



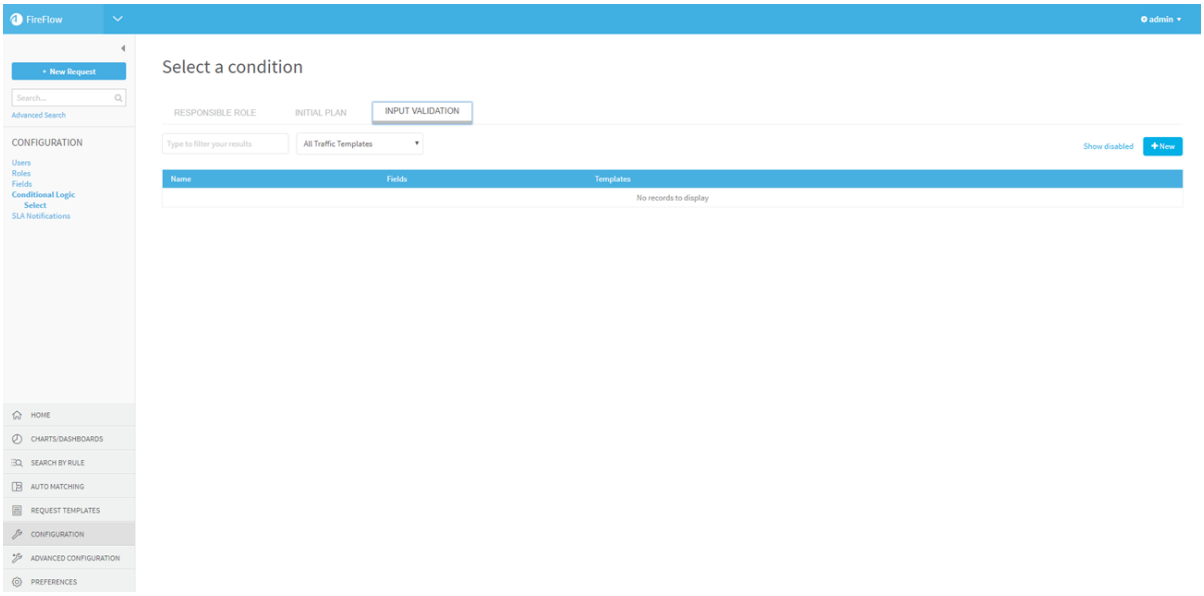
3. Click **Conditional Logic**.

   The **Select a condition** page appears.



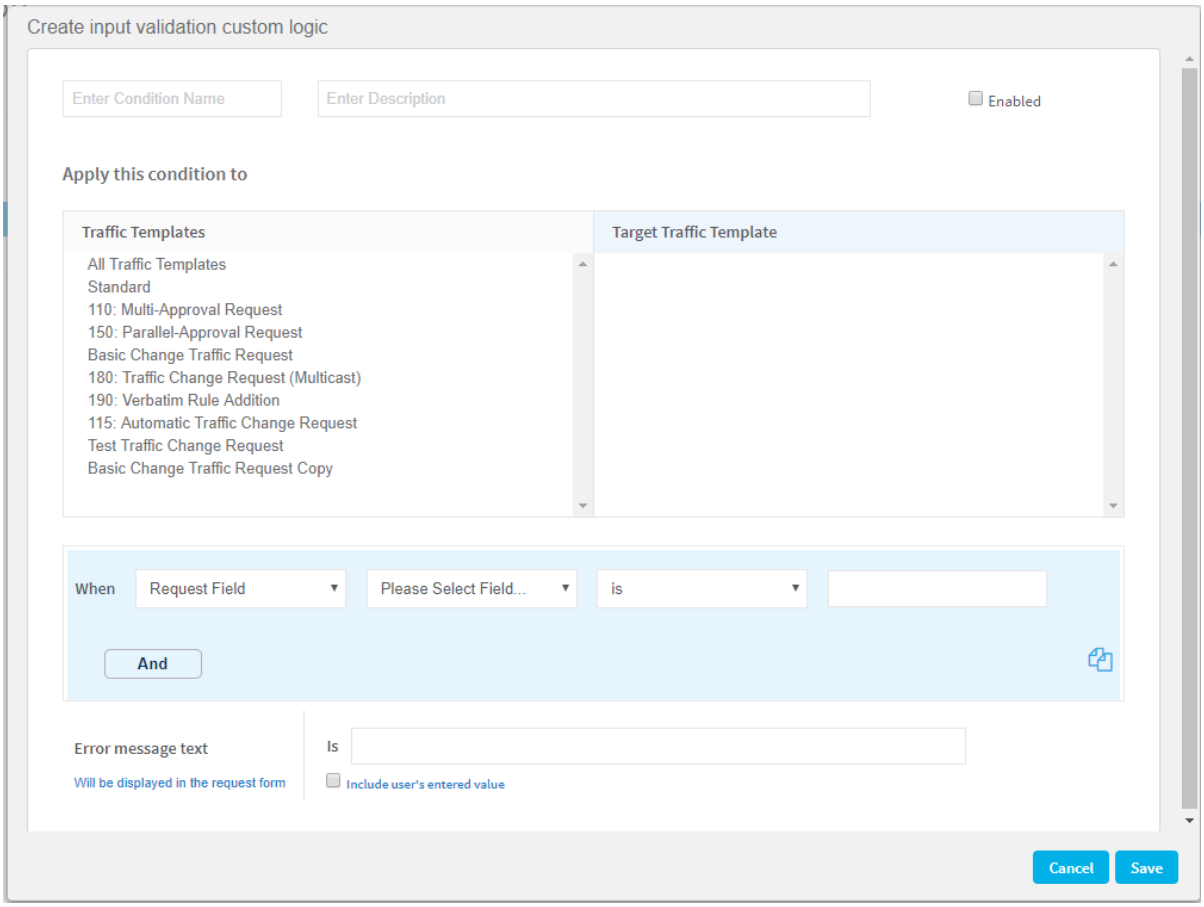
4. Click the **Input Validation** tab.

   The **Input Validation** tab appears.



5. Click +New.

The **Create input validation custom logic** window appears.



6. Complete the fields using the relevant information in Input Validation Custom Logic Fields (see Input validation custom logic fields).
7. Click **Save**.

Input validation custom logic fields

In this field...	Do this...
Enter Condition Name	Type a name to represent the condition.
Enter Description	Type the description of the condition.

In this field...	Do this...
Enabled	Select this check box to enable the condition.
Apply this condition to	Select the relevant traffic change request templates. The selected templates appear in the **Target Traffic Template** list. To remove a template, click the status in the **Target Traffic Templates** list.
When	Define the condition by selecting the condition type in the drop down menu and completing the relevant fields. You define the condition(s) for which you want the input validation to *fail*. • For the **Request Field** condition type, select the field, select the boolean operator, and type the value for the field. **Note:** For the operators **has format** and **does not have format**, all regular expressions are supported as input. • For the **Traffic** condition type, select the relevant endpoint(s), select the boolean operator, and type the IP address, range or CIDR for the field. • For the **Status** condition type, select the boolean operator and select the status.
AND	Click this to add another condition. **Note:** Validation will fail only when all conditions are true.
	Click this to duplicate a condition. This enables you to easily create an additional condition based on an existing one.
	Click this to remove a condition.
Error Message text is	Type the error message you want to appear when the condition(s) are true and validation therefore fails.

In this field...	Do this...
Include user's entered value	Select this check box to include the user's input in a field in the error message. The **Please Select Field...** drop down menu appears.
Please Select Field...	Select the desired field in the drop-down menu. In the error message, type <FIELD_VALUE> where you want the field value to appear. For example, "<FIELD_VALUE> is not a supported value."

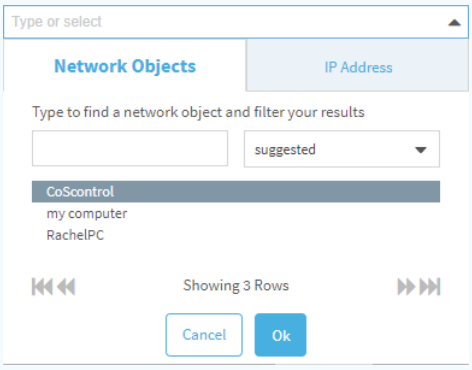
Customize change request wizards

When defining traffic in a change request, FireFlow provides suggested sources, destinations, and services. FireFlow allows you to customize which objects appear as options.

Configure the suggested sources / destinations list

When defining traffic in a change request, the **Source** and **Destination** fields provide wizards which help you select network objects. By default, the **suggested** list of objects appears when the wizard opens. You can configure objects to appear in this list, for example "email server" or "my computer", enabling the user to specify a common source or destination without knowing its IP address.

Note: If desired, you can change the default list of objects for the choose source/destination wizard. For details, see Configuring the Default Network Object Category in the Choose Source/Destination Wizard .



Do the following:

1. Log in to the FireFlow server using the username "root" and the related password.
2. Under the directory `/usr/share/fireflow/local/etc/`, locate the file `SuggestedAddressObjects_Config.xml`.

   Note: This is the original suggested sources/destinations list file, and it can be used to revert to defaults, as needed. Do not modify this file.

3. Under the directory `/usr/share/fireflow/local/etc/site/`, copy the contents of the original file into an override file that is also called `SuggestedAddressObjects_Config.xml`.
4. Open the override file.
5. To add a suggested source/destination to the list, add a new `object` tag inside the the `objects` tag.

   ```
   <object name="objectName" [ipversion="ipVersion"]>
       <value>objectValue</value>
   </object>
   ```

   Where:

- *objectName* is the source/destination name that should appear in the **suggested** list.
- *objectValue* is the value to which FireFlow should resolve the source/destination name. This can be a single IP address, an IP address range, or a network(CIDR).
- *ipVersion* is `ipv4` or `ipv6`.

  The default value is `ipv4`.

Note: All optional elements of the tag appear in square brackets **[ ]**

Note: The object "my computer" is a built-in suggested object. FireFlow resolves it to the IP address of the user's computer (the local host).

6. To remove an object from the list, delete the relevant tags.
7. Save the override file.
8. Restart FireFlow. For details, see Restart FireFlow.

Configuring the Default Network Object Category in the Choose Source/Destination Wizard

The default network object category in the source/destination wizard is the list of **suggested** objects. If desired, you can configure a different category of network objects to be the default list.

Using the generic procedure for overriding system defaults, set the following configuration parameter. For details, see Override FireFlow system defaults.

Configuration Parameter Name	Value
`RequestedObjectsRepository`	The desired default object repository. Possible values are the following: • `suggested`. The **suggested** list. (default). For details, see Configure the suggested sources / destinations list. • `all firewalls`. All network objects defined on all existing devices. • The name of any group defined in AFA. All network objects defined on all devices in the group.

Define protocols

When defining traffic in a change request, the **Service** field provides a wizard which helps you select service objects. The **common** list of objects appears when the wizard opens. If desired, you can define additional services which will appear in this list.

Defining new protocols in this manner additionally enables you to manually add support for any layer 3 protocol. By default, FireFlow supports all standard services (TCP, UDP, and ICMP), as well as many layer 3 protocols.

Do the following:

1. Log into the AlgoSec server using the username "root" and the related password.
2. Create a new file **/home/afa/.fa/user_def.srv**, and add the following to the file:

```
## User defined services declarations.#SERVICES {


}
```

   If the above file already exists, go to the next step.

3. Under the Services line (inside the brackets), add the service using the following syntax:

```
xxx = { ##[*] }
```

where **xxx** is the name of the service and **##** is the protocol number.

You can define groups using the following syntax:

xxx = { #1[*] }

yyy = { #2[*] }

zzz = {**xxx**,**yyy**}

where zzz is a service object containing **xxx** and **yyy**.

> **Note:** When defining groups, you must first define the content protocols of the group with names, and use the names of the content protocols when defining the group.

4. Save the file.
5. Restart FireFlow. For details, see Restart FireFlow.

Customize tabs for selecting objects

When defining traffic in a change request, the **Source**, **Destination**, and **Service** fields provide wizards which help you select network objects. By default, all tabs appear for authenticated users, and only the **common** tab appears for users using the No-Login Web Form.

For more details, see:

- Customize tabs for selecting objects per role
- Customize tabs for selecting objects for anonymous sers

Note: All permissions granted to anonymous users are automatically granted to authenticated users. Granting permissions to anonymous users overrides any permissions denied per role.

Customize tabs for selecting objects per role

Note: Global configurations for anonymous users will override specific role permissions. For more details, see Customize tabs for selecting objects for anonymous sers .

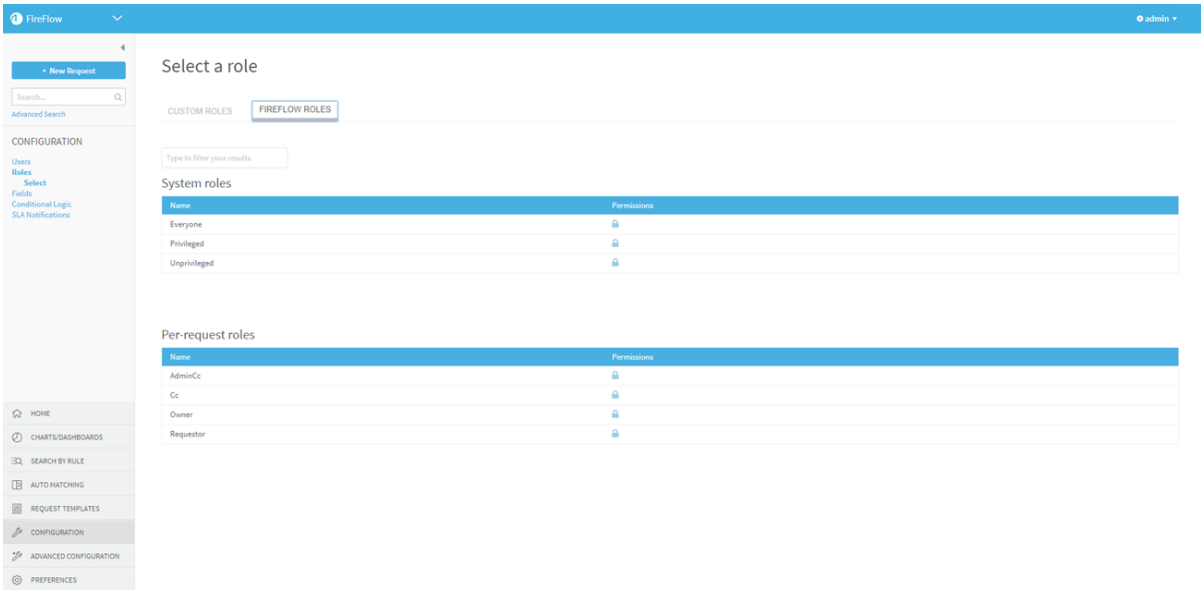
Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page appears.
3. Click **Roles**.

   The **Select a role** page appears.
4. Click the **FireFlow Roles** tab.

   The **FireFlow Roles** tab appears.



5. (Optional) To display disabled roles, click the **Show disabled** link.

   To revert to a list which only displays enabled roles, click the **Hide disabled** link.

6. (Optional) To search for the desired role, type your search in the **Type to filter your results** field.

   The roles which match your search appear in the **Functional roles** area.

7. In the row of the relevant role, click .

   The **Manage Permissions** window for the role you desire appears.

   > **Note:** For requestors, the relevant role is **Unprivileged**.

8. Click › next to **Basic**.

   The **Basic** sub-permissions appear.

9. To allow users with this user role to view tabs, select any of the following permissions:

   - To allow users with this role to view the **suggested** tab when choosing sources or destinations, select the check box next to **SeeSuggestedAddressObjects**.

- To allow users with this role to view device objects when choosing sources, destinations, or services select the check box next to **SeeFirewallAddressObjects**.
- To allow users with this role to view the **common** tab when choosing services, select the check box next to **SeeCommonServiceObjects**.

10. Click **Save**.

Customize tabs for selecting objects for anonymous sers

Note: These parameters configure both authenticated requests and requests from the No-Login Web Form. They override permissions for specific roles. For more details, see Customize tabs for selecting objects per role.

Do the following:

Using the generic procedure for overriding system defaults, set the following configuration parameter. For details, see Override FireFlow system defaults.

Configuration Parameter Name	Description	Value
`AllowAnonymousUserSeeSuggestedAddressObjects`	Controls whether the **Suggested** tab appears when choosing a source or destination.	**1**. To display the tab. **0**. To not display the tab. (Default)
`AllowAnonymousUserSeeFirewallAddressObjects`	Controls whether device objects appear when choosing a source, destination, or service.	**1**. To display the tab. **0**. To not display the tab. (Default)

Configuration Parameter Name	Description	Value
`AllowAnonymousUserSeeCommonServiceObjects`	Controls whether the **Common** tab appears when choosing a service.	**1**. To display the tab. (Default) **0**. To not display the tab.
`AllowAnonymousUserSeeApplicationsObjects`	Controls whether device objects appear when choosing applications.	**1**. To display the tab. **0**. To not display the tab. (Default)

Note: After setting these parameters you must restart FireFlow for the changes to take affect. For details, see Restart FireFlow.

Configure object names to appear with device names

By default, the object names that appear as options do not specify which device they are defined on. If desired, you can configure FireFlow to display the device name for each object in the following format:

```
object_name:device_name
```

Do the following:

Using the generic procedure for overriding system defaults, set the following configuration parameter. For details, see Override FireFlow system defaults.

Configuration Parameter Name	Value
`StoreFirewallSuffixInHostGroup`	**0**. To specify network objects should not appear with their device name. (Default) **1**. To specify network objects should appear with their device name.
`StoreFirewallSuffixInServiceGroup`	**0**. To specify service objects should not appear with their device name. (Default) **1**. To specify service objects should appear with their device name.

Note: After setting these parameters you must restart FireFlow for the changes to take affect. For details, see Restart FireFlow.

Add rule documentation for allowing rules

You can add rule documentation to the allowing (and partially allowing) device rules for a change request.

AFA finds these rules during the initial plan and validation queries, and when configured to do so, FireFlow stores the results in FireFlow fields.

You can access these rules and add documentation to them with your own custom scrip. The initial plan results are returned in XML format, and the validation results are returned in JSON format.

Add rule documentation

Do the following:

1. If you want to add rule documentation to allowing rules found in the initial plan query, configure FireFlow to store the allowing rules from the initial plan query. See Enabling/Disabling Storing Allowing Rules From the Initial Plan Query (see Enabling/Disabling Storing Allowing Rules from the Initial Plan Query).

For each change request, after Initial Planning, the allowing rules found in the initial plan query will be stored in FireFlow.

Note: If you want to add rule documentation to allowing rules found in the validation query, no FireFlow configuration is required. FireFlow always stores the allowing rules found in the change validation query.

2. Write a scrip to access the desired FireFlow field (see below) to get the list of rules, iterate them, and use the rule documentation API to add the rule documentation.

For allowing rules from the...	Access this FireFlow field...
Inital plan query	Initial Plan Results
Validation query	Validation Results

Both fields can be obtained from the ticket object. Once obtained, the initial plan results can be easily parsed as XML (see the example output below). The change validation results are in less readable JSON format. Therefore, they have a function that assists parsing the result which is `Ticket_Vendor::getAllowingRulesFromValidation`.

Allowing rules output format

For rules on Cisco devices, the rule ID will be in the HexUID field in the hash. All other brand's rule IDs will be in the UID field.

In the initial plan results, all the hash keys are lower-case, and in the validation results they are upper-case. For example, in the initial plan results, "uid" will appear as "uid", and in the validation results, "uid" will appear as "UID".

For more details, see:

- Initial plan allowing rules example
- Validation allowing rules example

For additional assistance, contact AlgoSec Professional Services.

Initial plan allowing rules example

```
<firewall data_time="installed-2013-06-10-113342" dst_default_routed="0"
name="10_20_110_1" src_default_routed="1" status="Partially Blocked">
<allowRules>
<rule hexuid="" num="51" rule_name="" uid="nantest2"
url="orig_rules.html?row=rule_nantest2" />
<rule hexuid="" num="59" rule_name="" uid="yaara_tmp_2"
url="orig_rules.html?row=rule_yaara_tmp_2" />
<rule hexuid="" num="36" rule_name="" uid="ssh_access" url="orig_rules.html?
row=rule_ssh_access" />
</allowRules>
<report receiveddate="2013-05-24 09:46:44" reportname="afa-6136" />
</firewall>
```

Validation allowing rules example

```
$VAR1 = [
{
'URL' => 'orig_rules.html?row=rule_20',
'UID' => '{C39F56C5-F985-4AD1-A0BE-B5162603FAD7}',
'Comment' => 'FireFlow #230FireFlow #954',
'Destination' => [
'a_10.110.17.82',
'a_10.110.17.66'
],
'Service' => [
'ftp'
],
'Number' => '20',
'Action' => 'accept',
'Application' => [],
'HexUID' => undef,
'Class' => 'FireFlow::WorkOrder::WorkOrderTrafficRule',
'Source' => [
```

```
'a_10.10.17.5'
],
'Name' => undef,
'DisplayId' => '20'
},
{
'URL' => 'orig_rules.html?row=rule_6',
'UID' => '{A0A2DD57-D0E6-4BDA-8EC3-59927B078228}',
'Comment' => '',
'Destination' => [
'Any'
],
'Service' => [
'Kaos'
],
'Number' => '6',
'Action' => 'accept',
'Application' => [],
'HexUID' => undef,
'Class' => 'FireFlow::WorkOrder::WorkOrderTrafficRule',
'Source' => [
'Any'
],
'Name' => undef,
'DisplayId' => '6'
},
```

Configure change request creation from file

This section explains how to configure change request creation from file.

Change request from file process

Requestors can create new change requests from files attached to change requests. The process is as follows:

1. The requestor chooses a request template that supports creating change requests from file, such as FireFlow's built-in sample template "240: Sample - Upload change requests from Excel". The requestor then attaches a file specifying the desired change's details.

   Note: In order to support creating change requests from a file, a request template's **Create change requests from file** field must be set to **Yes**, and the **Request Type** field must be set to **Generic Change**.

2. The requestor submits the change request.
3. FireFlow runs a parsing script that converts the attached file to XML format.

   If the parsing script is configured for single change request creation, then all traffic lines in the file are interpreted as multiple traffic lines in a single change request. If the script is configured for multiple change request creation, each traffic line in the file is interpreted as a separate change request, and the change requests will all be linked to each other via their **Depends On** field.

4. FireFlow converts the XML file to one or more change requests.

   By default, FireFlow uses an out-of-the-box parsing script, `/usr/share/fireflow/local/bin/parse_excel_example.pl`, which supports creating multiple change requests from a file, where all of the change request data is on a single worksheet, and the file format is one of the following:

   - xls (Microsoft Excel up to 2003)
   - xlsx (Microsoft Excel 2007 and up)
   - sxc (OpenOffice 1.0 Spreadsheet)

- ods (OpenOffice Spreadsheet)
- csv (Coma-separated text values)

If desired, you can customize change request creation from a file in the following ways:

- Enable the creation of change requests from files in additional formats.
- Configure whether multiple or single change requests are created from each file.
- Enable/disable file validity enforcement.

  By default, FireFlow automatically checks uploaded files for errors. If an error is detected in a file, FireFlow alerts the requestor and halts change request creation for this file, until the error has been fixed. If desired, you can disable validity enforcement, in which case change requests will be created only from valid lines in the file.
- Enable/disable automatic change request creation.

  By default, FireFlow automatically creates change requests from uploaded files. If desired, you can require change request creation to be triggered manually later in the change request workflow, when a certain button is clicked. For information on how to perform this customization, contact AlgoSec Support.
- Disable change request creation from a file (both automatic and manual).

To view a sample worksheet filled with data that is expected by the out-of-the-box parsing script, see `/usr/share/fireflow/local/extras/Firewall Rules Request example.xls`.

Configure change request creation from file

Note: If you are using multiple parsing scripts, you must perform this procedure for each script.

Do the following:

1. To enable the creation of change requests from files in a format that is not supported by the default parsing script, obtain a custom parsing script from AlgoSec Professional Services.
2. Log in to the FireFlow server using the username "root" and the related password.
3. Do one of the following:
   - To work with the default parsing script, copy `parse_excel_example.pl` from `/usr/share/fireflow/local/bin/` to `/usr/share/fireflow/local/etc/site/bin/`.
   - To work with a custom parsing script, save the custom script under `/usr/share/fireflow/local/etc/site/bin`.
4. Give the parsing script execute permissions, by running the following command:

   ```
   chmod a+x [script-name]
   ```

   Where *script-name* is the name of the parsing script.
5. Use the generic procedure to set the configuration parameters described below. For details, see Override FireFlow system defaults.

Configuration Parameter Name	Description	Value
`AttachmentParsingScripts`	Setting this parameter is required to configure change request creation from a file.	The path of the parsing script. For example, **"/usr/share/fireflow/local/etc/site/bin/custom_parsing_script1.pl" => ["xls", "xlsx", "sxc", "ods", "csv"]** Seperate multiple parsing script paths with commas

Configuration Parameter Name	Description	Value
`AutoCreateTicketsFromAttachments`	Enables/disables automatic creation of change requests from files.	**1.** To enable automatic creation of change requests from uploaded files. (Default) **0.** To require manual triggering of change request creation from uploaded files.
`ForceValidAttachmentsBeforeCreateTickets`	Enables/disables validity enforcement for uploaded files.	**1.** To enable validity enforcement for uploaded files. (Default) **0.** To disable validity enforcement for uploaded files.

6. To configure whether multiple change requests or a single change request is created from a file, do the following:
    a. Under `/usr/share/fireflow/local/etc/site/bin/`, open the parsing script.
    b. Locate the following lines:

```
# In this example: Multiple tickets modemy $mode =
$MULTIPLE_TICKETS_MODE;# Set mode to $SINGLE_TICKETS_MODE
if you wish to work in single ticket mode# my $mode =
$SINGLE_TICKETS_MODE;
```

    c. Uncomment the `my $mode` line that reflects the mode you want to use, and comment the `my $mode` line that reflects the mode you do not want to use.
    d. For example, to create a single change request from file, modify the lines as follows:

```
# In this example: Multiple tickets mode# my $mode =
$MULTIPLE_TICKETS_MODE;# Set mode to $SINGLE_TICKETS_MODE
if you wish to work in single ticket modemy $mode =
$SINGLE_TICKETS_MODE;
```

e. Save the script.

f. Restart FireFlow.

Disable change request creation from file

Using the generic procedure for overriding system defaults, disable the configuration parameter `AttachmentParsingScripts`. For details, see Override FireFlow system defaults.

Note: After disabling this parameter, you must restart FireFlow for the change to take affect. For details, see Restart FireFlow.

Manage custom fields

This topic describes how to manage FireFlow custom fields.

FireFlow custom field types

FireFlow includes two types of custom fields:

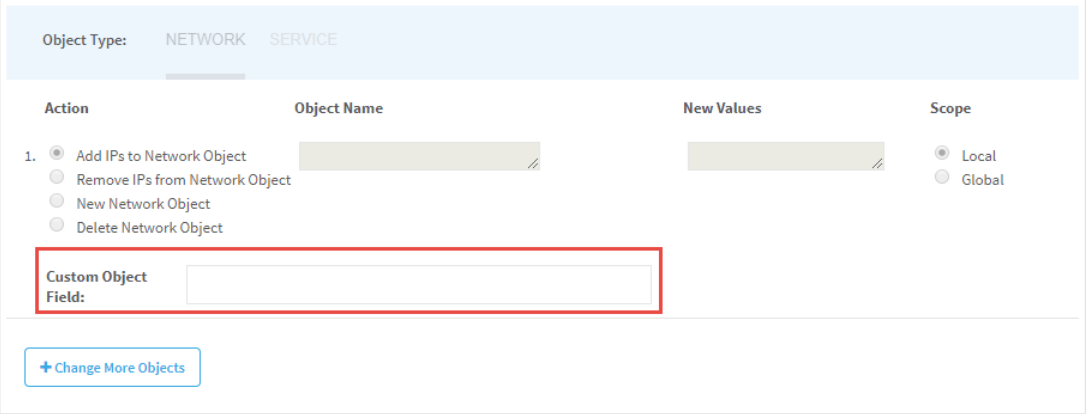
- User-defined fields
- FireFlow fields

Tip: You can edit, disable, configure the order of, and configure roles' permissions for custom or FireFlow fields.

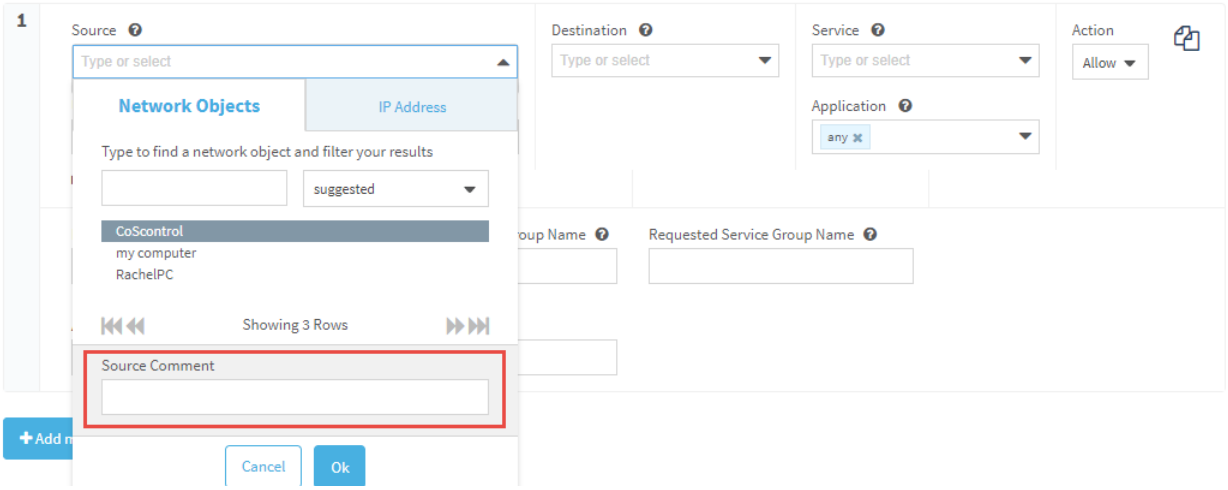
For more details, see Manage user permissions.

User-defined fields

You can define custom fields and add them to change requests, users, or user roles throughout the FireFlow user interface. For example, you can add a budget number field in change requests or an extension number field for users. In addition, it is possible to add custom fields to traffic change request traffic fields or object changes.



Custom fields for traffic fields can be added as an additional field (similar to custom fields for object changes) or as a field related to the Source, Destination, Service, Application or User fields.



FireFlow fields

FireFlow comes with a set of built-in custom fields called *FireFlow fields*. You can modify the display name and description of such fields.

All FireFlow fields appear in the Standard request template.

Note: For additional information on Cisco User Awareness - How to Define a User/User Group in a Rule, see this AlgoPedia Knowledge Base article.

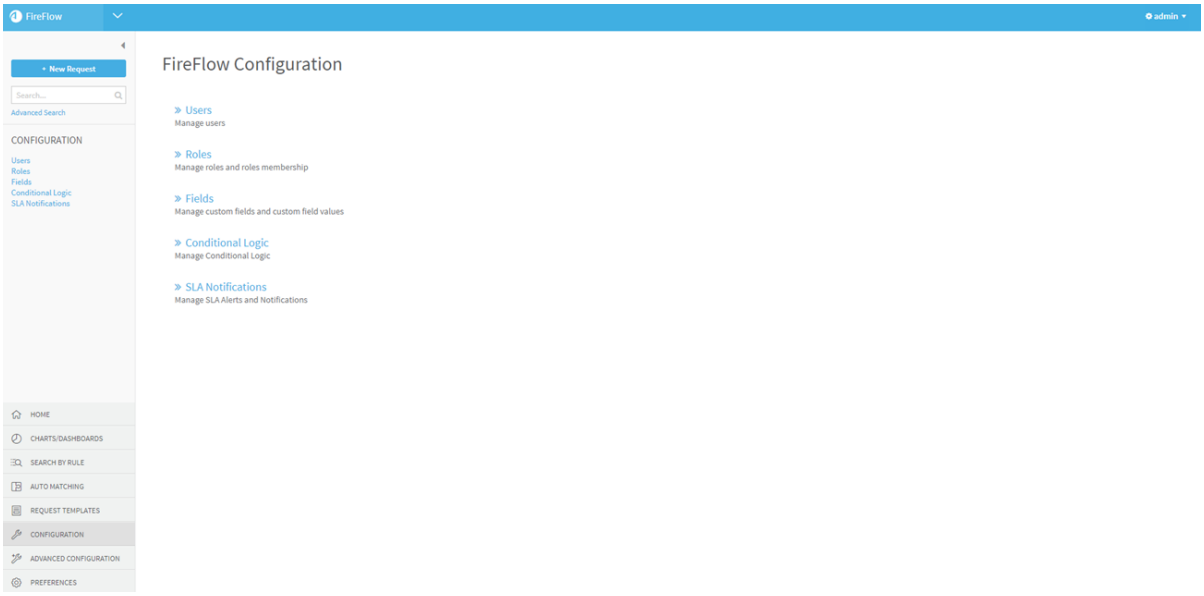
Add user-defined fields

Note: You cannot add user-defined custom fields that have the same name as a built-in FireFlow field. To view a list of built-in FireFlow fields, click **Advanced Configuration > FireFlow Fields**.

Do the following:

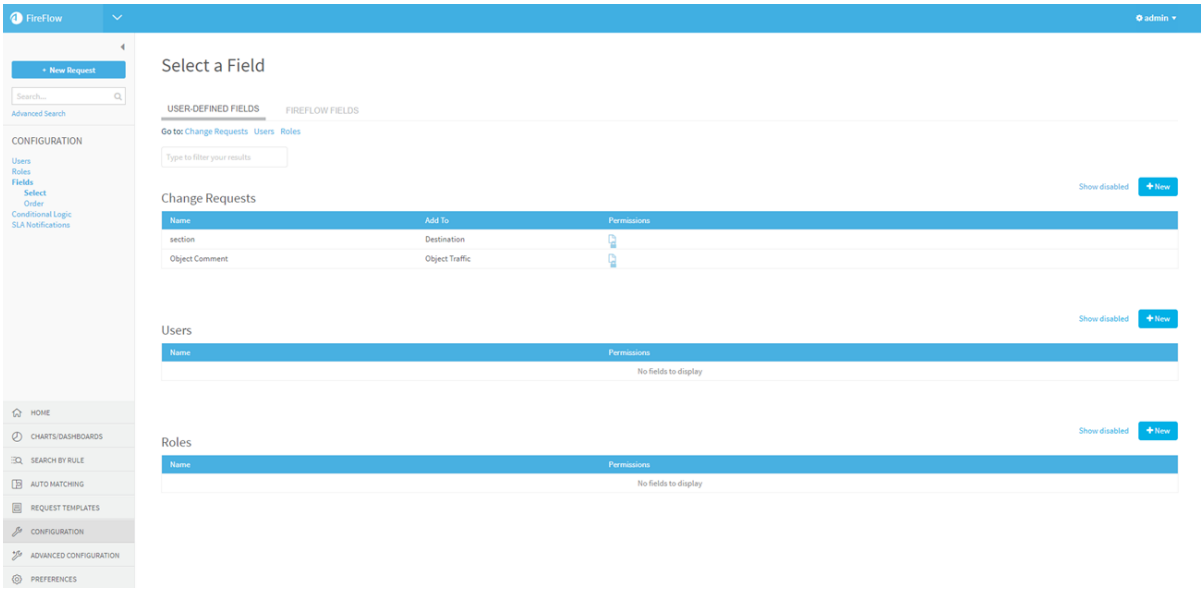
1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page appears.



3. Click **Fields**.

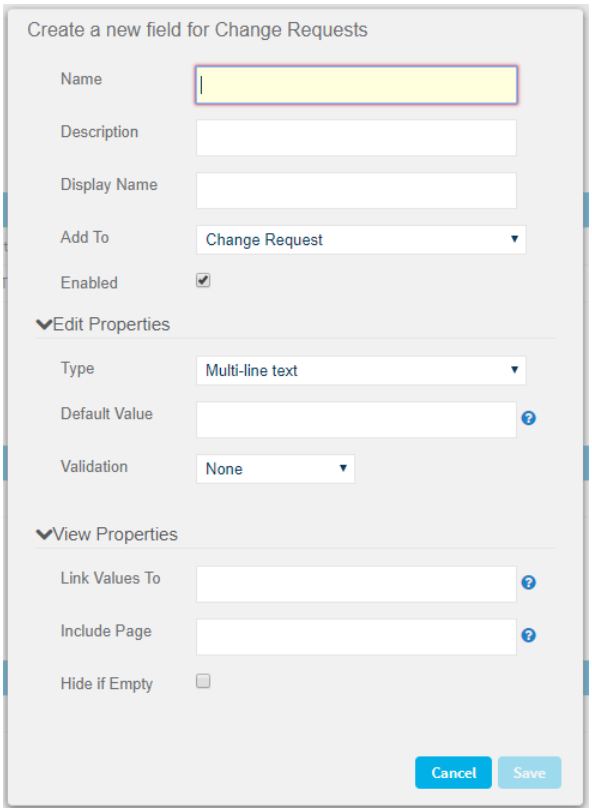
   The **Select a Field** page appears.



4. In the area for the type of field you want to add, click **+ New**.

   For example, if you want to add a custom field to change requests, click **+ New** in the **Change Requests** area.

   The **Create a New Change Requests Field** window appears.



5. Complete the fields using the relevant information in Custom Field Page Fields (see Custom Field Page Fields).
6. Click **Save**.

   The new field appears throughout the FireFlow user interface.

Note: By default, all user roles (including the Unprivileged role) are granted permission to view and modify the new custom field, except for the Read-Only role, which is only granted permission to view the new custom field. The Admin role is additionally granted permission to manage the new custom field.

For more details, see Manage user permissions.

Custom Field Page Fields

In this field...	Do this...
Name	Type a name to represent the field internally. This field is mandatory and must be filled in with a unique value containing any of the following: letters, digits, hyphen, underscore, dots, and spaces. **Note:** This is *not* the name that users will see in the FireFlow interface.
Description	Type a description of the field. This description will appear as a tooltip, when you mouse-over the custom field's name in the **Create Change Request** page.
Display Name	Type the name that should represent the field in the FireFlow interface.

In this field...	Do this...
Add To	Select the field's category. This can be any of the following: • **Change Request:** Allows creating a generic custom field for change requests. • **Hidden:** Allows creating a custom field which is not displayed. • **Source:** Allows creating a custom field that appears below a traffic change request's **Source** field. For example, select this category if you want to add a comment field next to a traffic source. • **Destination:** Allows creating a custom field that appears below a traffic change request's **Destination** field. For example, select this category if you want to add a comment field next to a traffic destination. • **Service:** Allows creating a custom field that appears below a traffic change request's **Service** field. For example, select this category if you want to add a comment field next to a traffic service. • **User:** Allows creating a custom field that appears below a traffic change request's **User** field. For example, select this category if you want to add a comment field next to a traffic user. **Note:** The **User** field only appears in FireFlow when user awareness is enabled. See Enabling/Disabling User and Network Application Awareness (see Enable / disable user and network application awareness). • **Application:** Allows creating a custom field that appears below a traffic change request's **Application** field. For example, select this category if you want to add a comment field next to a traffic application. **Note:** The **Application** field only appears in FireFlow when application awareness is enabled. See Enabling/Disabling User and Network Application Awareness (see Enable / disable user and network application awareness). • **Traffic:** Allows creating a custom field for each traffic change in a traffic change request. For example, select this category if you want to add a comment field to each line of traffic in a change request.

In this field...	Do this...
	• **Object:** Allows creating a custom field for each object change in an object change request. For example, select this category if you want to add a comment field to each object change in a change request. **Note:** This field only appears for change request fields.
Enabled	Select this check box to enable the field. If you do not enable the field, it will not appear in the FireFlow user interface.
Edit Properties	
Type	Select the field's type. This can be any of the following: • **Upload image.** Allows uploading an image file. This field type is only available for custom fields for **Change Requests**; it is not available for custom fields for **Users** or **Roles**. • **Date.** Allows selecting a date. • **Upload file.** Allows uploading a file. This field type is only available for custom fields for **Change Requests**; it is not available for custom fields for **Users** or **Roles**. • **Multiple Choice.** Allows selecting a value from options. • **Text.** Allows typing a block of text in the field. • **Type multiple values.** Allows typing multiple values in the field. • **Type or select.** Allows typing a value or selecting a value from a list. • **Select.** Allows selecting one value from a list. • **Multi-select.** Allows selecting multiple values from a list.

In this field...	Do this...
Values source	If the new field is a list (that is, you chose one of the "Select" options in the **Type** field), select the source of the values that should appear in the list. This can be any of the following: • **Provide list of values below:** When this options is selected, a **+** is displayed. Specify the list of values by clicking **+** and typing a name and a description for each value. You can sort the values by dragging and dropping them in the column, and you can delete them by clicking . • **Firewall names** • **Firewall hostgroup names** • **Firewall service group names** • **Available Workflows**
Default Value	Type a default value for the field. **Note:** FireFlow does not check whether the specified default value is valid for the field.

Validation	Select the form of validation to perform for this field. This can be any of the following:
	• **None:** FireFlow will not perform validation for the field.
	• **Mandatory Field:** FireFlow will require this field to be filled in.
	• **Custom:** FireFlow will require this field to be filled in the way that you specify.Type a regular expression in the field that is displayed.
	For example:
	• To require that the fields value must be a number, type the following:
	`^[d\.]+$`
	• To require that the fields value must be a year, type the following:
	`^[12]\d{3}$`

In this field...	Do this...
View Properties	
Link Values To	If you want the field's value to link to a Web page, enter the URL that should open upon clicking the link. The URL can include parameters, which FireFlow will replace as follows: • _id_. The record ID. • _CustomField_. The custom field's value. For example, if you specify the URL `https://Third-party_system/show_ticket?id=__CustomField__`, then the field's value will be a link. If the field's value for a specific change request is “123”, then clicking on the link will open a browser displaying the Web page `https://3rd_party_system/show_ticket?id=123`.
Include Page	If you want the field to display a Web page, enter the URL of the desired Web page. The URL can include the same parameters as **Link values to**. For example, if you specify the URL `https://Third-party_system/show_ticket?id=__CustomField__`, and the field's value for a specific change request is “123”, then the field will display the Web page `https://3rd_party_system/show_ticket?id=123`.
Hide if Empty	Select this option to indicate that the custom field should only appear in the FireFlow interface if it has a value.

Edit user-defined fields

Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page is displayed.

3. Click **Fields**.

   The **Select a Field** page is displayed.

4. (Optional) To display disabled user-defined custom fields, click the **Show disabled** link.

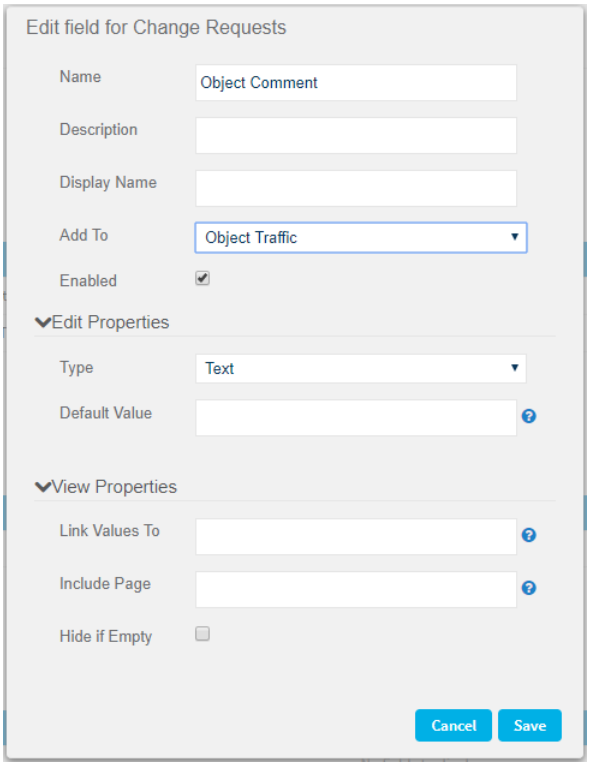
   To revert to a list which only displays enabled user-defined custom fields, click the **Hide disabled** link.

5. (Optional) To search for the desired user-defined custom field, type your search in the **Type to filter your results** field.

   The user-defined custom fields which match your search appear in the relevant area.

6. Click on the desired field's name.

   The **Edit a Field** window is displayed.



7. Modify the fields as desired, using the information in Custom Field Page Fields (see Custom Field Page Fields).

8. Click **Save**.

Edit FireFlow fields

For the FireFlow fields, you may change only the display name and description. Any other change will cause FireFlow to behave unpredictably.

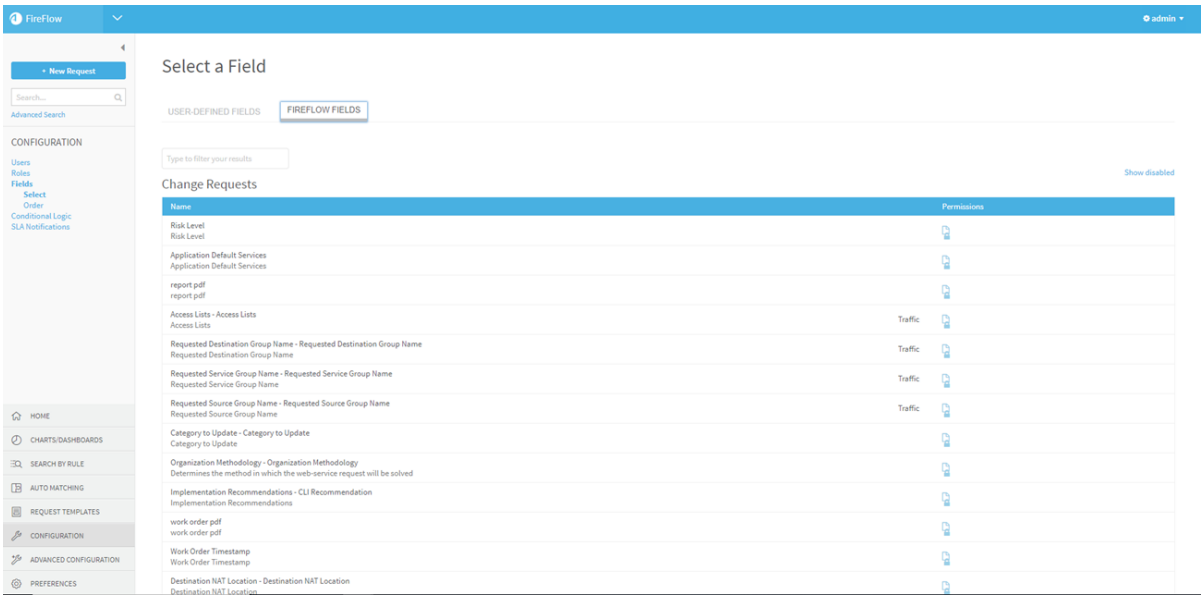
Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page is displayed.
3. Click **Fields**.

   The **Select a Field** page is displayed.
4. Click the **FireFlow Fields** tab.

   The **FireFlow Fields** tab is displayed.



5. (Optional) To display disabled FireFlow fields, click the **Show disabled** link.

To revert to a list which only displays enabled FireFlow fields, click the **Hide disabled** link.

6. (Optional) To search for the desired FireFlow field, type your search in the **Type to filter your results** field.

   The FireFlow fields which match your search appear in the relevant area.

7. Click on the desired custom field's name.

   The **Edit a Field** window is displayed.

8. In the **Description** field, type a description of the custom field.

   This description will appear as a tooltip, when you mouse-over the custom field's name in the **Create Change Request** page.

9. In the **Display Name** field, type the name that should represent the field in the FireFlow interface.

10. Click **Save**.

Disable / enable user-defined fields

If desired, you can disable a user-defined field, so that it no longer appears in the FireFlow interface. You can also re-enable disabled user-defined fields.

Note: Values that were entered for a user-defined field before it was disabled are retained in the FireFlow database.

Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.

2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page is displayed.

3. Click **Fields**.

The **Select a Field** page is displayed.

4. (Optional) To display disabled user-defined custom fields, click the **Show disabled** link.

   To revert to a list which only displays enabled user-defined custom fields, click the **Hide disabled** link.

5. (Optional) To search for the desired user-defined custom field, type your search in the **Type to filter your results** field.

   The user-defined custom fields which match your search appear in the relevant area.

6. Click on the desired field's name.

   The **Edit a Field** window is displayed.

7. Do one of the following:
   - To disable a user-defined custom field, clear the **Enabled** check box.
   - To enable a user-defined custom field, check the **Enabled** check box.

8. Click **Save**.

Configure the order of user-defined fields

When multiple user-defined fields are defined for change requests, users, or roles, you can configure the order they appear.

- For traffic and multicast traffic request templates (excluding IPv6 traffic templates), all fields are ordered per template (not globally).
- For all other request template types, traffic fields and object fields are ordered globally using the procedure below. All other fields for these templates are ordered per template.
- For ordering user and role fields, all fields are ordered globally using the procedure below.

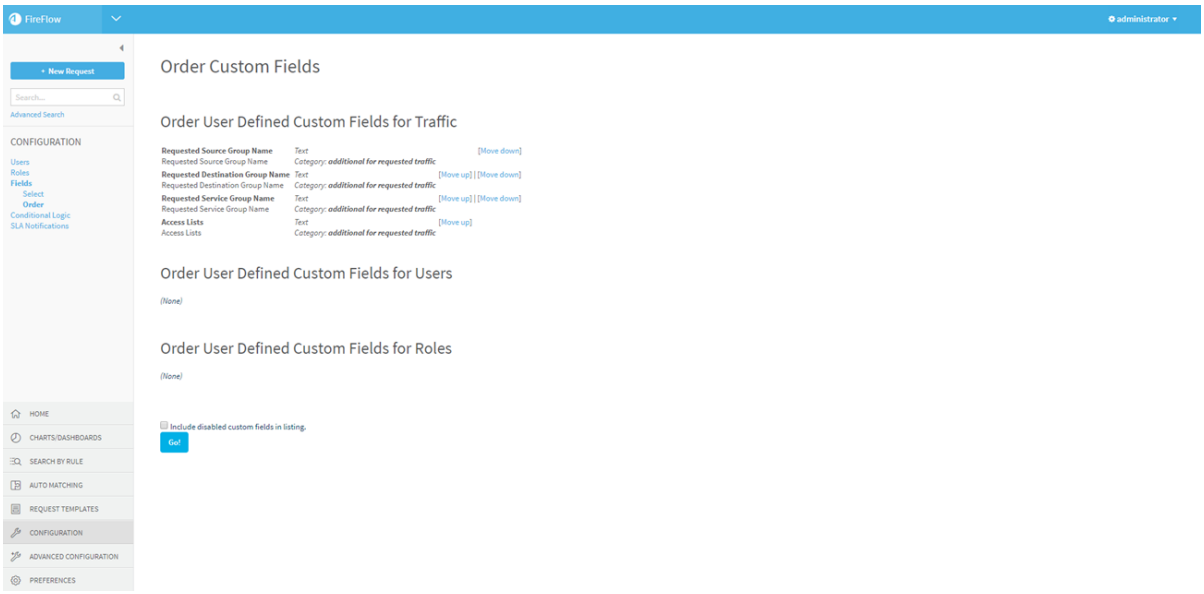
Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page is displayed.
3. Click **Fields**.

   The **Select a Field** page is displayed.
4. In the main menu, click **Order**.

   The **Order Custom Fields** page appears. Within each category, the fields are listed in the order that they will appear in the FireFlow Web interface.



5. In each category, do one or more of the following:
   - To move a change request up in the list, click **Move up** next to it.
   - To move a change request down in the list, click **Move down** next to it.

   The fields will appear in the specified order.

Note: These links only appear when there is more than one custom field in the category.

View role permissions for custom fields

You can view role permissions for user-defined fields or FireFlow fields.

For more details, see Manage user permissions.

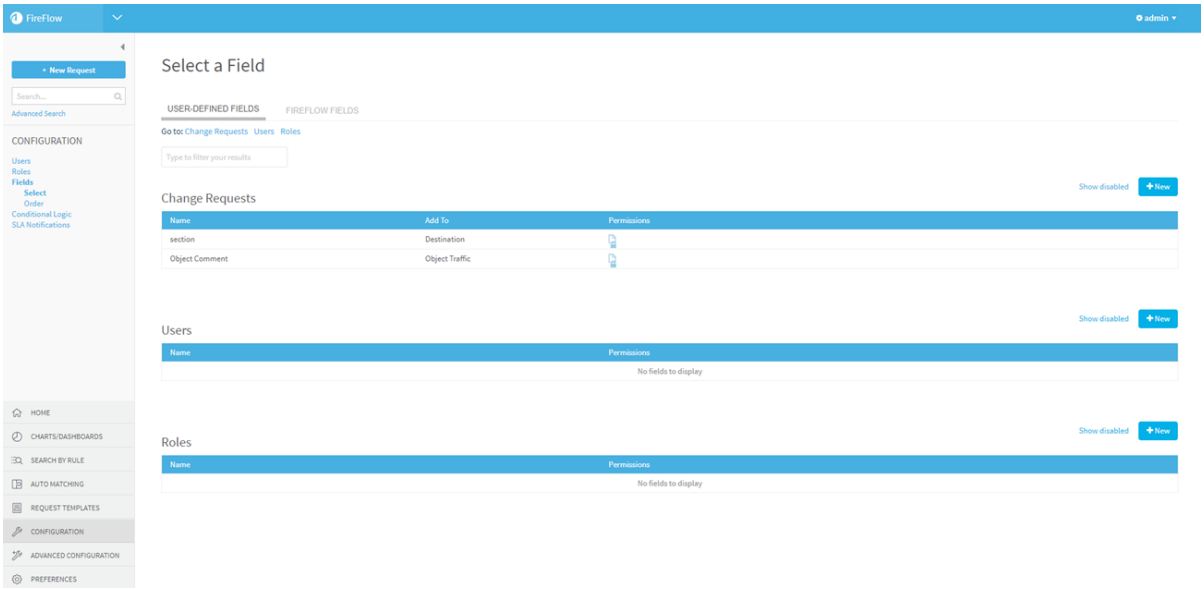
Do the following:

1. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page is displayed.

2. Click **Fields**.

   The **Select a Field** page is displayed.



3. If you want to view role permissions for a FireFlow field, click the **FireFlow Fields** tab.
4. (Optional) To display disabled fields, click the **Show disabled** link.

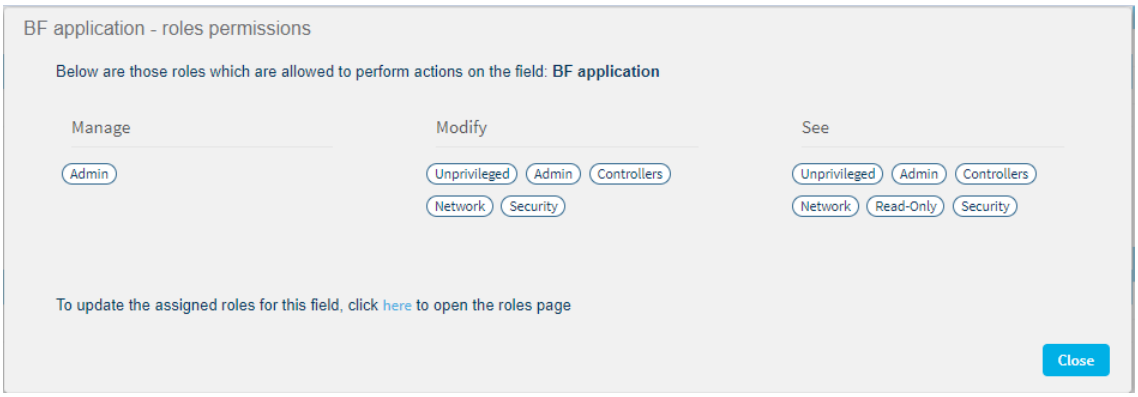
   To revert to a list which only displays enabled fields, click the **Hide disabled** link.

5. (Optional) To search for the desired field, type your search in the **Type to filter your results** field.

   The fields which match your search appear in their designated area.

6. In the row of the relevant role, click .

   The **roles permissions** window appears.



   Users assigned a role with permission to **Manage** the field can view and modify the field's definition (for example, they can modify the field's name, disable it, and so on).
   Users assigned a role with permission to **Modify** the field can modify the field's value.
   Users assigned a role with permission to **See** the field can only view the field's value.

7. Click **Close**.

Manage FireFlow emails and notifications

Relevant for: Administrators

This section describes how to manage FireFlow notifications and emails.

For details, see:

- Manage FireFlow email templates
- Configure incoming mail
- Manage SLA notifications

Manage FireFlow email templates

FireFlow sends emails to users upon various events in the change request lifecycle.

This topic describes how to manage the templates used for each type of email.

FireFlow email templates

This template...	Is used to send emails to...	And is used when...
Transaction	Change request owners	A reply is written for an item in a change request's history. A comment is written for an item in a change request's history. A change request's owner is changed.
Correspondence	Requestors	A reply is written for an item in a change request's history.
Resolved	Requestors	A change request is resolved.
Autoreply	Requestors	A new change request is created.
Notify External System Ticket Close	An external Change Management System (CMS)	A change request is resolved.

If desired, you can modify these templates.

Note: Other templates appear in the FireFlow interface; however, they are not used for FireFlow emails and should therefore be ignored.

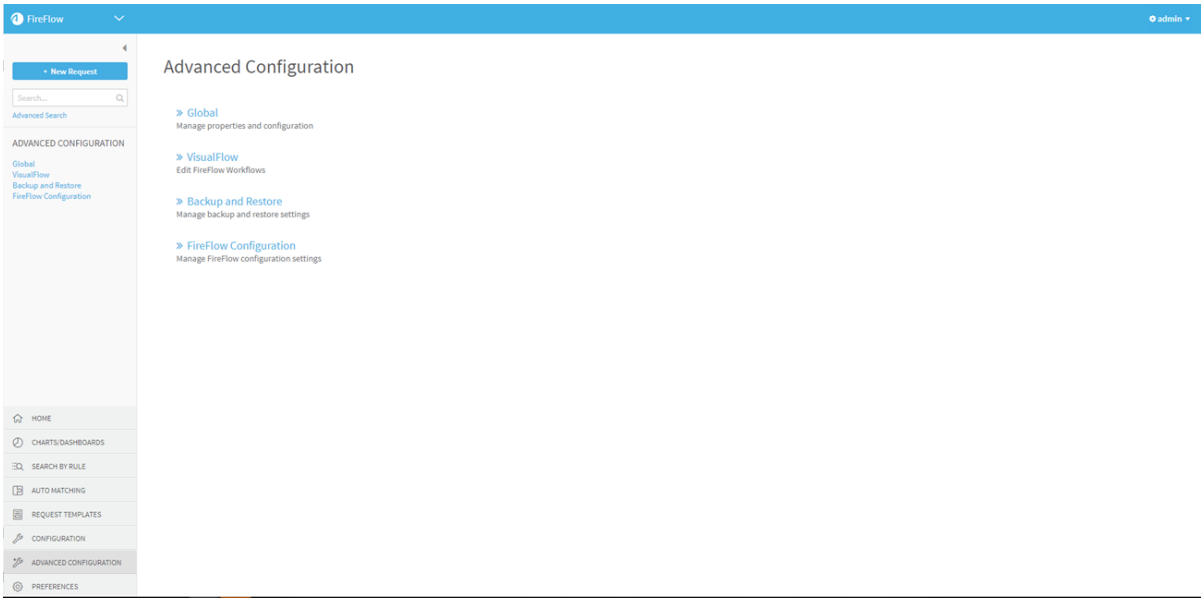
Note: It is possible to customize which events trigger email sending and to whom the emails are sent. For further information, contact AlgoSec.

Modify email templates

Do the following:

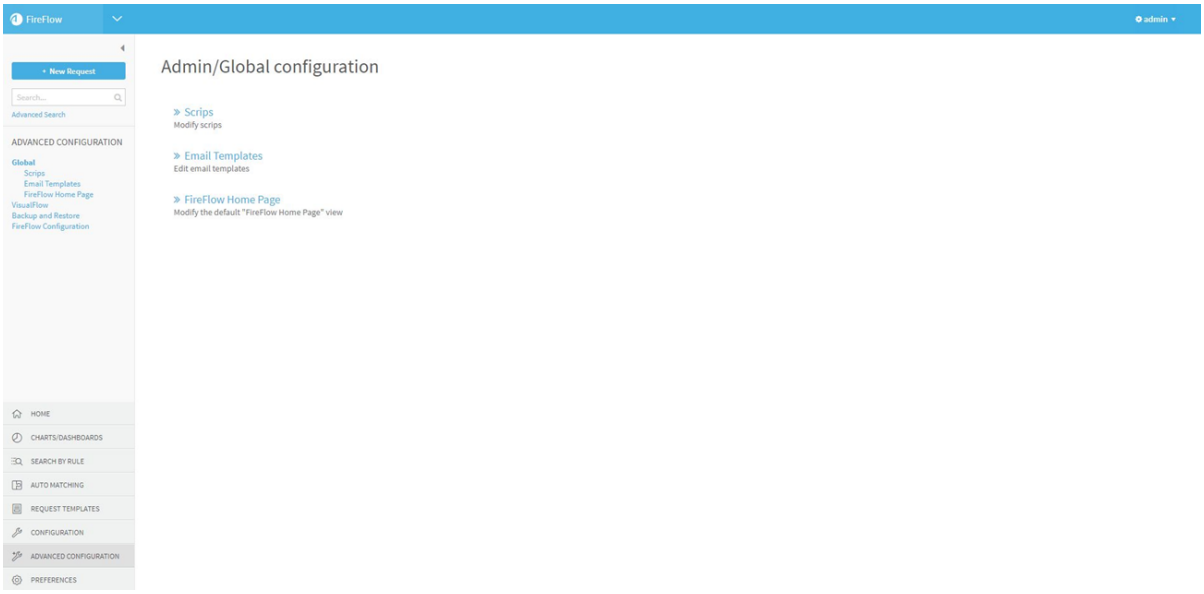
1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Advanced Configuration**.

   The **Advanced Configuration** page is displayed.



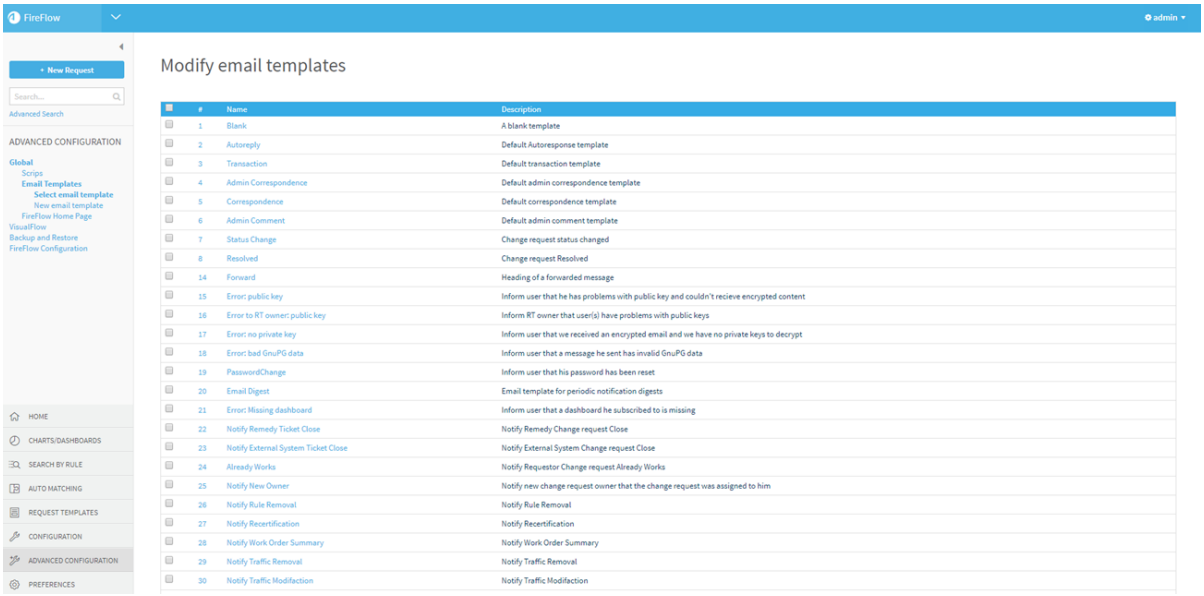
3. Click **Global**.

   The **Admin/Global configuration** page is displayed.



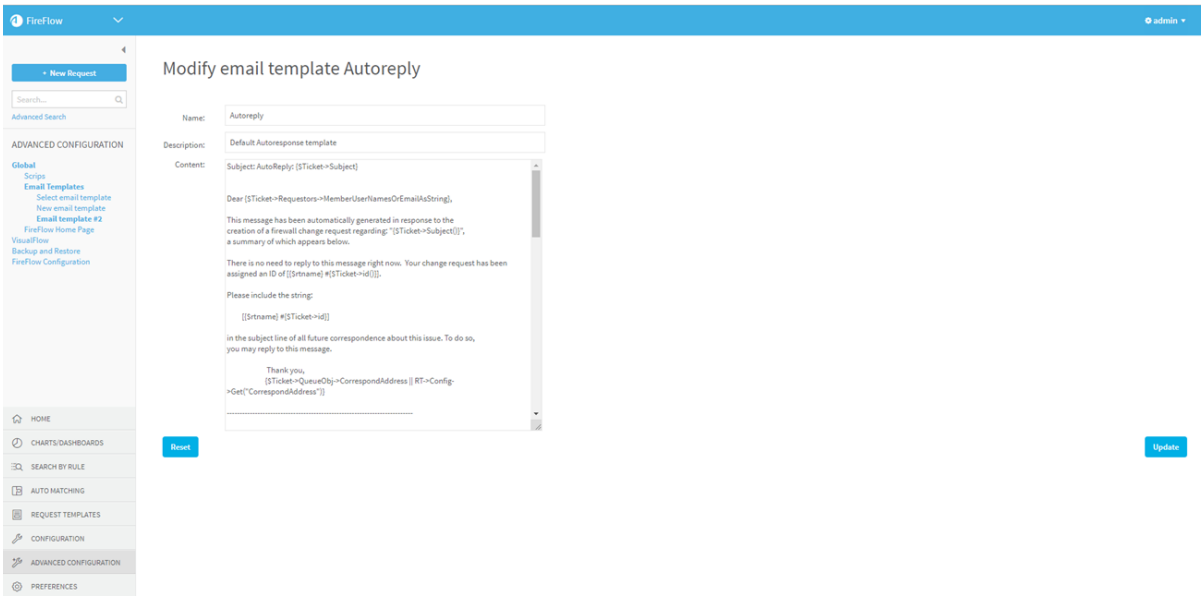
4. Click **Email Templates**.

   The **Modify email templates** page is displayed.



5. Click on the name of the desired template.

The **Modify email template Autoreply** page is displayed.



6. In the **Content** field, type the template's content.

   You can use variables in the template. For a list of popular variables and their explanations, see Email Template Variables (see Email template variables).

   > **Note:** Do not modify the **Name** and **Description** fields.

   > **Note:** The email template variables that include Perl code (appearing in curly braces {}) are subject to Perl syntax.

7. To reset the template to its default settings, click **Reset**.
8. Click **Update**.

Email template variables

{$Ticket->id}

The change request ID number. For example, **364**.

{$Ticket->Subject}

The change request subject. For example: **Need to open device ports for project Armageddon.**

{$Ticket->Status}

The change request status. For example: **plan**

{$Ticket->RequestorAddresses}

The requestor's email address. For example: **john.doe@mycompany.com**

{$Ticket->OwnerObj->Name}

The change request owner's username. For example: **ned.netop**

{$Ticket->getTicketAsXML()}

The change request in XML format (a flat ticket). For examples, see Flat Ticket Examples.

{$Ticket->getTicketAsXML(1)}

The change request in XML format (a flat ticket) with initial plan and/or work order information included.

> **Note:** Initial plan and work order information are only included in the flat ticket when they are enabled.
>
> For details, see Configure inclusion of work details in flat tickets and See Configure inclusion of work details in flat tickets.

For more details, see Flat Ticket Examples.

{$RT::WebURL}Ticket/Display.html?id={$Ticket->id}

The URL at which the change request is displayed.

> **Note:** To enable links, see Configuring Link URLs to FireFlow pages.

For example: **https://fireflow-demo.algosec.com/FireFlow/Ticket/Display.html?id=136**

{$Transaction->CreatedAsString}

The date and time at which the email is sent.

For example: **Mon Nov 17 16:58:44 2008**

Configure incoming mail

This topic explains how to configure incoming email for FireFlow, by either fetching emails from the mailbox using fetchmail, or by forwarding emails to FireFlow's MTA.

It is necessary to configure incoming mail for FireFlow, in order to enable users to do the following:

- Submit change requests to FireFlow via email.
- Add comments to change requests by replying to FireFlow system-generated emails.

Incoming mail configuration methods

FireFlow supports the following methods for retrieving incoming mail:

Configure fetchmail for incoming emails	This is the recommended method. It requires that your organization's email server support POP3 and/or IMAP4 access.
Configure sendmail to receive forwarded emails as an MTA	Use this method if POP3 and IMAP4 access are not supported by your organization's email server, or not allowed by your organization's security policy.

Configure fetchmail for incoming emails

Note: Regardless of which method you choose, you must first define an email account for the FireFlow server, such as **fireflow@mycompany.com**.

Do the following:

Configure incoming mail for FireFlow.

If you run into any issues, troubleshoot them as follows:

1. Log in to the FireFlow server using the username "root" and the related password.
2. Ensure that the file `/home/fireflow/.fetchmailrc` is owned by "fireflow" and that only this user has read/write permissions for the file.

   Do the following:

   a. Check the file's current owner and permissions, by entering the following command:

      ls -l /home/fireflow/.fetchmailrc

   b. If the owner and/or permissions require changing, enter the following commands:

      chown fireflow:fireflow /home/fireflow/.fetchmailrcchmod 600 /home/fireflow/.fetchmailrc

3. Open the file `/home/fireflow/.fetchmailrc`.
4. Do one of the following:

   - To configure fetchmail for POP3, add the following line in the file:

     ```
     poll <SERVER> protocol POP3 user <USER> pass <PASSWORD> mda "/usr/share/fireflow/local/bin/fireflow-mailgate"
     ```

   - To configure fetchmail for POP3 over SSL, add the following line in the file:

     ```
     poll <SERVER> protocol POP3 port <PORT> user <USER> pass <PASSWORD> ssl mda "/usr/share/fireflow/local/bin/fireflow-mailgate"
     ```

   - To configure fetchmail for IMAP, add the following line in the file:

     ```
     poll <SERVER> protocol IMAP user <USER> pass <PASSWORD> mda "/usr/share/fireflow/local/bin/fireflow-mailgate"
     ```

   In each case, replace the parameters as follows:

`<SERVER>` - The email server's IP address or hostname

`<PORT>` - The relevant port for the protocol used

`<USER>` - The username required for accessing the mailbox (for example, fireflow@mycompany.com)

`<PASSWORD>` - The password required for accessing the mailbox

5. Save the file.
6. Ensure that the crontab of user “fireflow” runs fetchmail every 1 minute, by doing the following:
    a. Enter the following command:

    crontab -u fireflow -l

    You should see the following line:

    ```
    */1 * * * *    /usr/bin/fetchmail --silent
    ```

    The line should not be commented out by a # prefix.

    b. If such a line does not exist, or if it is commented out, then edit the crontab of user “fireflow” by entering the command:

    crontab -u fireflow -e

7. To verify that fetchmail was configured correctly, submit a request by sending an email to the FireFlow server's email address.

    FireFlow should create a new change request within a couple of minutes.

Note: All fetchmail output is written to the log file `/var/log/fetchmail.log`, when it is executed without the `--silent` flag. This file is useful for troubleshooting purposes.

Configure sendmail to receive forwarded emails as an MTA

This solution involves configuring the organization’s main email server to forward emails that are addressed to FireFlow to the MTA running on the FireFlow server.

The outcome is that all emails sent to the FireFlow email address (fireflow@mycompany.com) are automatically forwarded to the address on the FireFlow server (fireflow@fireflow.mycompany.com). The emails are received by the MTA running on the FireFlow server (sendmail) and processed by FireFlow.

Do the following:

1. Create a DNS entry (MX record) for the FireFlow server on the organization's main DNS server (for example, **fireflow.mycompany.com**).
2. Log in to the FireFlow server using the username "root" and the related password.
3. If sendmail is not configured to listen on external interfaces, do the following:
    a. Enter the following commands to back up the current sendmail configuration and then edit it:

    cp -p /etc/mail/sendmail.mc /etc/mail/sendmail.mc_bkpcp -p /etc/mail/sendmail.cf /etc/mail/sendmail.cf_bkpvi /etc/mail/sendmail.mc

    b. Comment the following line by adding a `dnl #` prefix:

    ```
    dnl # DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
    ```

    c. Save the file and exit vi.

    d. Enter the following command to compile the sendmail configuration:

    m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
4. Use the **algosec_conf** script to configure the hostname to be same as the FireFlow server's DNS entry name.
5. Configure sendmail to process emails that are sent to the FireFlow server's address (fireflow@fireflow.mycompany.com) using fireflow-mailgate, by doing the following:
    a. Enter the following commands to backup the current aliases and then edit it:

    cp -p /etc/aliases /etc/aliases_bkpcp -p /etc/aliases.db /etc/aliases.db_bkpln -s /usr/share/fireflow/local/bin/fireflow-mailgate /etc/smrsh/vi /etc/aliases

b. Add the following line to the end of the file:

```
fireflow:       "|/etc/smrsh/fireflow-mailgate"
```

c. Save the file and exit vi.

d. Enter the following command to compile the aliases file:

[root@algosec /]# newaliases

e. Restart sendmail, by entering the following command:

/etc/init.d/sendmail restart

6. To verify that sendmail was configured correctly, submit a request by sending an email to the FireFlow server's email address.

FireFlow should create a new change request within a couple of minutes.

Troubleshoot issues with sendmail

Do the following:

1. If emails are not reaching FireFlow, you may need to configure sendmail to agree to relay messages from the main SMTP server, by doing the following:

   a. Enter the following commands to backup the current access file and then edit it:

   cp -p /etc/mail/access /etc/mail/access_bkpcp -p /etc/mail/access.db /etc/mail/access.db_bkpvi /etc/mail/access

   b. Add a line to the file, allowing RELAY from the SMTP server's IP address.

   For example, if the SMTP server's IP address is 192.168.2.34, the line should appear as follows:

   ```
   192.168.2.34                    RELAY
   ```

   c. Save the file and exit vi.

d. Enter the following command to compile the access file:

makemap hash /etc/mail/access.db < /etc/mail/access

2. Check whether sendmail is configured to listen on external interfaces, by doing one of the following:

   a. Try to connect to the FireFlow server on port 25, by entering the following command on another machine:

   ```
   telnet <SERVER> 25
   ```

   Replace `<SERVER>` with the FireFlow server's IP address.

   If the connection does not succeed, then sendmail is not configured to listen on external interfaces.

   b. Check if there is a process listening on port 25, on an interface other than 127.0.0.1, by entering the following command:

   ```
   netstat -an | grep 25
   ```

   If the output consists of only one line that specifies 127.0.0.1, then sendmail is not configured to listen on external interfaces.

3. Sometimes the specific setup requires additional steps to configure incoming email as MTA:

   a. Add the DNS name of the FireFlow server to `/etc/mail/local-host-names`.

   b. Add the following lines to sendmail config:

      - `define('MAIL_HUB','DOMAIN.com')dnl`
      - `define('LOCAL_RELAY','DOMAIN.com')dnl`

   c. Create an email address matching what is being forwarded and assign it to the FireFlow Linux user.

   d. Change the entry in the sendmail config to use the external IP instead of

`localhost`.

e. Allow incoming SMTP through iptables.

Note: All sendmail output is written to the log file `/var/log/maillog`. This file is useful for troubleshooting purposes.

Manage SLA notifications

Relevant for: Administrators

FireFlow enables you to create custom pages displaying a specific set of SLO data. These pages are called *SLA notifications*, and they can be made available to you only, certain user roles, or system-wide.

In addition, users can be subscribed to SLA notifications, so that they periodically receive the SLA notifications' content via email.

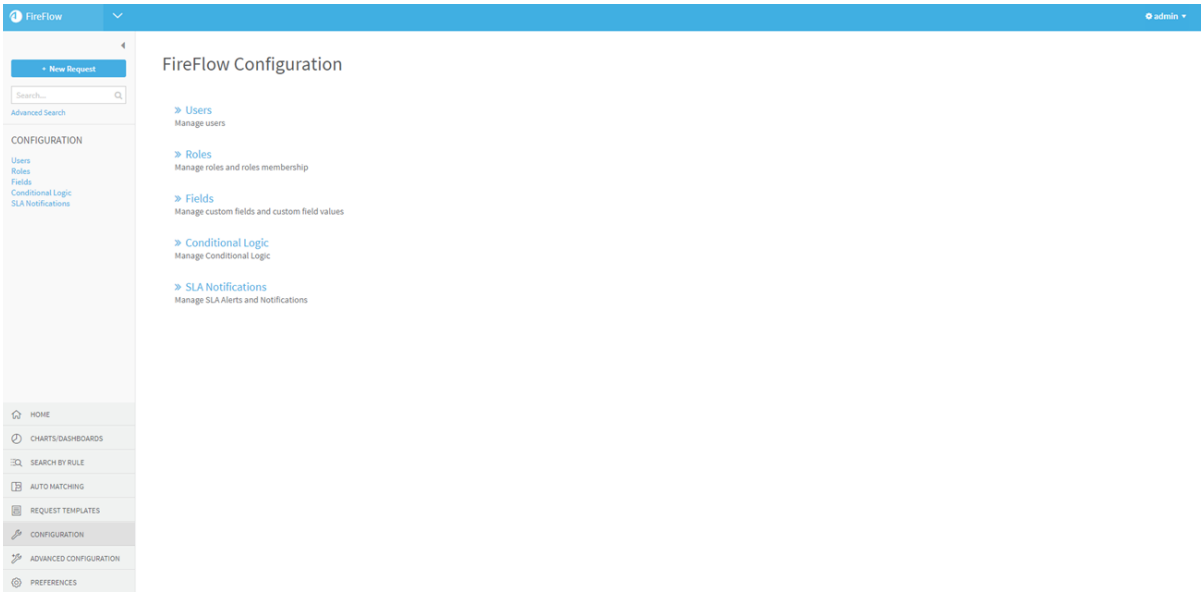
This section explains how to configure SLA notifications.

Add SLA notifications

Do the following:

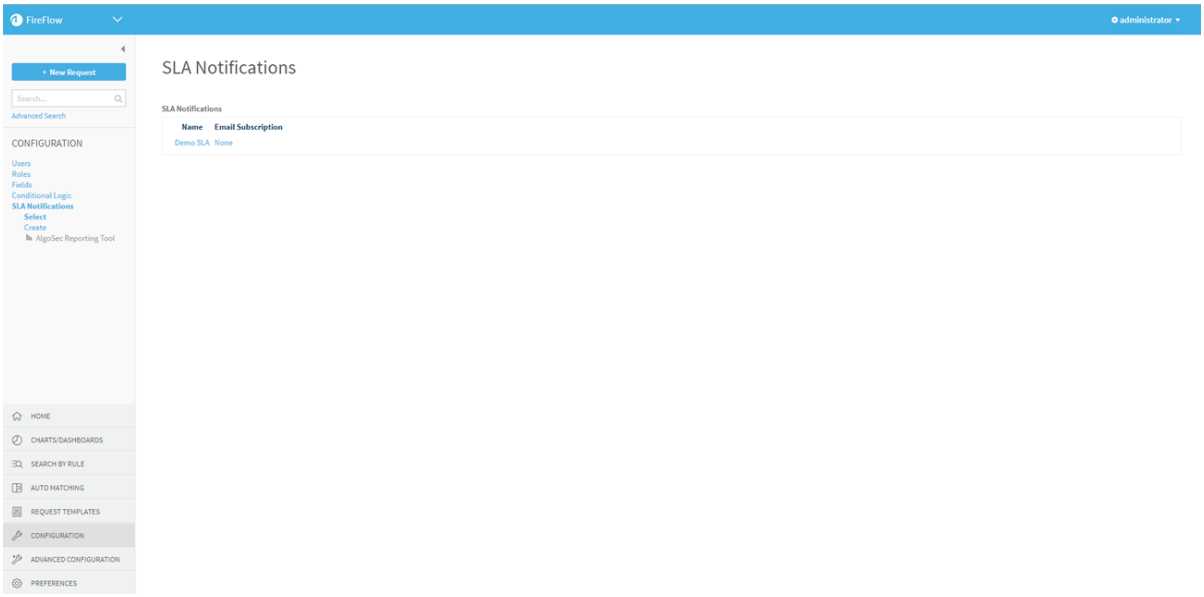
1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page is displayed.



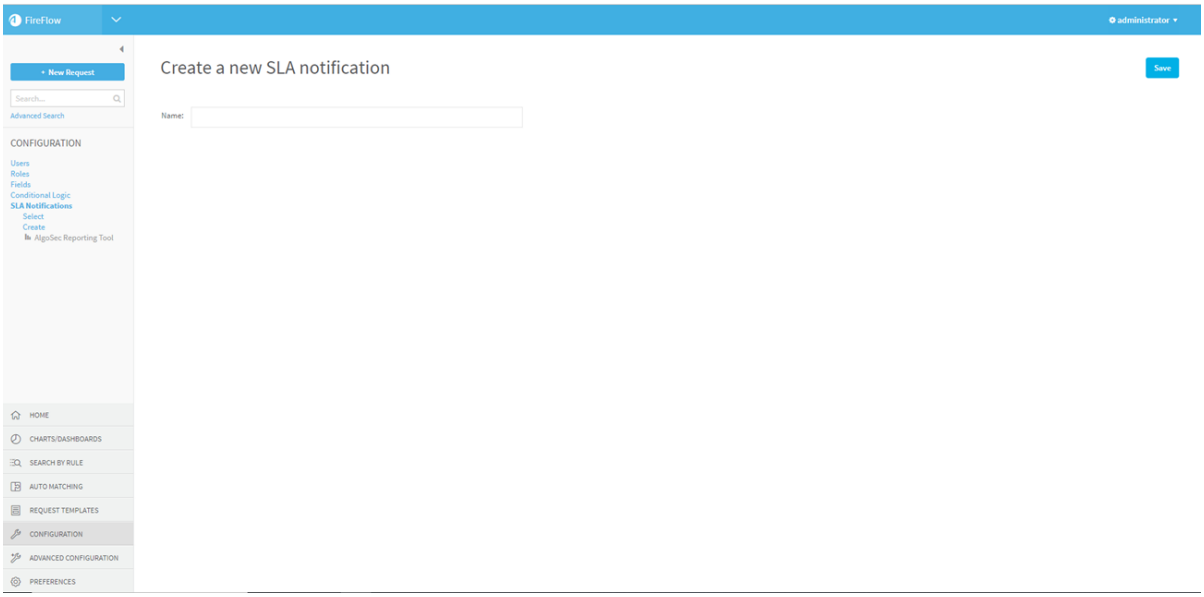
3. Click **SLA Notifications**.

   The **SLA Notifications** page is displayed.



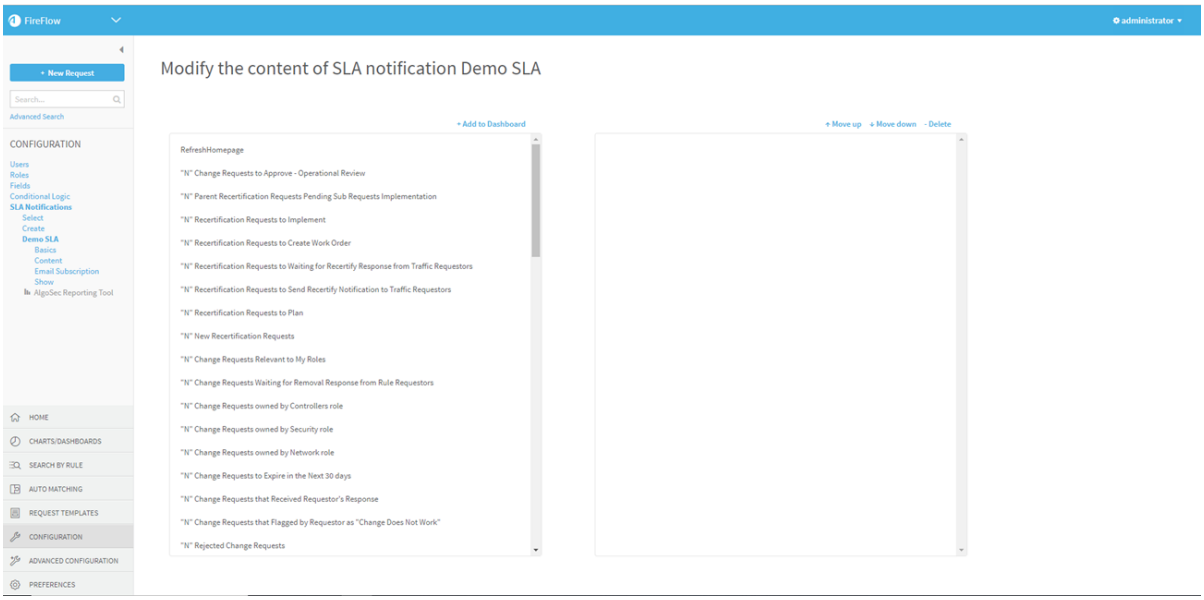
4. In the main menu, click **Create**.

   The **Create a new SLA notification** page is displayed.



5. In the **Name** field, type a name for the SLA notification.
6. Click **Save**.
7. In the main menu, under the SLA notification's name, click **Content**.

   The **Modify the content of SLA notification** page is displayed.



8. For each element you want to add to the SLA notification, do the following:

a. In the **Available** list box, select the element you want to add.

   For information on each element, see SLA Notification Elements (see SLA notification elements).

b. Click + Add to Dashboard .

   The selected element moves to the right list box. The order that the elements appear in the box represents the order in which they will appear in the SLA notification.

c. To move the element up or down in the box, select the element and click the ↓ Move down or ↑ Move up buttons.

d. To delete the element, select it and click **Delete**.

Your changes are saved.

SLA notification elements

Select this element...	To add this to the SLA notification...
"N" Soon to be due change requests	Pre-defined search results consisting of a list of open change requests in the system that have a due date that has passed, that is the current date, or that is the day after the current date.
"N" New Recertification Requests	Pre-defined search results consisting of a list of recertification requests in the system that are new and still in the Request stage.
"N" New Change Requests	Pre-defined search results consisting of a list of change requests in the system that are new and still in the Request stage, and whose traffic has already been checked against devices.
"N" Open Change Requests	Pre-defined search results consisting of a list of change requests in the system that are currently open.

Select this element...	To add this to the SLA notification...
"N" Parent Recertification Requests Pending Sub Requests Implementation	Pre-defined search results consisting of a list of parent recertification requests in the system that are currently in the Implement stage and awaiting implementation of the relevant sub-requests.
"N" Parent Requests Pending Sub Request Implementation	Pre-defined search results consisting of a list of parent requests in the system that are currently in the Implement stage and awaiting implementation of the relevant sub-requests.
"N" Recertification Requests to Create Work Order	Pre-defined search results consisting of a list of recertification requests in the system that are currently in the Implement stage and awaiting a work order to be created.
"N" Recertification Requests to Implement	Pre-defined search results consisting of a list of recertification requests in the system that are currently in the Implement stage and awaiting implementation.
"N" Recertification Requests to Plan	Pre-defined search results consisting of all recertification requests in the system that are currently in the Plan stage.
"N" Recertification Requests to Send Recertify Notification to Traffic Requestors	Pre-defined search results consisting of a list of recertification requests in the system that are currently in the Approve stage, and for which a recertification notification will be sent to the traffic requestors.
"N" Recertification Requests to Validate	Pre-defined search results consisting of a list of recertification requests in the system that are currently in the Validate stage.
"N" Recertification Requests Waiting for Recertify Response from Traffic Requestors	Pre-defined search results consisting of a list of recertification requests in the system that are currently in the Approve stage and awaiting confirmation from the traffic requestors that the requested recertification is approved.
"N" Rejected Change Requests	Pre-defined search results consisting of a list of change requests in the system that were rejected.

Select this element...	To add this to the SLA notification...
"N" Resolved Change Requests	Pre-defined search results consisting of a list of change requests in the system that have been resolved.
"N" Change Requests owned by Controllers group	Pre-defined search results consisting of a list of change requests in the system that are owned by the Controllers role.
"N" Change Requests owned by Network group	Pre-defined search results consisting of a list of change requests in the system that are owned by the Network role.
"N" Change Requests owned by Security group	Pre-defined search results consisting of a list of change requests in the system that are owned by the Security role.
"N" Change Requests Relevant to My Groups	Pre-defined search results consisting of a list of change requests in the system that are relevant to the user roles to which you belong.
"N" Change Requests that are due to be recertified	Pre-defined search results consisting of a list of traffic change requests in the system that expired, and which should be recertified.
"N" Change Requests Flagged by Requestor as "Change Does Not Work"	Pre-defined search results consisting of a list of change requests in the system that have been flagged by the requestor as "Change Does Not Work".
"N" Change Requests that Received Requestor's Response	Pre-defined search results consisting of a list of change requests in the system that are currently in the Validate stage and received the requestor's confirmation that the requested change was implemented successfully.
"N" Change Requests to Approve	Pre-defined search results consisting of a list of change requests in the system that are currently in the Approve stage.
"N" Change Requests to Create Work Order	Pre-defined search results consisting of a list of change requests in the system which are currently in the Implement stage and awaiting a work order to be created.

Select this element…	To add this to the SLA notification…
"N" Change Requests to Expire in the Next 30 days	Pre-defined search results consisting of a list of change requests in the system that will expire within the next 30 days.
"N" Change Requests to Implement	Pre-defined search results consisting of a list of change requests in the system that are currently in the Implement stage and awaiting implementation.
"N" Change Requests to Plan	Pre-defined search results consisting of all change requests in the system that are currently in the Plan stage.
"N" Change Requests to Review	Pre-defined search results consisting of a list of change requests in the system that are currently in the Review stage and awaiting a controller's review.
"N" Change Requests to Send Removal Notification to Rule Requestors	Pre-defined search results consisting of a list of change requests in the system that are currently in the Approve stage, and for which a rule removal notification will be sent to the rule's traffic requestors.
"N" Change Requests to Validate	Pre-defined search results consisting of a list of change requests in the system that are currently in the Validate stage.
"N" Change Requests Waiting for Removal Response from Rule Requestors	Pre-defined search results consisting of a list of change requests in the system that are currently in the Approve stage and awaiting confirmation from the rule’s traffic requestors that the requested rule removal is approved.
"N" Change Requests Waiting for Requestor's Response	Pre-defined search results consisting of a list of change requests in the system that are currently in the Validate stage and awaiting the requestor's confirmation that the requested change was implemented successfully.
"N" Total New Change Requests	Pre-defined search results consisting of a list of all change requests in the system that are new and still in the Request stage, including change requests whose traffic has not yet been checked against devices.
Bookmarked Change Requests	A list of change requests that the user bookmarked.

Select this element...	To add this to the SLA notification...
My Change Requests	Pre-defined search results consisting of a list of change requests in the system that are owned by you.
RefreshHomepage	Controls for refreshing the page.
Unowned Change Requests	Pre-defined search results consisting of a list of change requests in the system that currently have no owner.
Saved Search Name	A custom search that was saved under "FireFlow's saved searches", and which is available to your user role.
Chart Name	A chart that was saved under "FireFlow's saved searches", and which is available to your user role.
Search for chart *Chart Name*	A custom search on which a certain chart is based.

Edit SLA notifications

Do the following:

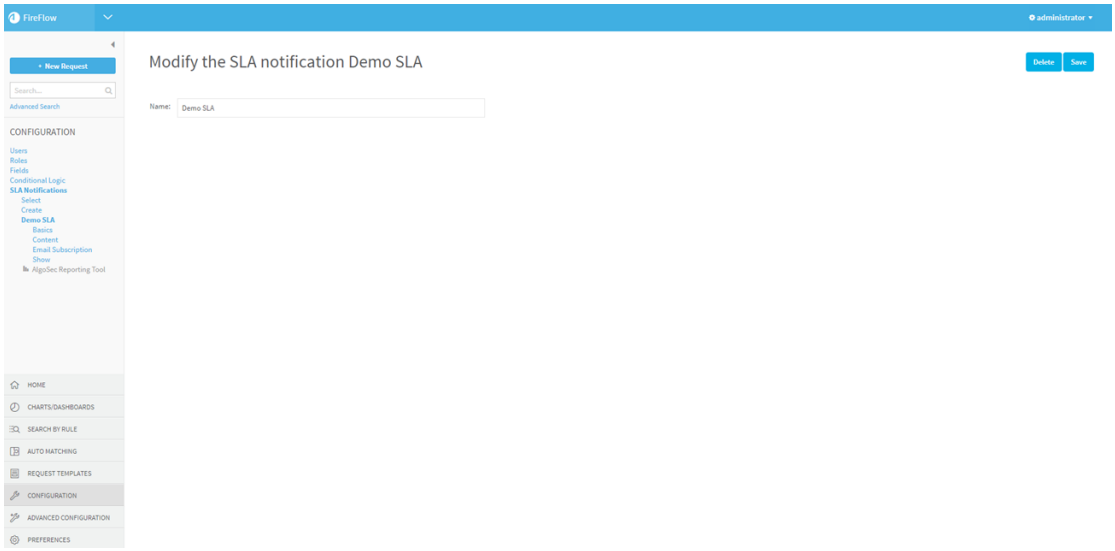
1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page is displayed.
3. Click **SLA Notifications**.

   The **SLA Notifications** page is displayed.
4. Click on the name of the desired notification.

   The SLA notification appears.
5. To modify the SLA notification's name, do the following:
   a. In the main menu, under the SLA notification's name, click **Basics**.

      The **Modify the SLA notification** page is displayed.



b. In the **Name** field, type a name for the SLA notification.

c. Click **Save**.

6. To modify the SLA notification's content, do the following:

   a. In the main menu, under the SLA notification's name, click **Content**.

      The **Modify the content of SLA notification** page is displayed.

   b. For each element you want to add to the SLA notification, do the following:

      i. In the **Available** list box, select the element you want to add.

         For information on each element, see SLA Notification Elements (see SLA notification elements).

      ii. Click **+Add to Dashboard**.

         The selected element moves to the right list box. The order that the elements appear in the box represents the order in which they will appear in the SLA notification.

      iii. To move the element up or down in the box, select the element and click **Move down** or **Move up**.

      iv. To delete the element, select it and click **- Delete**.

Your changes are saved.

Manage email subscriptions to SLA notifications

By default, when you create an SLA notification, you are automatically subscribed to it, and emails containing the SLA notification's content will be sent to the email address associated with your account. If desired, you can configure FireFlow to send these emails to other recipients, and/or change the frequency and time at which these emails are sent.

Do the following:

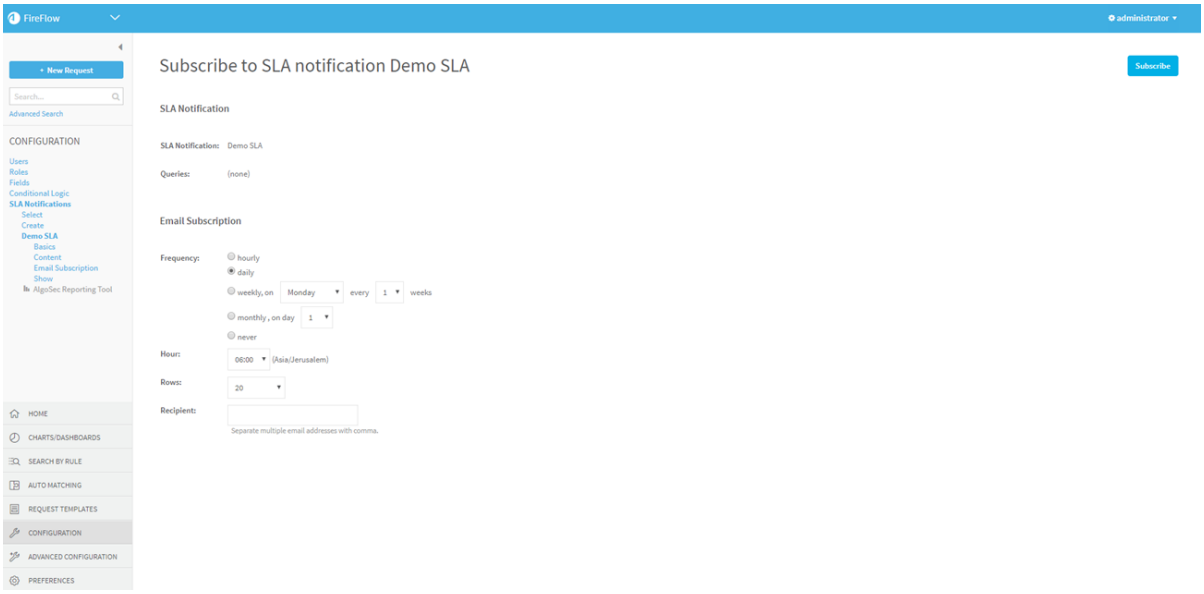
1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page is displayed.
3. Click **SLA Notifications**.

   The **SLA Notifications** page is displayed.
4. Click on the name of the desired notification.

   The SLA notification appears.
5. In the main menu, under the SLA notification's name, click **Email Subscription**.

   The **Subscribe to SLA notification** page is displayed.



6. Configure the fields as needed. For details, see Email Subscription Fields.
7. Click **Subscribe**.

Email Subscription Fields

In this field...	Do this...
Frequency	Specify how often emails containing SLA notification content should be sent. This can have the following values: • **hourly:** Emails will be sent once an hour. • **daily:** Emails will be sent once a day. • **weekly:** Emails will be sent once every specified number of weeks on the specified day. • **monthly:** Emails will be sent once a month on the specified day of the month. • **never:** Emails will not be sent.
Hour	Select the hour in the displayed time zone, at which emails containing SLA notification content should be sent. **Note:** The time zone can be configured in your user settings.

In this field...	Do this...
Rows	Select the number of change requests in each saved search that should appear in emails containing dashboard content.
Recipient	Type a list of email addresses to which emails containing SLA notification contents should be sent. The email addresses must be separated by commas. If this field is left empty, emails will be sent only to the email address associated with your FireFlow user account. However, if this field is filled in, emails will *not* be sent to the email address associated with your FireFlow user account, unless you include your email address in the list.

Delete SLA notifications

Do the following:

1. Log in to FireFlow for configuration purposes. For details, see Log in for configuration purposes.
2. In the main menu, click **Configuration**.

   The **FireFlow Configuration** page is displayed.
3. Click **SLA Notifications**.

   The **SLA Notifications** page is displayed.
4. Click on the name of the desired notification.

   The SLA notification apears.
5. In the main menu, under the SLA notification's name, click **Basics**.

   The **Modify the SLA notification** page is displayed.
6. Click **Delete**.

   A confirmation message appears.

7. Click **OK**.

   The SLA notification is deleted.

FireFlow hooks

You can streamline the change request lifecycle, by using hooks to control certain parameters, such as the name of the workflow to assign the change request in the Request stage, or the device group against which to check traffic. FireFlow will extract the desired parameters on the fly.

This section explains how to use hooks with FireFlow.

FireFlow hook reference

It is possible to configure FireFlow to extract certain parameters on the fly, by using hooks. This helps streamline the change request lifecycle and is particularly helpful for managed security service providers (MSSPs).

For example, during the Initial Plan stage of the change request lifecycle, FireFlow checks the requested traffic against the ALL_FIREWALLS group, by default. If you have several customers, each of which is a large organization with numerous devices, checking traffic against all of the devices of each organization is unnecessary and time consuming. By using hooks, it is possible to configure FireFlow to check traffic only against the devices of the organization that issued the change request.

FireFlow supports the following hooks:

EditRuleSectionHeader	Select the header under which a new rule is recommended to be added. Relevant for change requests for Check Point R80 and R77 devices.
ExcludeAcl	Sets which, if any, ACLs to exclude from the work order.
FilterInitialPlanResults	Filter initial planning results to remove devices.
GetAdditionalRealGroupNames	Retrieve the names of the additional responsible user roles for the change request in a lifecycle stage with parallel actions.
GetExternalRisks	Return detected risks and their details.

GetFirewallGroupName	Retrieve the device group against which traffic should be checked in the Initial Plan stage.
GetRealGroupName	Retrieve the name of the user role responsible for the change request in each lifecycle stage.
GetRequestorSearches	Retrieve searches in the Requestors Web Interface.
GetWorkFlowName	Retrieve the name of the workflow to assign the change request in the Request stage.
LoadConfigHook	Save pre-calculated data or configurations to the FireFlow server in-memory configuration and retrieve the data later.
SuggestCommentSuffix	Add suffixes to add to suggested rule comments in the work order.
SuggestGroupName	Suggest group names to match groups of IP addresses or services with no associated group name in a work order.
SuggestHostName	Suggest host names to match IP addresses with no associated hostname in a work order.
SuggestPropertyValue	Suggest new values for the rule properties for Palo Alto and Fortimanager device work orders.
SuggestSectionName	Suggest a value for a section of a new rule when the work order suggests adding a new rule.
SuggestServiceName	Suggest names to match services with no associated name in the work order.
ValidateTicket	Validate a new or modified change request.
ValidateWorkOrderEdit	Validate host names, groups, and comments in a manually edited work order.

Use hooks to control parameters

Do the following:

1. Log in to the FireFlow server using the username "root" and the related password.
2. Under the `/usr/share/fireflow/local/etc/site/lib` directory, create a Perl pm file.

   The file can have any name.

   For example, you can create the file `/usr/share/fireflow/local/etc/site/lib/MyHooks.pm`, and should begin with the line:

   ```
   package FireFlow::Hooks;
   ```
3. In the file you created, implement the desired hooking functions.
4. Use the generic procedure for overriding system defaults in the CLI to set the configuration parameter `HooksFileNames` to the name of the Perl pm file you created. For details, see Override FireFlow system defaults.

   In the example above, the value would be **MyHooks**.
5. Restart FireFlow. See Restarting FireFlow (see Restart FireFlow).

Hook usage examples

For a comprehensive example, refer to the following files on the FireFlow server:

- A sample Perl module is located under `/usr/share/fireflow/local/Hooks/ExampleHooks.pm`
- The related XML data is located under `/usr/share/fireflow/local/etc/site/Hooks/Example_Config.xml`

GetWorkFlowName

Syntax

```
sub GetWorkFlowName
```

Description

This function is called for every change request, when the change request is created and its workflow must be determined. It receives the change request as input and returns the name of the workflow that FireFlow should assign the change request.

Input parameters

`$context`	A Perl hash reference containing a single key called `flatTicket`, which points to the flat ticket representation of the change request. For details, see Flat Ticket Examples.

Return Values

One of the following values:

The desired workflow's name	
""	Use the default behavior: Assign a workflow based on the configured workflow conditions.

GetFirewallGroupName

Note: Most of this hook's functionality can be accomplished by configuring conditional logic in the FireFlow web interface. For more details, see Configure initial plan device group conditions. If conditional logic is defined in the web interface and this hook is being used, the hook has lower precedence. The hook is executed only if no condition is met for a specific change request.

Syntax

```
sub GetFirewallGroupName
```

Description

This function is called for every change request just before initial planning is executed on the change request. It receives the change request as input and returns the name of

the device group against which FireFlow will check traffic in the Initial Plan stage.

Input Parameters

`$context`	A Perl hash reference containing a single key called `flatTicket`, which points to the flat ticket representation of the change request. For details, see Flat Ticket Examples.

Return Values

One of the following values:

The desired device group's name	This must be the group's real name, not its display name.
""	Use the default behavior: FireFlow will check traffic against the group configured as `$FAQueryDefaultGroup` in the configuration file. (The default is the ALL_FIREWALLS group.)

GetRealGroupName

Note: Most of this hook's functionality can be accomplished by configuring conditional logic in the FireFlow web interface. For details, see Manage user roles.

If conditional logic is defined in the web interface and this hook is being used, the hook has lower precedence. The hook is executed only if no condition is met for a specific change request.

Syntax

```
sub GetRealGroupName
```

Description

This function is called for every change request, when the change request transitions from one status to another. It receives the change request as input, as well as the “meta group” name that the change request's workflow specifies, as the responsible role for

the change request's new status. It returns the name of the user role that is responsible for the change request in its current status.

Input Parameters

`$context`	A Perl hash reference containing a single key called `flatTicket`, which points to the flat ticket representation of the change request. For details, see Flat Ticket Examples.
`$metaGroup`	A user role name, as it appears in the workflow configuration. This may be a meta role's name. For example if the meta role's name is "security", the hook may then return the user role "securityA" for requestors of company A, and the user role "securityB" for requestors of company B, where "securityA" and "securityB" are real user roles (not meta roles) that exist in FireFlow.

Return Values

One of the following values:

The desired user role's name	
""	Use the default behavior: The user role specified in the workflow configuration will be responsible for the change request.

GetAdditionalRealGroupNames

Syntax

```
sub GetAdditionalRealGroupNames
```

Description

This function is called for every change request with parallel actions, when the change request transitions from one status to another. It receives the change request as input, as well as user role names that the change request's workflow specifies as the responsible roles for the change request's new status. It returns the names of additional responsible roles for the change request's current status.

Input Parameters

`$context`	A Perl hash reference containing a single key called `flatTicket`, which points to the flat ticket representation of the change request. For details, see Flat Ticket Examples.
`$metaGroupsArrayRef`	A perl array reference with user role names, as they appear in the workflow configuration. These may be the names of a meta role. For example if a meta role's name is "security", the hook may then return the user role "securityA" for requestors of company A, and the user role "securityB" for requestors of company B, where "securityA" and "securityB" are real user role (not meta roles) that exist in FireFlow.

Return Values

One of the following values:

A Perl array reference containing an array of all additional responsible roles.	**Note:** The role names appear in the same order as in `$metaGroupsArrayRef`.
`[]`	Use the default behavior: The user roles specified in the workflow configuration will be responsible for the change request.

GetRequestorSearches

Syntax

```
sub GetRequestorSearches
```

Description

This function allows adding searches to the Requestors Web Interface. It receives the requestor's user properties as input, as well as the name of the page in the Requestors Web Interface on which the search should appear. It returns a search on the specified page.

Note: By default, requestors can only view change requests that they requested themselves. Therefore, if the hook returns a search query with change requests that other users requested, those change requests will not appear. To enable displaying change requests requested by other users, it is necessary to assign requestors this permission. See Working with Permissions (see Manage user permissions).

Input Parameters

`$requestor`	A hash reference to the requestor's user properties. For a list of user properties that are included in the hash. For information on modifying the list of included properties, see Configuring the List of User Properties (see Configuring Requestor User Properties).
`$friendly_status`	The Requestors Web Interface page that is currently being displayed. This can have the following values: • `Open` • `Awaiting Response` • `Closed`

Return Values

An array, in the following format:

```
my $search = {Field1 => Value1, Field2 => Value2, ...};
```

Where each field in the array is a hash reference representing a search.

Supported fields are:

`Title`	The search's title. This will appear in the Requestors Web Interface. This field is mandatory.

`Format`	A string containing a comma-separated list of columns that should be included in the search results.
	For example:
	`my $Format = qq{`
	`'<B><A HREF="}. RT->Config->Get('WebPath')`
	`.qq{/SelfService/Display.html?id=__id__">__id__</a></B>/TITLE:Id',`
	`'<B><A HREF="}. RT->Config->Get('WebPath')`
	`.qq{/SelfService/Display.html?id=__id__">__Subject__</a>`
	`</B>/TITLE:Subject',`
	`'__CustomField.{Workflow}__`
	`',Status,OwnerName,Priority,CreatedRelative,LastUpdatedRelative};`
	This field is mandatory.

`Query`	An SQL query. For example: `Queue = 'Firewalls' AND id > 100 AND Requestor.EmailAddress LIKE 'algosec.com'` **Note:** If a field is missing from the query, a warning will be written to the log and the search will not be displayed. This field is mandatory.
`OrderBy`	An array of columns names, indicating the column by which search results should be sorted by default. The default value is `('LastUpdated')`. This field is optional.
`Order`	An array indicating the default sort order of the search results. This can have the following values: • `ASC`. Show the oldest search results first. • `DESC`. Show the most recent search results first. The default is `('DESC')`. This field is optional.
`Rows`	The number of search result rows to display per page. The default value is null. This field is optional.

For example:

```
my $search = {Title => "The title of the search",Format => $Format,Query => $Query,Orde
```

ValidateTicket

Note: The functionality of this hook is available in the FireFlow Web Interface as well. See Configuring Input Validation For Change Request Fields (see Configure field input validation).

Note: If you are validating fields that are not user defined custom fields, for the sake of parsing efficiency, you may want to disable the inclusion of these fields in the XML of a change request (*flat ticket*). See Enabling/Disabling Inclusion of User-Defined Custom Traffic Fields in Flat Tickets (see Enable / disable inclusion of user-defined custom traffic fields in flat tickets).

Syntax

```
sub ValidateTicket
```

Description

This function is called for every change request that is created or modified via the Web interface. It receives the change request (when the change request is new) as well as changes to the fields in the change request as input. It returns a return code and a list of error messages, so as to validate the change request.

Configuration

By default, this hook is not called. To configure the hook, complete the procedure below. You can optionally configure the hook to validate change requests with traffic information.

To enable the `ValidateTicket` hook, use the generic procedure for overriding system defaults to set the configuration parameter `ExternalValidateTicketFields` to the value 1. For details, see Override FireFlow system defaults.

Note: After setting this parameter, you must restart FireFlow for the change to take affect. See Restarting FireFlow (see Restart FireFlow).

Input Parameters

`$ticket`	A Perl hash reference containing a single key called `flatTicket`, which points to the flat ticket representation of the change request. **Note:** The hash will contain only data that was entered in the request form. The `ID` field will be set to "New". For details, see Flat Ticket Examples.
$isModify	A flag that says whether this is a newly created ticket, or a modification of an existing ticket.
$changes	A Perl hash of the changes for the ticket. In the case of a new ticket, this is all the values entered. If hook was called due to an action that modified the ticket, **$changes** contains a key named `actionTargetStatus` with the target status of the action.

Return Values

A return code and a list of error messages.

SuggestHostName

Syntax

```
sub SuggestHostName
```

Description

This function is called for every change request, in which the work order contains an IP address or subnet that is not associated with a hostname. It receives the change request as input, as well as the IP address/subnet and an indication of whether the IP address/subnet is a source or destination. It returns a suggested hostname for the IP address/subnet.

Configuration

By default, this hook is not called. To configure the hook, complete the procedure below.

To enable the `SuggestHostName` hook, ue the generic procedure for overriding system defaults to set the configuration parameter `SuggestHostNameInWorkOrder` to the value **1**. For details, see Override FireFlow system defaults.

Note: After setting this parameter, you must restart FireFlow for the change to take affect. See Restarting FireFlow (see Restart FireFlow).

Input Parameters

`$ticket`	A Perl hash reference containing a single key called `flatTicket`, which points to the flat ticket representation of the change request. For details, see Flat Ticket Examples.
`$ip`	The IP address or subnet that does not have an associated hostname.
`$field`	The IP address or subnet's function. This can have the following values: • `Source` • `Destination`

Return Values

A suggested hostname for the IP address/subnet.

SuggestGroupName

Note: The function of this hook is supported in the Web Interface via the following FireFlow traffic fields: **Requested Source Group Name**, **Requested Destination Group Name**, **Requested Service Group Name**.These fields appear in the **Standard** change request template by default, and they can be added to custom request templates.

For more details, seeManage request templates.

Note: Service group support can also be added via CSV file.

Syntax

```
sub SuggestGroupName
```

Description

This function is called for every change request, in which the work order contains a group of IP addresses/subnets or services that are not associated with a group name. It receives the change request as input, as well as the IP addresses/subnets or services (members) and an indication of whether the members are a source, destination, or service. It returns a suggested group name for the members.

Configuration

By default, this hook is not called. To configure the hook, complete the procedure below.

To enable the `SuggestGroupName` hook, use the generic procedure for overriding system defaults to set the configuration parameter `SuggestGroupNameInWorkOrder` to the value 1. For details, see Override FireFlow system defaults.

Note: After setting this parameter, you must restart FireFlow for the change to take affect. See Restart FireFlow.

Input Parameters

`$ticket`	A Perl hash reference containing a single key called `flatTicket`, which points to the flat ticket representation of the change request. For details, see Flat Ticket Examples.
`$trafficLineNumber`	The current traffic line in the change request.

`$trafficFieldType`	The IP addresses/subnets or services' function. This can have the following values: • `Source` • `Destination` • `Service`

Return Values

A suggested group name for the members.

SuggestPropertyValue

Syntax

```
sub SuggestPropertyValue
```

Description

This function is called for every change request in which the work order contains a Palo Alto or Fortimanager device. It returns a suggested value for the specified property in the change request's work order.

Input Parameters

`$ticket`	A Perl hash reference containing a single key called `flatTicket`, which points to the flat ticket representation of the change request. For details, see Flat Ticket Examples.
`$trafficLineNumber`	The current traffic line in the change request.
`$propertyName`	The name of the property to suggest. One or more of the following: • `SecurityProfileGroup` (for Panorama and Fortimanager) • `LogForwardingProfile` (for Panorama) • `Tags` (for Panorama) • `QualityOfService` (for Panorama)
`$currentValue`	The current value of the property, string, or reference to array.

Return Values

The suggested value for the property. This may be a string, or any array of strings. The string or array may be empty.

Note: Regardless of whether you suggest values for these properties with this hook, you can modify them by editing individual work orders. Any property excluded from the hook's logic will appear in the work order with FireFlow's default value. If desired, you can set custom default values for the `SecurityProfileGroup` and `LogForwardingProfile` properties. See Configuring the Security Profile and Log Forwarding Profile for Panorama Devices (see Configure security and log forwarding profiles for panorama devices).

SuggestServiceName

Syntax

```
sub SuggestServiceName
```

Description

This function is called for every change request, in which the work order contains a service that is not associated with a name. It receives the change request as input, as well as the service. It returns a suggested name for the service.

Configuration

By default, this hook is not called. To configure the hook, complete the procedure below.

To enable the `SuggestServiceName` hook, use the generic procedure for overriding system defaults to set the configuration parameter `SuggestHostNameInWorkOrder` to the value 1. For details, see Override FireFlow system defaults.

Note: This configuration parameter configures this hook as well as the SuggestHostName hook.

Note: After setting this parameter, you must restart FireFlow for the change to take affect. See Restarting FireFlow (see Restart FireFlow).

Input Parameters

`$ticket`	A Perl hash reference containing a single key called `flatTicket`, which points to the flat ticket representation of the change request. For details, see Flat Ticket Examples.
`$service`	The service that does not have an associated name.

Return Values

A suggested name for the service.

SuggestCommentSuffix

Syntax

```
sub SuggestCommentSuffix
```

Description

This function is called for every change request, in which the work order contains a suggested rule comment. It receives the change request as input, as well as the original rule comment and the rule comment suggested by FireFlow. It returns a suffix to be added to the rule comment suggested by FireFlow.

Configuration

By default, this hook is not called. To configure the hook, complete the procedure below.

To enable the `SuggestCommentsSuffix` hook, use the generic procedure for overriding system defaults to set the configuration parameter `SuggestCommentSuffixForWorkOrder` to the value **1**. For details, see Override FireFlow system defaults.

Note: After setting this parameter, you must restart FireFlow for the change to take affect. See Restarting FireFlow (see Restart FireFlow).

Input Parameters

`$ticket`	A Perl hash reference containing a single key called `flatTicket`, which points to the flat ticket representation of the change request. For details, see Flat Ticket Examples.
`$origComment`	The original rule comment.
`$commentValue`	The rule comment suggested by FireFlow.

Return Values

A suffix to be added to the rule comment suggested by FireFlow.

ValidateWorkOrderEdit

Syntax

```
sub ValidateWorkOrderEdit
```

Description

This function is called for every change request, in which the work order contains hostnames, host and service groups, and/or comments that were manually edited. It receives the change request as input, as well as the edited work order elements. It returns the elements that are invalid.

Configuration

By default, this hook is not called. To configure the hook, complete the procedure below.

To enable the **ValidateWorkOrderEdit** hook, use the generic procedure for overriding system defaults to set the configuration parameter **ExternalValidateWorkOrderEdit** to the value **1**. For details, see Override FireFlow system defaults.

Note: After setting this parameter, you must restart FireFlow for the change to take affect. For details, see Restart FireFlow.

Input Parameters

$ticket	A Perl hash reference containing a single key called **flatTicket**, which points to the flat ticket representation of the change request. For details, see Flat Ticket Examples.
$validationHash	A Perl hash reference containing the work order elements that were manually edited. The hash contains the following elements: • **objects** - The object names to be validated. • **groups** - The host and service groups to be validated. • **comments** - The comments to be validated.
$ruleNameInput	The rule name to be validated.

Return Values

$invalidHash	A Perl hash reference containing the work order elements that were found to be invalid.

EditRuleSectionHeader

Enables FireFlow administrators to select the header under which a new rule is recommended to be added.

This hook is relevant for change requests for Check Point R80 and R77 devices.

Note: Using this hook requires that the **AlgoSec_EA_CKP_R80_Layers** is set to **no**.

Syntax

```
sub EditRuleSectionHeader
```

Input Parameters

$sectionName	The name of the policy section under which you want new rules are recommended to be added.

Return Values

None.

ExcludeAcl

Syntax

```
sub ExcludeAcl
```

Description

This function is called while calculating a work order for every Cisco device in order to determine whether one or more ACLs that will appear in the work order should be excluded. If an ACL is excluded, the check box next to it will appear unchecked when the user views the work order.

Tip: See `$ExcludeACLsInWorkOrderByName` configuration parameter for a simpler method to exclude ACLs based on regular expression matching on the ACL name. For details, see Work order parameters.

Configuration

By default, this hook is not called. To configure the hook, complete the procedure below.

To enable the ExcludeAcl hook, use the generic procedure for overriding system defaults to set the configuration parameter `ExcludeACLsInWorkOrderByHook` to the value 1. For details, see Override FireFlow system defaults.

Note: After setting this parameter, you must restart FireFlow for the change to take effect. See Restart FireFlow.

Input Parameters

`$ticket`	A Perl hash reference containing a single key called `ticket`, which points to the ticket object.
`$aclName`	Name of the ACL.
`$interfacesNames`	Comma separated string of names of interfaces.
`$direction`	Direction of this ACL. One of the following: • `Incoming` • `Outgoing` • `Incoming,Outgoing`

Return Values

One of the following values:

1	ACL should be excluded. Do not add rules to this ACL.
0	ACL can be used.

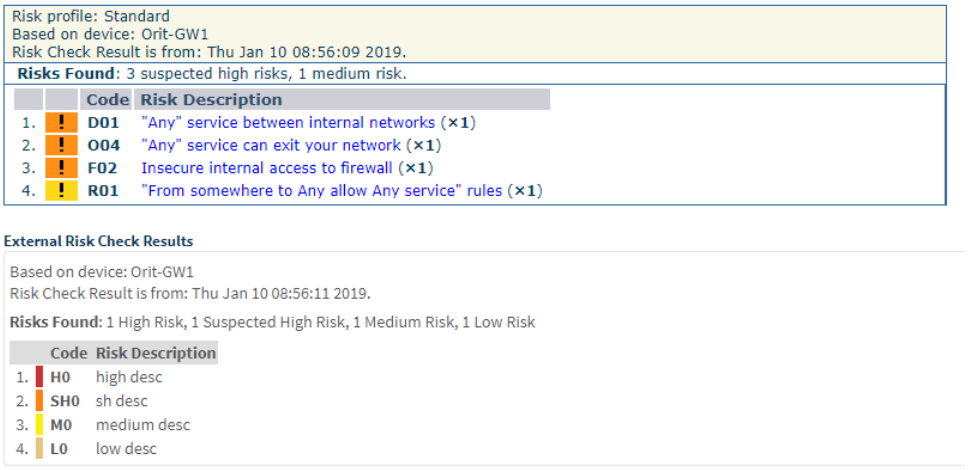
GetExternalRisks

Syntax

```
sub GetExternalRisks
```

Description

This function is called for every change request, after FireFlow has finished running a risk check. It receives the change request as input, along with a list of devices on which a risk check should be run. The risk check is run on an external system, and the function then returns the risk check results. These results are displayed in FireFlow after the FireFlow risk check results, for example:



Risk profile: Standard
Based on device: Orit-GW1
Risk Check Result is from: Thu Jan 10 08:56:09 2019.

Risks Found: 3 suspected high risks, 1 medium risk.

		Code	Risk Description
1.	!	D01	"Any" service between internal networks (×1)
2.	!	O04	"Any" service can exit your network (×1)
3.	!	F02	Insecure internal access to firewall (×1)
4.	!	R01	"From somewhere to Any allow Any service" rules (×1)

External Risk Check Results

Based on device: Orit-GW1
Risk Check Result is from: Thu Jan 10 08:56:11 2019.

Risks Found: 1 High Risk, 1 Suspected High Risk, 1 Medium Risk, 1 Low Risk

	Code	Risk Description
1.	H0	high desc
2.	SH0	sh desc
3.	M0	medium desc
4.	L0	low desc

Input Parameters

`$ticket`	A Perl hash reference containing a single key called `flatTicket`, which points to the flat ticket representation of the change request. For details, see Flat Ticket Examples.
`$firewall`	A Perl array reference containing an array of device names on which a risk check should be run. **Note:** These are the same devices on which the FireFlow risk check ran.

Return Values

A Perl hash reference containing the following keys:

- `RiskList`. An array of all the risks that were detected, sorted from high to low severity, where each risk is represented by a hash reference containing the risk's name, description, code, and severity.
- `profile`. The risk check's profile.
- `high`. The number of risks at the High severity level.
- `low`. The number of risks at the Low severity level.
- `medium`. The number of risks at the Medium severity level.
- `suspected high`. The number of risks at the Suspected High severity level.

Note: If there are no risks at a certain severity level, the relevant key will have no value defined.

FilterInitialPlanResults

Syntax

```
sub FilterInitialPlanResults
```

Description

This function is called for every change request, after FireFlow performs initial planning. It enables the removal of devices from the initial planning results. It receives the change request results from the AFA initial planning query, and the policy names of each device in the query results. It returns a list of devices removed from the initial query results. In the case when the hook removes all devices in the results, it will be ignored, and a warning will be issued.

Input Parameters

`$ticket`	A Perl hash reference containing a single key called `flatTicket`, which points to the flat ticket representation of the change request. For details, see Flat Ticket Examples.
`$firewallGroupQueryResult`	A Perl hash reference containing results from the AFA initial planning query.
`$firewallsHash`	A Perl hash reference containing the policy name of each device in the query results.

Return Values

A Perl array reference containing an array of device names which were removed from the initial planning results.

LoadConfigHook

Syntax

```
sub LoadConfigHook
```

Description

This function is called for every change request during initial planning. It enables saving pre-calculated data or configurations to the FireFlow server in-memory configuration, and retrieving the data later via other hooks or scrips. It receives the current program name as input.

Input Parameters

`$progName`	The current program name. The possible values are: • $FireFlow::Hooks::PROG_NAME_HTTPD • $FireFlow::Hooks::PROG_NAME_START_WORKER

Return Values

None.

Copy FireFlow customizations

AlgoSec® FireFlow™ includes a copy customization utility that can be used to copy user customizations between sites.

This section explains how to use this utility and the elements that are copied.

Copied files

The utility copies the following items:

Database entities

The utility copies the following database entities:

Queues	The following information is copied for each queue: • Description • CorrespondAddress • CommentAddress • InitialPriority • FinalPriority • DefaultDueIn • SubjectTag • Disabled • Attributes: AdminGroupID, SecurityGroupID, NetworkGroupID, ReadOnlyGroupID, ControllersGroupID (according to the ID of the created groups) **Note:** If a queue's name is changed on the original site, the utility will create both a queue with the original name and a queue with the new name on the target site.

Roles	The following information is copied for each role: • Description • Disabled • Global permissions, including permissions for roles • Queue permissions per queue, including permissions for roles • Role Permissions • Home Page settings • The role's membership in other role **Note:** When updating FireFlow, global permissions, queue permissions, and role permissions that are not in a customization file will be revoked. **Note:** If a role's name is changed on the original site, the utility will create both a role with the original name and a role with the new name on the target site. **Note:** Since the utility does not copy users and their role memberships, it will be necessary to define the users as members of the new role on the target site.

Custom fields	All custom fields are copied, including those for change requests, users, and roles. The following information is copied for each custom field: • Description • DisplayName • Type • ValuesClass • LookupType • Pattern • LinkValueTo • IncludeContentForValue • Category • DefaultValue • Disabled • HideIfEmpty **Note:** When updating FireFlow, custom fields that do not appear in the customization file will be removed. Furthermore, custom fields referring to queues, system role permissions, or user-defined role permissions that do not appear in the customization file will be removed. **Note:** If a custom field's name is changed on the original site, the utility will create both a custom field with the original name and a custom field with the new name on the target site.

Request templates	The following information is copied for each request template: • Description • All defined values **Note:** If a request template's name is changed on the original site, the utility will create both a template with the original name and a template with the new name on the target site. **Note:** Request templates cannot be disabled; therefore, the utility will not remove them from the target site.
Email templates	All email templates are copied, including both global and per queue. The following information is copied for each email template: • Name • Description • Content **Note:** Email templates cannot be disabled; therefore, the utility will not remove them from the target site.
Scrips	All scrips are copied, including both global and per queue. The following information is copied for each scrip: • Description • Stage • CustomIsApplicableCode (in case of a user-defined condition) • CustomPrepareCode (in case of a user-defined action) • CustomCommitCode (in case of a user-defined action) • ScripAction name • ScripCondition name • Email Template name **Note:** FireFlow scrips have no name; therefore, if two scrips have the same description, only one of them will be updated.

Saved searches
Global Home Page settings

Configuration files

The utility copies the following configuration files:

Workflows_Config.xml	The workflow configuration file `/usr/share/fireflow/local/etc/site/Workflows_Config.xml` The utility overwrites this file on the target site.
Workflows directory	All workflow files located under `/usr/share/fireflow/local/etc/site/Workflows/` The utility overwrites everything in this folder on the target site.
SuggestedAddressObjects_Config.xml	The suggested source/destination addresses list `/usr/share/fireflow/local/etc/site/SuggestedAddressObjects_Config.xml` The utility overwrites this file on the target site.
FireFlow_Config.json	The FireFlow site configuration file `/usr/share/fireflow/local/etc/site/FireFlow_Config.json` The utility adds all parameters in the file that do not include the words Email, Password, Address, or FAUser to the the parallel file on the target site, that is, all user and password-related parameters are not copied. Other parameters are updated or added to the end of the file on the target site. The file on the original site is backed up before it is edited.

Translation files

The utility copies all translation files located under `/usr/share/fireflow/local/etc/site/po`.

Scripts for uploading change requests from files

The utility copies all scripts for uploading change requests from files, located under `/usr/share/fireflow/local/etc/site/bin`.

Hook Files

The utility copies all hook files and related configuration files located under `/usr/share/fireflow/local/Hooks` and `/usr/share/fireflow/local/etc/site/Hooks`.

Web Service Clients

The utility copies all Web service clients located under `/usr/share/fireflow/local/WebServiceClient/`. It overwrites everything in this folder on the target site.

Create a customization file to copy

In order to copy customizations from the original site to a target site, you must create a customizations file using the following procedure.

Do the following:

1. On the original site, open a terminal and log in using the username "root" and the related password.
2. Enter the following command:

   ```
   /usr/share/fireflow/local/sbin/copy_fireflow_customization.pl
   --run -d -fCustFile [-e]
   ```

   For more details, see Customizations Utility Flags.

   A customizations file is created containing the data described in Copied files, and saved to the current directory.

Customizations Utility Flags

Flag	Description
-f ***CustFile***	The name under which to save the customizations file. The default value is `user_customizations_yyyy-mm-dd-hhmmss.tar.gz`, where yyyy-mm-dd-hhmmss is a timestamp. For example: `user_customizations_2010-09-07-091318.tar.gz`
-e	Do not include disabled roles and disabled custom fields in the customizations file.

Load a customizations file to the Target Site

Once you have created a customizations file, you can load it to the target site.

After running `copy_fireflow_customization.pl -l` to load the customization, the workflow files that were loaded need to enter the VisualFlow internal database, discarding any information that was already there.

Do the following:

1. On the target site, open a terminal and log in using the username "root" and the related password.

   Note: The "root" user must have read permissions for the customizations file; otherwise, loading the file will fail.

2. Enter the following command:

   ```
   /usr/share/fireflow/local/sbin/copy_fireflow_customization.pl
   --run -l -f CustFile [-u] [-r]
   ```

   For more details, see Customizations Utility Flags.

   The `fireflow_backup` utility runs and backs up FireFlow to the directory `/var/fireflow/backup`.

   Apache Web service and FireFlow workers both stop.

The customizations file is loaded to the target site. Data is overwritten and/or added as described in Copied files.

Apache Web service restarts.

FireFlow workers start automatically every 5 minutes, as configured on the server's cron.

3. Refresh the workflows, by doing the following:
    a. Access VisualFlow. For details, see Get started in VisualFlow.
    b. In the VisualFlow main menu, click **Apply Workflow Changes**.

       The **Apply Changes** page is displayed.
    c. To delete all workflow drafts, in the Discard changes to workflows section, click **Discard all changes**.

       A confirmation message appears.
    d. Click **OK**.
    e. Click **Refresh Workflows**.

The workflows are loaded into FireFlow.

Customizations Utility Flags

Flag	Description
`-f` *CustFile*	The name under which to save the customizations file. The default value is `user_customizations_yyyy-mm-dd-hhmmss.tar.gz`, where yyyy-mm-dd-hhmmss is a timestamp. For example: `user_customizations_2010-09-07-091318.tar.gz`
`-u`	Update existing elements on the target site with data from the customizations file. If this flag is not used, only new elements will be added. **Note:** This option is available when -l is used.

Flag	Description
`-r`	Remove database entities that do not appear in the customizations file from the target site. The entities will be marked as disabled. **Note:** This option is available when -l is used.
-d	Dump customization to file **Note**: -d and -l are mutually exclusive.
-l	Load customization from file **Note**: -d and -l are mutually exclusive.
-e	Do not include disabled roles and disabled custom fields in the customizations file.
-x	Skip backup

Restart FireFlow

After making certain FireFlow configuration changes, it is necessary to restart all FireFlow workers that are running background tasks, as well as restart Apache. The FireFlow restart utility enables you to perform all the necessary restart actions with a single command.

Note: Any procedures that require restarting FireFlow are marked as such.

Do the following:

1. Log in to the FireFlow server using the username "root" and the related password.
2. Enter the following command:

```
restart_fireflow
```

All FireFlow workers that are currently running background tasks are restarted.

Apache is restarted.

FireFlow troubleshooting

This section explains how to troubleshoot FireFlow.

Consult FireFlow log files

You can download a ZIP containing all FireFlow log files.

If desired, you can also access the following log files directly:

- **/usr/share/fireflow/var/log/fireflow.log**. The main FireFlow log file.
- **/usr/share/fireflow/local/VisualFlow/log/production.log**. The VisualFlow log file.
- **/var/log/httpd/error_log**. The Apache error log file.

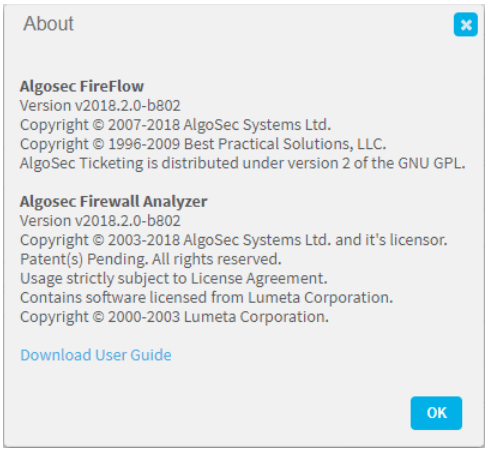
Note: In order to access these log files directly, you must log in to the FireFlow server via SSH with the username "root". The default password for this user on an AlgoSec Hardware Appliance or a VM is "algosec".

Download FireFlow logs

Do the following:

1. In the toolbar, click your username.
2. A drop-down menu appears.
3. Select **About.**

   The **About** dialog box appears.



4. To **Download General Support Zip**, click **Support** in the **Admministrator** drop-down menu.

   A ZIP file called `FireFlow_support.zip` is downloaded to your computer.

5. Click **OK**.

Configure debug mode and send updated log files

On occasion, the AlgoSec support team may request that you configure debug mode, which produces log files with additional detail.

Do the following:

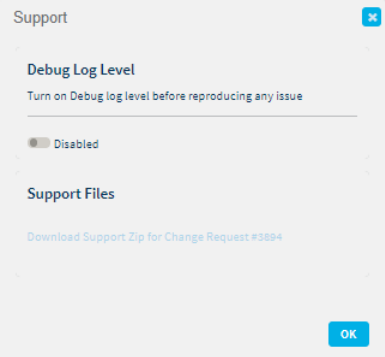
1. Open the **Support** dialog box, by doing the following:

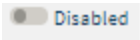
   a. In the toolbar, click your username.

      A drop-down menu appears.

   b. In the menu, select **Support**.

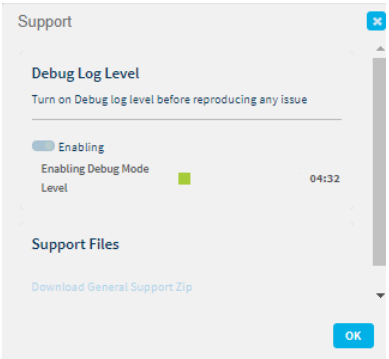
The **Support** dialog box opens.



2. Enable Debug mode by clicking 

.

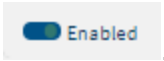
   The icon changes to **Enabling**, and the progress bar appears.



   When the process completes successfully, the following occurs:

   - Debug mode is enabled
   - The icon toggles to **Enabled**
   - The **Download Support Zip** link is enabled
   - A notification appears at the top of the page

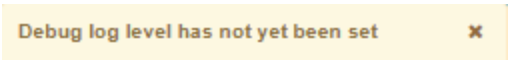
3. Reproduce the problem you experienced.
4. Reopen the **Support** dialog box.
5. Download the support files by clicking the **Download General Support Zip** link.

6. Disable Debug mode by clicking 

.

   When the process completes successfully, the following occurs:

   - Debug mode is disabled
   - The icon toggles to **Disabled**
   - The **Download Support Zip** link is disabled
   - A notification appears at the top of the page

7. Send the files to customer support.

Send us feedback

Let us know how we can improve your experience with the Configuration Guide.

Email us at: techdocs@algosec.com

Note: For more details not included in this guide, see the online ASMS Tech Docs.