# AlgoSec FireFlow

Software Version: A30.10

# User Guide

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

**Document Release Date**: 12 April, 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.

# Contents

# Welcome to FireFlow

AlgoSecFireFlow automates the security policy change lifecycle, from the time a change request is submitted to auditing the change made. Use FireFlow to make changes on your security policies ensures that device changes are approved, necessary, and implemented as intended.

## Change request lifecycles

FireFlow translates each request made into an actionable policy change, and then analyzes any related devices, routers, and VPNs to verify that the change is indeed needed.

FireFlow identifies the exact rules that need changing, checking the impact of the request on the overall network security. FireFlow makes these change to identify potential risks.

FireFlow ActiveChange enables you to make the change on the device directly from FireFlow. After the change is made, either manually or via ActiveChange, FireFlow validates the change made to ensure that it matches the request correctly.

### Default templates and workflows

FireFlow's templates and workflows enable you to carry each change request through the following default steps:

- Request changes
- Initial planning
- Approve planned changes
- Review change requests
- Implement changes
- Validate changes
- Match changes to requests

- Re-certify traffic
- Manage change requests

While FireFlow's templates and workflows are highly customizable, the out-of-the box defaults are fully functional for standard and common tasks. For more details, see Request templates and workflows.

## FireFlow users

FireFlow users include the following:

- **Unprivileged users**. Includes requestors, who can only open change requests and track the status of their own requests. Requestors have a minimized FireFlow interface, showing only the elements available to them.
- **Privileged users**. Includes all other FireFlow users, such as network operators, security officers, and FireFlow administrators. Privileged users have access to more areas of the UI, depending on their user configuration.

## Navigate around FireFlow

Use FireFlow's main menu on the left to navigate around FireFlow and determine the details shown in the workspace.

- To hide and un-pin the main menu, click ◀ at the top of the screen. Click ▶ to show the menu again and keep it pinned.
- On each page in the workspace, click ▶ to expand details for each area. Click ▼ to hide it again.

# 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

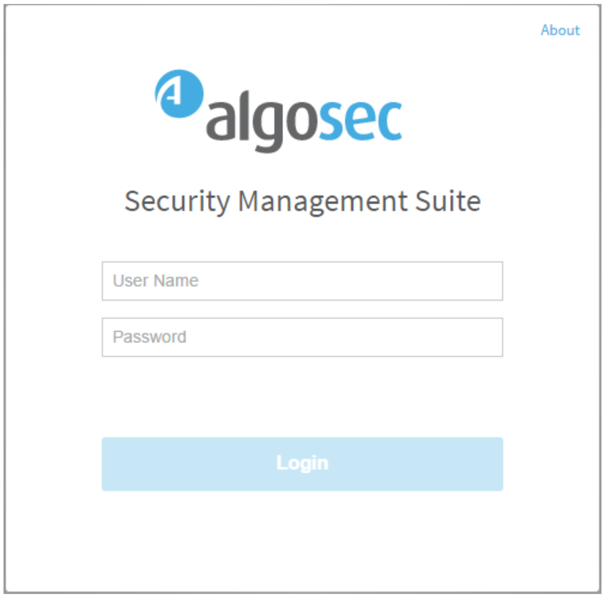
Log in to ASMS from any desktop computer using the credentials provided by an AFA administrator.

### 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.

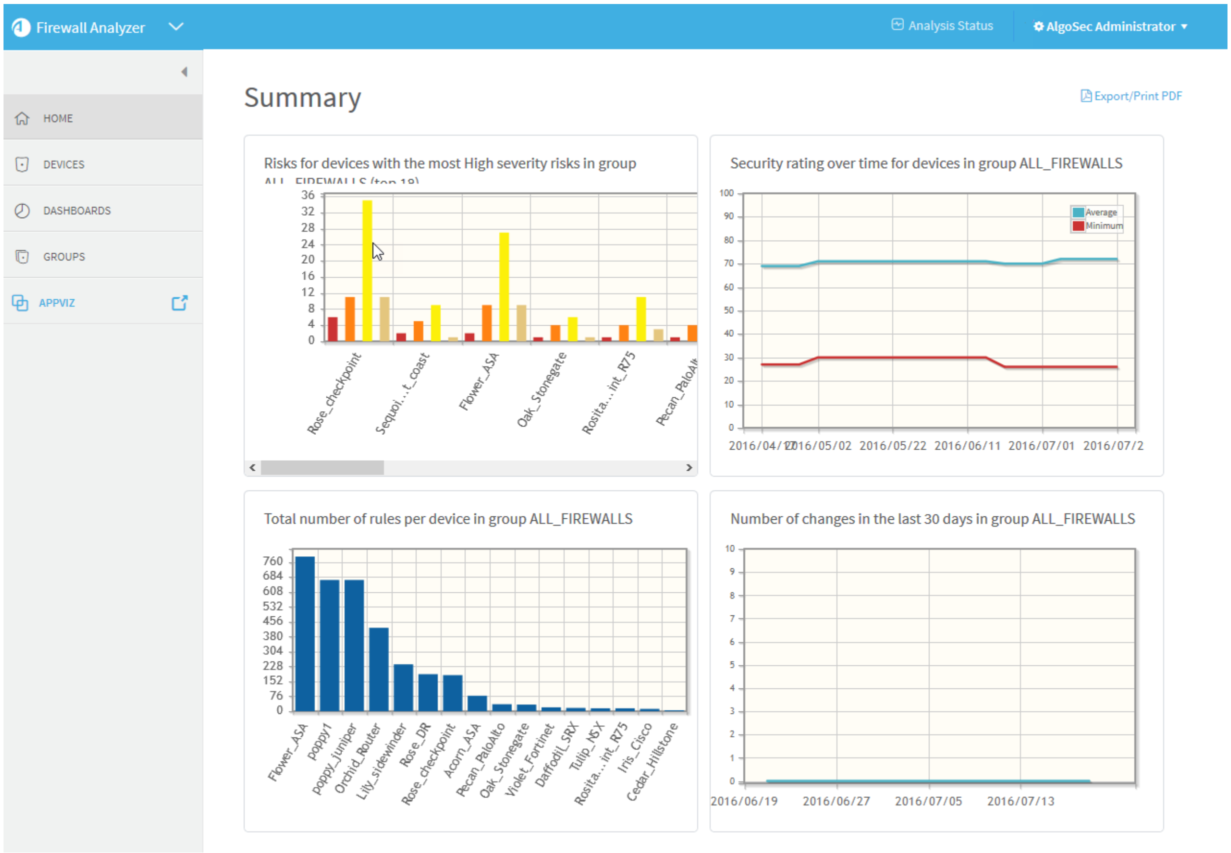
   The **Security Management Suite** login page appears.



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

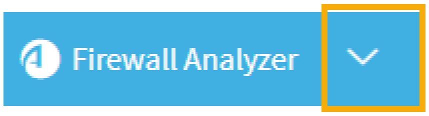
You are logged in, and ASMS displays AFA by default.

For example:

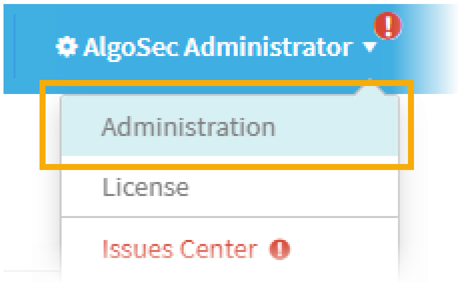


## Switch ASMS products

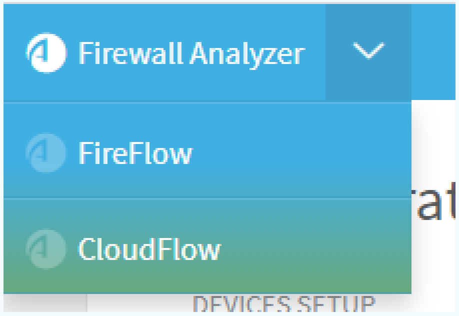
If you are a user in multiple ASMS products, such as AFA, FireFlow, and AppViz, switch between products using the dropdown at the top-left, above the main menu.



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.

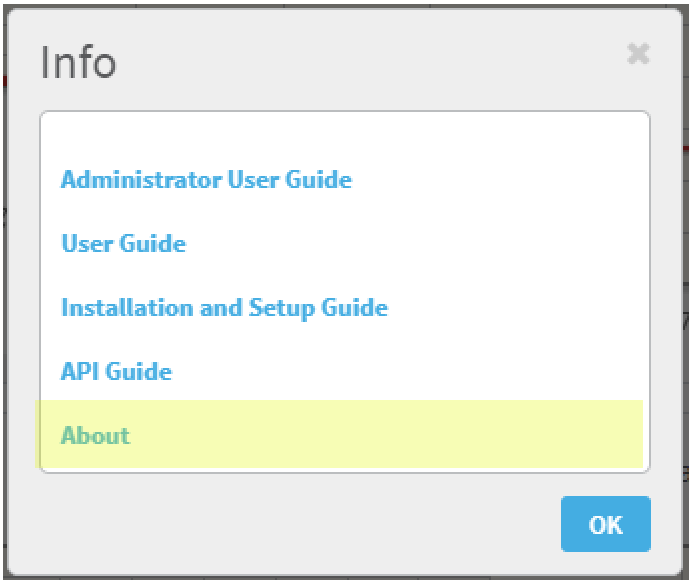
- **To adjust the size of the main menu**, hover between the menu and the workspace and drag the border left or right.
- **To collapse the menu entirely**, click ◀ at the top. When collapsed, click ▶ to expand it again.

## View ASMS product details

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

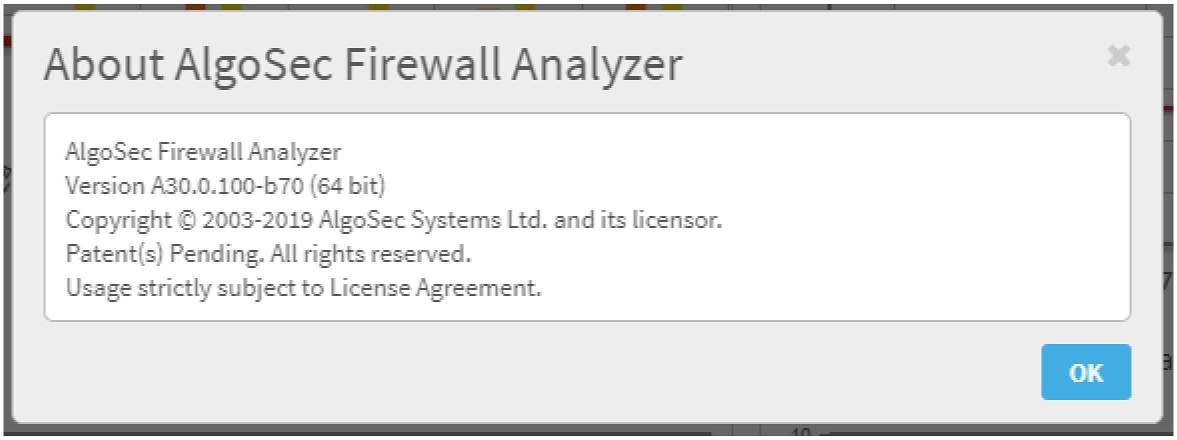
### Do the following:

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:



AlgoSec Firewall Analyzer
Version A30.0.100-b70 (64 bit)
Copyright © 2003-2019 AlgoSec Systems Ltd. and its licensor.
Patent(s) Pending. All rights reserved.
Usage strictly subject to License Agreement.

**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*.

# Request templates and workflows

The lifecycle of a FireFlow change request differs, depending on the request template used, and the workflow configured for that template.

This topic describes the lifecycles provided by the default request templates and workflows.

FireFlow administrators can also configure changes and create custom request templates and workflows.

## Default request templates

FireFlow provides the following request templates out-of-the box, each configured for one or more default workflows. The links in this section reference descriptions of the default stages included in each of these workflows.

For details about how to perform related procedures for each stage, see Default lifecycle stages.

**Tip:** Custom workflows can aso be configured for default templates as relevant.

### Requestor change requests

The following change request templates are open to all FireFlow users.

| Name | Description |
|---|---|
| **Traffic change requests** | Used to request changes in network traffic. By default, related to the following workflows:<br>• **Basic**<br>• **Standard**<br>• **Multi-Approval**<br>• **Parallel-Approval**<br>• **Automatic Traffic Change**<br>For details, see Traffic change workflow. |

| Name | Description |
|---|---|
| **IPv6 traffic change requests** | Used to create traffic change requests for IPv6 traffic, for Cisco devices only.<br>By default, related to the **Traffic Change Request (IPv6)** workflow.<br>For details, see IPv6 traffic change workflow. |
| **Multicast traffic change requests** | Used to create multicast traffic change requests, for Cisco devices only.<br>By default, related to the **Traffic Change Request (Multicast)** workflow.<br>For details, see Multicast traffic change workflow. |
| **Web filter change requests** | Used to request changes in web filtering.<br>By default, related to the **Web-Filter** workflow.<br>For details, see Web filtering change workflow. |
| **New device configuration change requests** | Used to create requests for new device configurations.<br>By default, related to the **New Device Configuration** workflow. |
| **Generic change requests** | Used to create generic change requests, unrelated to traffic changes, device/object changes, enabling or disabling device rules, or web filtering.<br>By default related to the **Generic** workflow.<br>For details, see Generic change workflow. |

## Privileged change request templates

The following change request templates are open to privileged users only.

| Name | Description |
|---|---|
| **Object Change (single device) requests** | Used to create change requests for object changes on a single device.<br>By default, related to the **Object Change** workflow.<br>For details, see Object change workflow. |

| Name | Description |
|---|---|
| **Object Change (multiple devices) requests** | Used to create change requests for object changes on a multiple devices.<br>By default, related to the **Object Change Multi Device** workflow.<br>Supported only via API.<br>For details, see Multi-device object change workflow. |
| **Rule Removal requests** | Used to create change requests to remove a network policy rule.<br>By default, related to the **Rule Removal** workflow.<br>For details, see Rule removal workflow. |
| **Rule Modification requests** | Used to create change requests to modify a network policy rule.<br>By default, related to the **Rule Modification** workflow.<br>For details, see Rule modification workflow. |
| **Recertification requests** | Used to create requests to recertify Allow traffic added as the result of a traffic request.<br>Available only to network operations users only.<br>By default, related to the **Request-Recertification** workflow.<br>For details, see Re-certification workflow. |

## Default workflows

When a FireFlow user opens a new change request, FireFlow uses the workflow assigned to the request's configured template. If a request template has no workflow configured, FireFlow uses a set of rules to determine the workflow to use.

If these rules still cannot find the required workflow, FireFlow uses the Basic workflow by default.

The following tables describe FireFlow's built-in workflows, as they are configured out-of-the-box.

For more details, see Default templates and workflows.

## Traffic change workflows

The following workflows are relevant for changes requested in traffic.

| Workflow | Description |
|---|---|
| **Standard** | Default workflow, suitable for all traffic requests.<br>Default stages include: Request, Plan, Approve, Implement, Validate, Match, Resolved, and Audit. |
| **Multi-Approval** | Used for traffic change requests that require sequential approval from multiple users, and includes the extra **Review** approval stage, performed by a controller user.<br>Default stages include: Request, Plan, Approve, Review, Implement, Validate, Resolved, and Audit. |
| **Parallel-Approval** | Used for traffic change requests that require parallel approval from multiple users, and includes the extra **Review** approval stage, performed by a controller user.<br>Default stages include: Request, Plan, Approve, Review, Implement, Validate, Resolved, and Audit. |
| **IPv6-Traffic** | Used for requests involving IPv6 traffic, for Cisco devices only.<br>Default stages include: Request, Plan, Approve, Implement, Validate, Resolved, and Audit. |
| **Request-Recertification** | Used to determine whether **Allow** traffic added to a device policy as the result of an expired traffic change request is still relevant.<br>If the rule is no longer relevant, a Rule Removal change request is created to remove it.<br>Default stages include: Request, Certify, Implement, Validate, Resolved, and Audit. |
| **Multicast-Traffic** | Used for requests for Multicast traffic changes, for Cisco devices only.<br>Default stages include: Request, Plan, Approve, Implement, Validate, Resolved, and Audit. |

| Workflow | Description |
|---|---|
| **Automatic-Traffic-Change** | Used for traffic requests with **Allow** traffic only. Lifecycle changes proceed automatically.<br>Default stages include: Request, Plan, Approve, Implement, Validate, Match, Resolved, and Audit. |

## Device and rule change workflows

The following workflows are used for changes requested on devices or device rules.

| Workflow | Description |
|---|---|
| **Change-Object** | Used for requests to add, remove, or modify device objects.<br>Default stages include: Request, Approve, Implement, validate, Resolved, and Audit. |
| **Object-Change-Multi-Device** | Used for requests to change device objects on multiple devices.<br>Available only for change requests opened via API.<br>Default stages include: Request, Plan, Approve, Implement, Validate, Resolved, and Audit. |
| **Rule-Removal** | Used for requests to remove or disable device rules.<br>Default stages include: Request, Approve, Implement, Validate, Resolved, and Audit. |
| **Rule-Modification** | Used for requests to modify a rule's fields, such as source, destination, or service.<br>Default stages include: Request, Approve, Implement, Validate, Match, Resolved, and Audit. |
| **Bulk-Rules-Addition** | Used for requests to add many rules to a device.<br>Default stages include: Request, Plan, Implement, Resolved, Match, and Audit. |

## Other workflows

The following workflows are used on changes requested for anything other than traffic, device, or rules.

| Workflow | Description |
|---|---|
| **Generic** | Used for requests not related to traffic.<br>No device change planning or matching device changes to the request are required.<br>Default stages include: Request, Approve, Implement, Validate, Resolved, and Audit. |
| **Web-Filter** | Used for requests to filter Web connections. Relevant for Symantec Blue Coat devices only.<br>Default stages include: Request, Plan, Approve, Implement, Validate, Resolved, and Audit. |

## Default lifecycle stages

The following table lists each default lifecycle stage with action items for users, and the types of FireFlow users who perform that stage.

| Stage | Description |
|---|---|
| **Request** | Performed by all FireFlow users.<br>For details, see Request changes. |
| **Plan** | Performed by network operators.<br>For details, see Initial planning. |
| **Approve** | Performed by network operators or information security officers.<br>For details, see Approve planned changes. |
| **Review** | Performed by controllers only. For details, see Review change requests. |
| **Implement** | Performed by network operators only. For details, see Implement changes. |
| **Validate** | Performed by network operators only. For details, see Validate changes. |
| **Match** | Performed by information security officers. For details, see Match changes to requests. |
| **Resolved** | Performed by network operators only. For details, see Re-certify traffic. |

**Tip:** FireFlow also enables you to perform more advanced operations, and also view data in reports and dashboards.

For details, seeReports, charts, and dashboards.

## Generic change workflow

This topic describes the events that occur in each stage in a default generic change workflow.

**Note:** FireFlow is fully configurable, and your system may differ.

### Request

In the Request stage, a requestor submits a request for a generic change, initiating the FireFlow change request lifecycle. This stage consists of the following steps:

1. The requestor selects a template on which to base their request.
2. If the template specifies a workflow, FireFlow assigns the request to that workflow.
3. The requestor submits the request to FireFlow.
4. FireFlow receives the request information and creates a *change request*.
5. If a workflow has not yet been assigned, FireFlow assigns a workflow. For more details, see Request templates and workflows.
6. The *default assignee* of the role handling new change requests (by default, the Network Operations role) is assigned as the change request's *owner*.
7. FireFlow sends an email message informing the requestor that the change request was created, and specifying the change request ID in the format [FireFlow #<*number*>], for example [FireFlow #49].

### Approve

In the Approve stage, a user with the information security role determines the security risks entailed in satisfying the request. This stage consists of the following steps:

1. The *default assignee* of the role handling change requests in the Approve stage (by default, the Information Security role) is assigned as the change request's owner.
2. The change request may change ownership in one of the following ways:
   - The change request owner assigns it to a user with the information security role.
   - An information security user chooses to take responsibility for the change request.
3. The information security user initiates a manual check to determine whether there would be any risks entailed in implementing the requested change.
4. The information security user does one of the following:
   - Approves the change request and sends it on to the next stage.
   - Rejects the change request. In this case the change request returns to the start of the Approve stage.
   - Rejects and closes the change request. In this case, an email message is sent to the requestor, indicating that the request is denied.
   - Contacts the requestor and asks for more information.

## Implement

In the Implement stage, the network operations user plans and executes request implementation. This stage consists of the following steps:

1. The change request's ownership is returned to the network operations user.
2. The network operations user implements the requested changes.
3. The network operation user sends the change request on to the next stage.

## Validate

In the Validate stage, the requestor checks that the request was implemented, and the network operations user resolves the change request. This stage consists of the following steps:

1. The network operations user composes an email message in FireFlow, notifying the requestor that the requested changes were implemented.
2. FireFlow sends the email to the requestor.
3. The requestor checks that the requested change was implemented and the desired result was achieved.
4. One of the following things happens:
    - If the desired result was not achieved, the requestor responds via an email message or via the Web interface, and the network operations user then re-initiates the implementation stage.
    - If the desired result was achieved, the requestor responds via an email message or via the Web interface, and the network operations user then resolves the change request.
    - If the requestor does not respond, the network operations user can choose to resolve the change request anyway.

At this point, the change request's lifecycle has effectively ended, and no further user action is required. However, the change request remains available in the system for auditing purposes, as described in the final stages.

### Resolved

Once the change request has been validated, it enters the Resolved stage.

### Audit

The Audit stage for generic change request lifecycles is identical to the Audit stage for traffic change request lifecycles. See Audit (see Audit).

## Traffic change workflow

This topic describes the events that occur in each stage in a default traffic change workflow.

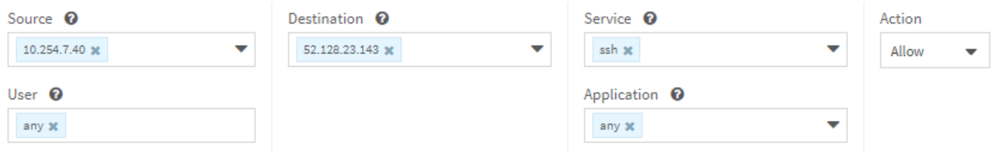
**Note:** FireFlow is fully configurable, and your system may differ.

## Request

In the Request stage, a requestor submits a request for a device traffic change, initiating the FireFlow change request lifecycle. This stage consists of the following steps:

1. The requestor selects a template on which to base their request.
2. If the template specifies a workflow, FireFlow assigns the request to that workflow.
3. The requestor submits the request to FireFlow.

   The request **must** include information about the relevant source, destination, service/application, and action for the change. For example, the requestor may submit the following request:

   Source: 10.254.7.40

   User: any

   Destination: 52.128.23.143

   Service: ssh

   Application: any

   Action: Allow

4. FireFlow receives the request information and creates a *change request*.
5. If a workflow has not yet been assigned, FireFlow assigns a workflow. For more details, see [Request templates and workflows](#).
6. The *default assignee* of the role handling new change requests (by default, the Network Operations role) is assigned as the change request's *owner*.
7. FireFlow sends an email message informing the requestor that the change request was created, and specifying the change request ID in the format [FireFlow #<*number*>], for example [FireFlow #49].
8. FireFlow checks the traffic specified in the change request against the network security policy. If the traffic is already allowed (in case of a request to allow traffic), then FireFlow automatically closes the change request and sends you an email indicating that the change request was closed.

## Plan

In the Plan stage, a user with the network operations role plots out the technical changes needed in order to satisfy the change request. This stage consists of the following steps:

1. The change request may change ownership in one of the following ways:
   - The change request owner assigns it to a user with the network operations role.
   - A network operations user chooses to take responsibility for the change request.
   - Conditional logic was configured to dynamically choose the responsible role, based on request properties.
2. FireFlow initiates a query on the indicated device group (by default, the ALL_FIREWALLS group) to identify relevant devices or policies.

   If the requestor did not provide adequate information, the network operations user contacts the requestor to clarify the request details and then modifies the request details as needed.
3. The network operations user uses the FireFlowinitial plan results to identify the devices or policies that are relevant to the requested change.
4. If the network user modified the traffic, FireFlow tests whether the requested traffic is already allowed. If the traffic is already allowed, the network operations user closes the change request, and FireFlow sends an email message to the requestor indicating that the change request was closed.
5. If there is more than one device or policy that is relevant to the change, the network operations user selects the devices or policies on which to implement the change.
6. The network operation user confirms the devices, sending the change request to the next stage.
7. If the network operations user selected multiple devices or policies, FireFlow will generate sub-requests for each.

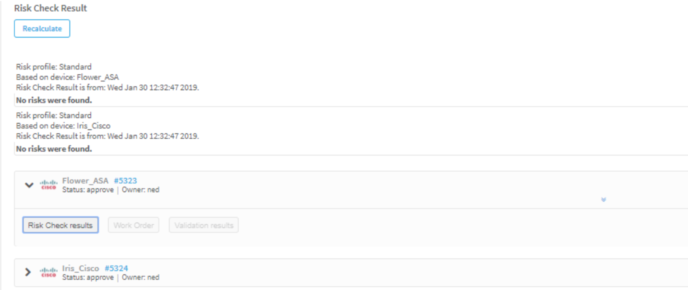
## Approve

In the Approve stage, a user with the information security role determines the security risks entailed in satisfying the request. This stage consists of the following steps:

1. The *default assignee* of the role handling change requests in the Approve stage (by default, the Information Security role) is assigned as the change request's owner.
2. The change request may change ownership in one of the following ways:
   - The change request owner assigns it to a user with the information security role.
   - An information security user chooses to take responsibility for the change request.
   - Conditional logic was configured to dynamically choose the responsible role, based on request properties.
3. If the change request includes an "Allow" action, FireFlow initiates a risk check, to determine whether implementing the requested Allow traffic change will introduce risks.

   FireFlow returns the number and severity of risks detected:

   In the case of policy-based requests, the risk check runs on one of the devices with the policy.

   Risk Check Result

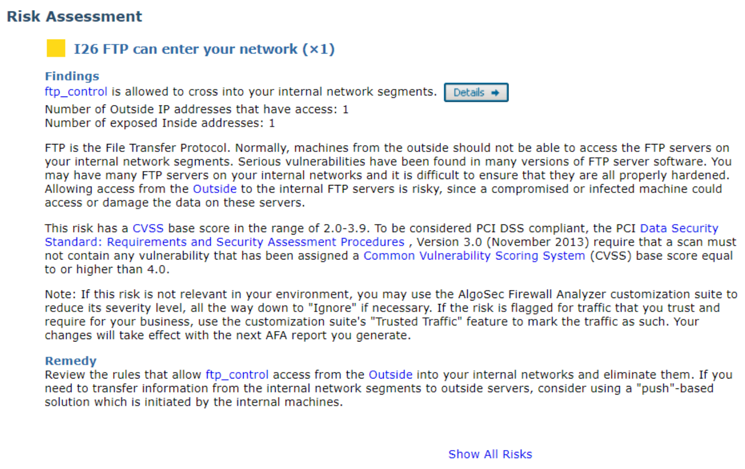
   Risk profile: Standard
   Based on device: Flower_ASA
   Risk Check Result is from: Wed Jan 30 12:32:47 2019.
   **No risks were found.**

   Risk profile: Standard
   Based on device: Iris_Cisco
   Risk Check Result is from: Wed Jan 30 12:32:47 2019.
   **No risks were found.**

   Flower_ASA #5323
   Status: approve | Owner: ned

   Iris_Cisco #5324
   Status: approve | Owner: ned

   The user can view a risk assessment of each risk:



**Risk Assessment**

🟨 **I26 FTP can enter your network (×1)**

**Findings**
ftp_control is allowed to cross into your internal network segments.
Number of Outside IP addresses that have access: 1
Number of exposed Inside addresses: 1

FTP is the File Transfer Protocol. Normally, machines from the outside should not be able to access the FTP servers on your internal network segments. Serious vulnerabilities have been found in many versions of FTP server software. You may have many FTP servers on your internal networks and it is difficult to ensure that they are all properly hardened. Allowing access from the Outside to the internal FTP servers is risky, since a compromised or infected machine could access or damage the data on these servers.

This risk has a CVSS base score in the range of 2.0-3.9. To be considered PCI DSS compliant, the PCI Data Security Standard: Requirements and Security Assessment Procedures , Version 3.0 (November 2013) require that a scan must not contain any vulnerability that has been assigned a Common Vulnerability Scoring System (CVSS) base score equal to or higher than 4.0.

Note: If this risk is not relevant in your environment, you may use the AlgoSec Firewall Analyzer customization suite to reduce its severity level, all the way down to "Ignore" if necessary. If the risk is flagged for traffic that you trust and require for your business, use the customization suite's "Trusted Traffic" feature to mark the traffic as such. Your changes will take effect with the next AFA report you generate.

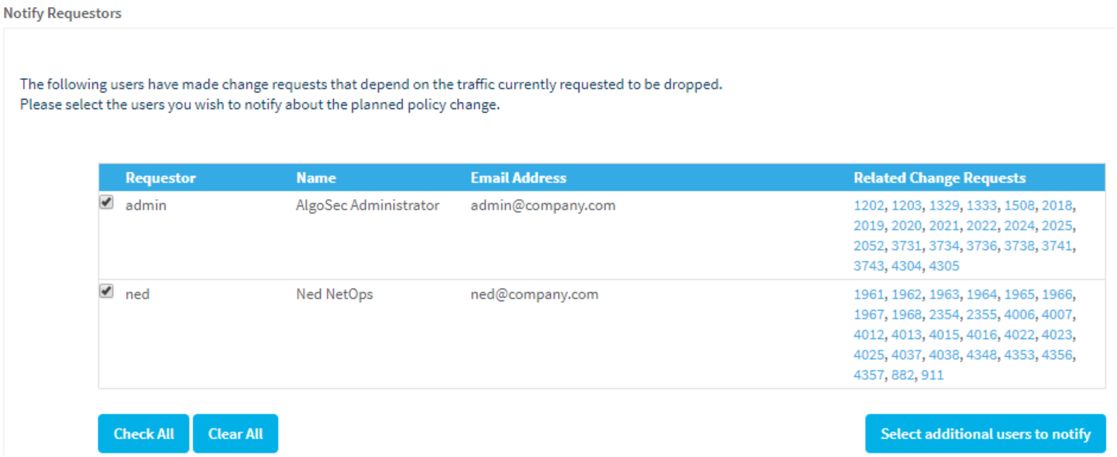
**Remedy**
Review the rules that allow ftp_control access from the Outside into your internal networks and eliminate them. If you need to transfer information from the internal network segments to outside servers, consider using a "push"-based solution which is initiated by the internal machines.

4. If the change request includes a "Drop" action, the following happens:

   a. The network operations user initiates a search for change requests whose traffic will be blocked by the "Drop" action.

   b. FireFlow returns a list of related change requests.

   c. The network operations user then specifies which of the related change requestors (and optionally other users) should receive a notification that the traffic will be blocked.



Notify Requestors

The following users have made change requests that depend on the traffic currently requested to be dropped.
Please select the users you wish to notify about the planned policy change.

| Requestor | Name | Email Address | Related Change Requests |
|---|---|---|---|
| ☑ admin | AlgoSec Administrator | admin@company.com | 1202, 1203, 1329, 1333, 1508, 2018, 2019, 2020, 2021, 2022, 2024, 2025, 2052, 3731, 3734, 3736, 3738, 3741, 3743, 4304, 4305 |
| ☑ ned | Ned NetOps | ned@company.com | 1961, 1962, 1963, 1964, 1965, 1966, 1967, 1968, 2354, 2355, 4006, 4007, 4012, 4013, 4015, 4016, 4022, 4023, 4025, 4037, 4038, 4348, 4353, 4356, 4357, 882, 911 |

   d. FireFlow sends an email to the selected requestors.

   e. The requestors respond via an email message or the web interface.

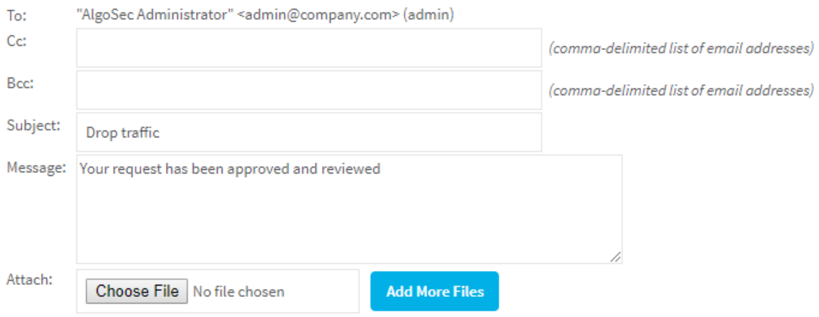
5. The information security user does one of the following:

- Approves the change request and sends it on to the next stage.
- Rejects the change request and returns it to the Plan stage.
- Rejects and closes the change request. In this case, an email message is sent to the requestor, indicating that the request is denied.
- Contacts the requestor and asks for more information.

## Review

If the request uses the Multi-Approval or Parallel-Approval workflow, then its lifecycle includes a Review stage, in which a controller reviews the change request. This stage consists of the following steps:

1. The controller examines the change request.
2. The controller then composes an email message in FireFlow, notifying the requestor that the change request was reviewed and approved for implementation.



To: "AlgoSec Administrator" <admin@company.com> (admin)

Cc: *(comma-delimited list of email addresses)*

Bcc: *(comma-delimited list of email addresses)*

Subject: Drop traffic

Message: Your request has been approved and reviewed

Attach: No file chosen

3. FireFlow sends the email to the requestor.
4. The change request is sent on to the next stage.

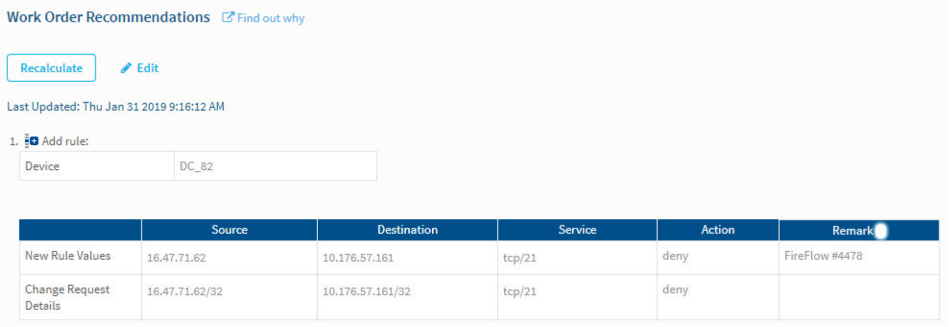
## Implement

In the Implement stage, the network operations user plans and executes request implementation.

This stage consists of the following steps:

1. The change request's ownership is returned to the network operations user.
2. FireFlow creates a work order and displays a list of recommendations for

implementing the requested change.



Work Order Recommendations

Last Updated: Thu Jan 31 2019 9:16:12 AM

1. Add rule:

| | |
|---|---|
| Device | DC_82 |

| | Source | Destination | Service | Action | Remark |
|---|---|---|---|---|---|
| New Rule Values | 16.47.71.62 | 10.176.57.161 | tcp/21 | deny | FireFlow #4478 |
| Change Request Details | 16.47.71.62/32 | 10.176.57.161/32 | tcp/21 | deny | |

3. The network operations user can edit the work order.

   For most devices, the user can edit the list of recommendations. For all devices, the user can add notes to the work order, to be viewed by the implementing team.

4. The network operations user implements the requested changes on the security device according to the work order, by doing one of the following:

   - The user manually implements the changes or implements the changes using the relevant management system (for example, Check Point Dashboard or Juniper NSM).
   - The user implements the changes from FireFlow using ActiveChange.

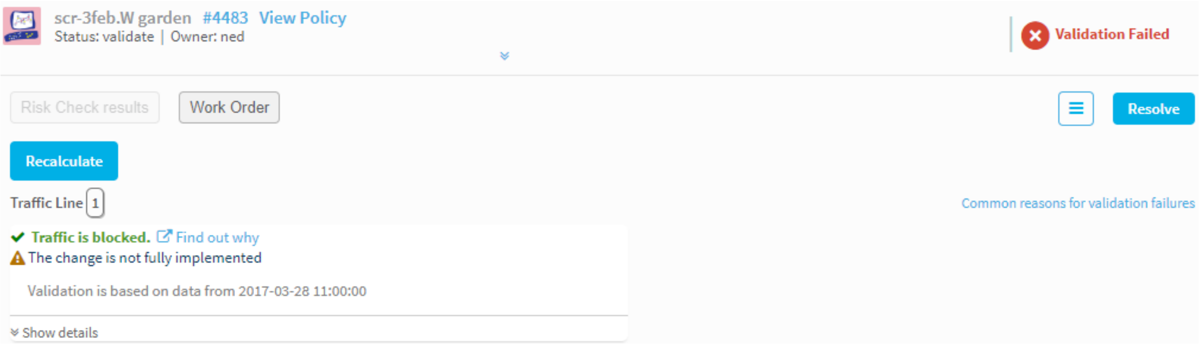
   > **Note:** In order to use ActiveChange, it must be licensed and enabled. For more details, see Implement changes with ActiveChange.

5. The network operation user sends the change request on to the next stage.

## Validate

In the Validate stage, FireFlow validates the implemented device policy changes against the change request and presents validation results to the network operation user. The requestor then checks that the request was implemented, and the network operations user resolves the change request. This stage consists of the following steps:

1. FireFlow validates the implemented device policy changes against the change request.



scr-3feb.W garden #4483

Status: validate | Owner: ned

Validation Failed

Traffic Line 1

✓ Traffic is blocked.

⚠ The change is not fully implemented

Validation is based on data from 2017-03-28 11:00:00

2. The validation process checks both that the requested traffic is not allowed or blocked, and also that the changes were done according to the work order.
3. If validation indicates that the implemented changes did *not* achieve the desired result specified in the change request, then the network operations user re-initiates the Implement stage.
4. For the Standard, Multi-Approval, or Parallel-Approval workflows:

   Once the changes have been successfully validated, the network operations user composes an email message in FireFlow, notifying the requestor that the requested changes were implemented.
5. FireFlow sends the email to the requestor.
6. The requestor checks that the requested change was implemented and the desired result was achieved.
7. One of the following happens:
   - If the desired result was not achieved, the requestor responds via an email message or via the Web interface, and the network operations user then re-initiates the implementation stage.

- If the desired result was achieved, the requestor responds via an email message or via the Web interface, and the change request is resolved automatically.
- If the requestor does not respond, the network operations user can choose to resolve the change request anyway.

At this point, the change request's lifecycle has effectively ended, and no further user action is required. However, the change request remains available in the system for auditing purposes, as described in the final stages.

## Match

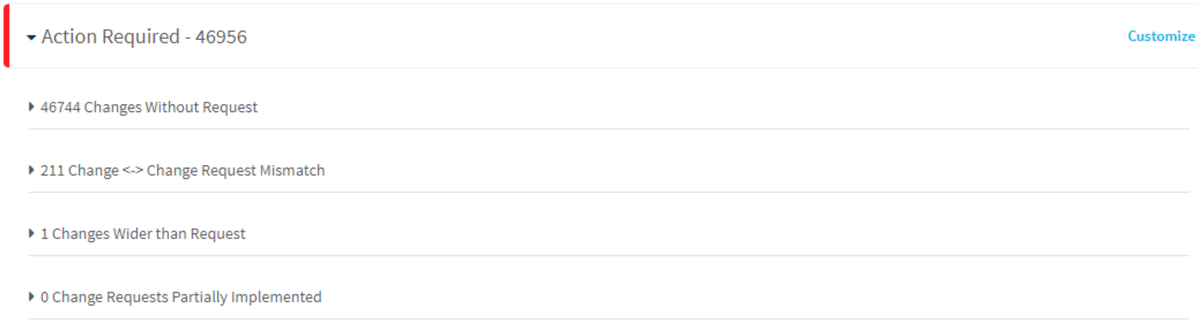
According to a configurable schedule, FireFlow automatically checks all devices for rule changes and determines the following:

- Each change is associated with a change request.
- Each change request is associated with a change.
- Each change is associated with the *correct* change request.
- The scope of each change matches the approved scope in the associated change request.

If there are no problems with a given change request, FireFlow automatically marks it as matched.

For control purposes, an information security user periodically checks that all change requests were matched successfully, and resolves any problems that FireFlow may have detected during auto matching. The Match stage consists of the following steps:

1. The information security user checks whether FireFlow detected any matching problems with the validated change requests in the system.



▾ Action Required - 46956

▸ 46744 Changes Without Request

▸ 211 Change <-> Change Request Mismatch

▸ 1 Changes Wider than Request

▸ 0 Change Requests Partially Implemented

2. If a problem is detected for a change request, the information security user does one of the following:

   - Re-opens the change request.
   - Manually approves the mismatch.

> **Note:** It is recommended to perform these steps on a weekly or monthly basis.

## Resolved

Once the change request has been matched to the relevant change(s), it enters the Resolved stage.

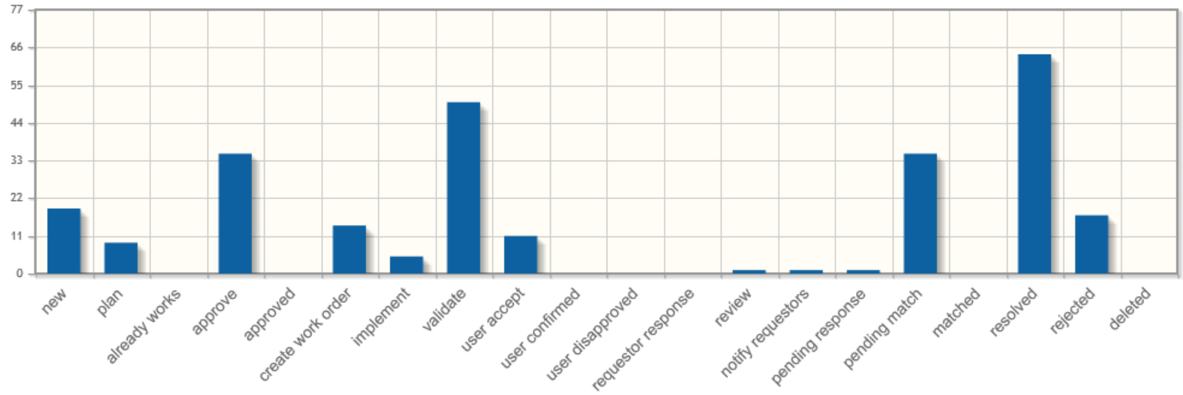
## Audit

FireFlow enables you to perform a variety of auditing tasks, including:

- Viewing the full history of any change request, including who requested the change, who approved the change request, what device rule changes were implemented, and comments on the change request.
- Searching and filtering according to dates, requestor, device, and other criteria.
- Generating a variety of reports, including reports based on:
- Change request owner
- Change request status
- Create, due, update, or resolve date, for a daily, monthly, or annual period

- Specific fields in the request
- SLA parameters

Reports can be viewed in FireFlow or exported to a .csv file (that can be viewed in Excel, for example).



# IPv6 traffic change workflow

This topic describes the events that occur in each stage in a default iPv6 traffic change workflow.

This type of traffic change is supported only for Cisco devices.

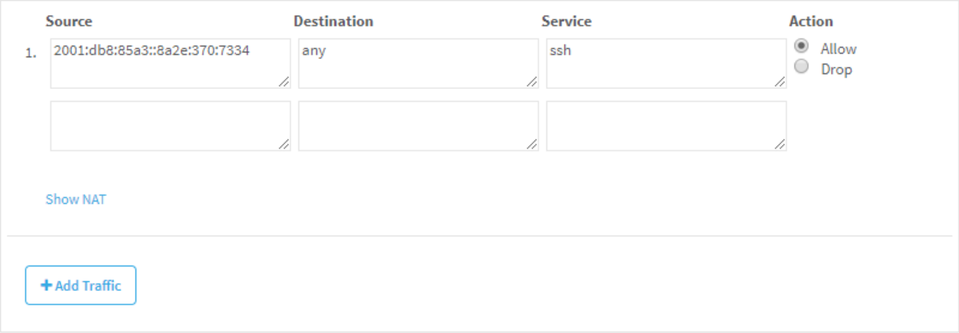
**Note:** FireFlow is fully configurable, and your system may differ.

## Request

In the Request stage, a requestor submits a request for an IPv6 traffic change, initiating the FireFlow change request lifecycle. This stage consists of the following steps:

1. The requestor selects a template on which to base their request.
2. If the template specifies a workflow, FireFlow assigns the request to that workflow.
3. The requestor submits the request to FireFlow.

The request may include information about the relevant source, destination, service, and action for the change. For example, the requestor may submit the following request:



|  | Source | Destination | Service | Action |
|---|---|---|---|---|
| 1. | 2001:db8:85a3::8a2e:370:7334 | any | ssh | ● Allow<br>○ Drop |
|  |  |  |  |  |

4. FireFlow receives the request information and creates a *change request*.
5. If a workflow has not yet been assigned, FireFlow assigns a workflow. For more details, see Request templates and workflows.
6. The *default assignee* of the role handling new change requests (by default, the Network Operations role) is assigned as the change request's *owner*.
7. FireFlow sends an email message informing the requestor that the change request was created, and specifying the change request ID in the format [FireFlow #<*number*>], for example [FireFlow #49].

## Plan

In the Plan stage, a user with a network operations role plots out the technical changes needed in order to satisfy the change request. This stage consists of the following steps:

1. The change request may change ownership in one of the following ways:
    - The change request owner assigns it to a user with the network operations role.
    - A network operations user chooses to take responsibility for the change request.
2. The network operations user confirms the devices that are relevant to the requested change.
3. The network operation user sends the change request on to the next stage.

4. If the network operations user selected multiple devices, FireFlow generates a sub-request for each.

## Approve

In the Approve stage, a user with the information security role determines the security risks entailed in satisfying the request. This stage consists of the following steps:

1. The *default assignee* of the role handling change requests in the Approve stage (by default, the Information Security role) is assigned as the change request's owner.
2. The change request may change ownership in one of the following ways:
   - The change request owner assigns it to a user with information security role.
   - An information security user chooses to take responsibility for the change request.
3. The information security user does one of the following:
   - Approves the change request and sends it on to the next stage.
   - Rejects the change request and returns it to the Plan stage.
   - Rejects and closes the change request. In this case, an email message is sent to the requestor, indicating that the request is denied.
   - Contacts the requestor and asks for more information.

## Implement

In the Implement stage, the network operations user plans and executes request implementation.

This stage consists of the following steps:

1. The change request's ownership is returned to the network operations user.
2. FireFlow creates a work order and displays a list of recommendations for implementing the requested change.

3. The network operations user edits the list of recommendations and adds notes to the work order.
4. The network operations user manually implements the requested changes on the devices according to the work order.
5. The network operation user sends the change request on to the next stage.

## Validate

In the Validate stage, the requestor checks that the request was implemented, and the network operations user resolves the change request. This stage consists of the following steps:

1. The network operations user composes an email message in FireFlow, notifying the requestor that the requested changes were implemented.
2. FireFlow sends the email to the requestor.
3. The requestor checks that the requested change was implemented and the desired result was achieved.
4. One of the following things happens:
   - If the desired result was not achieved, the requestor responds via an email message or via the Web interface, and the network operations user then re-initiates the implementation stage.
   - If the desired result was achieved, the requestor responds via email message or via the Web interface, and the network operations user then resolves the change request.
   - If the requestor does not respond, the network operations user can choose to resolve the change request anyway.

At this point, the change request's lifecycle has effectively ended, and no further user action is required. However, the change request remains available in the system for auditing purposes, as described in the final stages.

### Resolved

Once the change request has been validated, it enters the Resolved stage.

### Audit

The Audit stage for IPv6 traffic change request lifecycles is identical to the Audit stage for traffic change request lifecycles. See Audit.

## Multicast traffic change workflow

This topic describes the events that occur in each stage in a default Multicast traffic change workflow.

This type of traffic change is supported only for Cisco devices.

**Note:** FireFlow is fully configurable, and your system may differ.

### Request

In the Request stage, a requestor submits a request for a device multicast traffic change, initiating the FireFlow change request lifecycle. This stage consists of the following steps:

1. The requestor selects a template on which to base their request.
2. If the template specifies a workflow, FireFlow assigns the request to that workflow.
3. The requestor submits the request to FireFlow.

   The request may include information about the relevant source, destination, service, and action for the change. For example, the requestor may submit the following request.
4. FireFlow receives the request information and creates a *change request*.
5. If a workflow has not yet been assigned, FireFlow assigns a workflow. For more details, see Request templates and workflows.

6. The *default assignee* of the role handling new change requests (by default, the Network Operations role) is assigned as the change request's *owner*.
7. FireFlow sends an email message informing the requestor that the change request was created, and specifying the change request ID in the format [FireFlow #<*number*>], for example [FireFlow #49].

## Plan

In the Plan stage, a user with the network operations role plots out the technical changes needed in order to satisfy the change request. This stage consists of the following steps:

1. The change request may change ownership in one of the following ways:
   - The change request owner assigns it to a user with the network operations role.
   - A network operations user chooses to take responsibility for the change request.
2. The network operations user chooses or confirms the already chosen devices that are relevant to the requested change.
3. The network operation user sends the change request on to the next stage.
4. FireFlow will generate a separate change request for each device or policy to be modified.

## Approve

In the Approve stage, a user with the information security role determines the security risks entailed in satisfying the request. This stage consists of the following steps:

1. The *default assignee* of the role handling change requests in the Approve stage (by default, the Information Security role) is assigned as the change request's owner.
2. The change request may change ownership in one of the following ways:
   - The change request owner assigns it to a user with the information security role.

- An information security user chooses to take responsibility for the change request.

3. The information security user does one of the following:
   - Approves the change request and sends it on to the next stage.
   - Rejects the change request and returns it to the Plan stage.
   - Rejects and closes the change request. In this case, an email message is sent to the requestor, indicating that the request is denied.
   - Contacts the requestor and asks for more information.

## Implement

In the Implement stage, the network operations user plans and executes request implementation.

This stage consists of the following steps:

1. The change request's ownership is returned to the network operations user.
2. FireFlow creates a work order and displays a list of recommendations for implementing the requested change.
3. The network operations user edits the list of recommendations and adds notes to the work order.

   For multicast traffic requests, the user must edit the work order to choose the relevant ACLs and rule locations for the CLI commands to be generated.

4. The network operations user manually implements the requested changes on the device according to the work order.
5. The network operation user sends the change request on to the next stage.

## Validate

In the Validate stage, the requestor checks that the request was implemented, and the network operations user resolves the change request. This stage consists of the following steps:

1. The network operations user composes an email message in FireFlow, notifying the requestor that the requested changes were implemented.
2. FireFlow sends the email to the requestor.
3. The requestor checks that the requested change was implemented and the desired result was achieved.
4. One of the following things happens:
   - If the desired result was not achieved, the requestor responds via an email message or via the Web interface, and the network operations user then re-initiates the implementation stage.
   - If the desired result was achieved, the requestor responds via an email message or via the Web interface, and the network operations user then resolves the change request.
   - If the requestor does not respond, the network operations user can choose to resolve the change request anyway.

At this point, the change request's lifecycle has effectively ended, and no further user action is required. However, the change request remains available in the system for auditing purposes, as described in the final stages.

### Resolved

Once the change request has been validated, it enters the Resolved stage.

### Audit

The Audit stage for Multicast traffic change request lifecycles is identical to the Audit stage for traffic change request lifecycles. See Audit (see Audit).

## Re-certification workflow

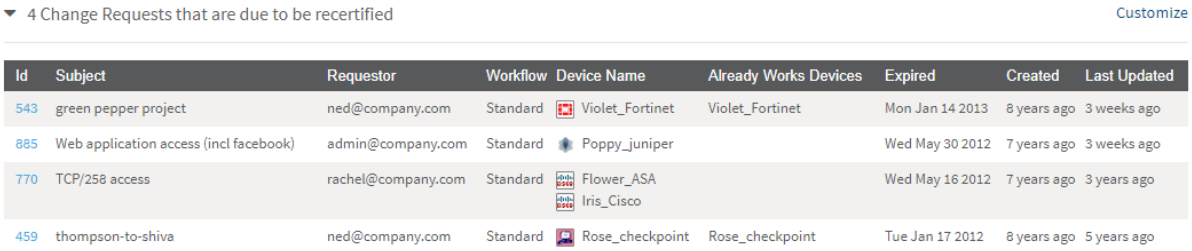
This topic describes the events that occur in each stage in a default re-certification change.

**Note:** FireFlow is fully configurable, and your system may differ.

## Request

In the Request stage, a network operations user submits a request to recertify an expired traffic change request, initiating the FireFlow change request lifecycle. This stage consists of the following steps:

1. The network operations user views a list of change requests that are due to be recertified.



4 Change Requests that are due to be recertified

| Id | Subject | Requestor | Workflow | Device Name | Already Works Devices | Expired | Created | Last Updated |
|---|---|---|---|---|---|---|---|---|
| 543 | green pepper project | ned@company.com | Standard | Violet_Fortinet | Violet_Fortinet | Mon Jan 14 2013 | 8 years ago | 3 weeks ago |
| 885 | Web application access (incl facebook) | admin@company.com | Standard | Poppy_juniper |  | Wed May 30 2012 | 7 years ago | 3 weeks ago |
| 770 | TCP/258 access | rachel@company.com | Standard | Flower_ASA<br>Iris_Cisco |  | Wed May 16 2012 | 7 years ago | 3 years ago |
| 459 | thompson-to-shiva | ned@company.com | Standard | Rose_checkpoint | Rose_checkpoint | Tue Jan 17 2012 | 8 years ago | 5 years ago |

2. The network operations user then selects the change request to recertify.

   **Note:** It is possible to select multiple change requests to recertify.

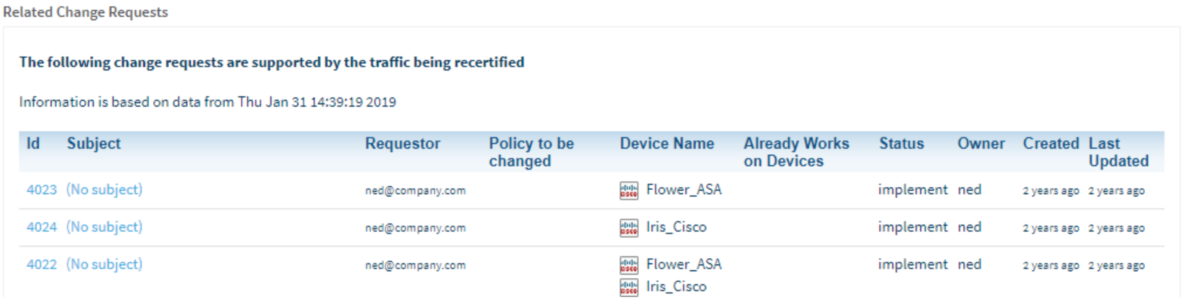
3. FireFlow creates a *change request* and assigns the request to the Request-Recertification workflow.
4. The *default assignee* of the role handling new change requests (by default, the Network Operations role) is assigned as the change request's *owner*.

## Certify

In the Certify stage, the network operations user determines the network issues entailed in satisfying the request. This stage consists of the following steps:

1. The change request may change ownership in one of the following ways:
    - The change request owner assigns it to a user with the network operations role.
    - A network operations user chooses to take responsibility for the change request.
2. The network operations user initiates a search for change requests whose traffic intersects that of the Allow traffic that was added by the expired change request.

    FireFlow returns a list of related change requests:

    Related Change Requests

    **The following change requests are supported by the traffic being recertified**

    Information is based on data from Thu Jan 31 14:39:19 2019

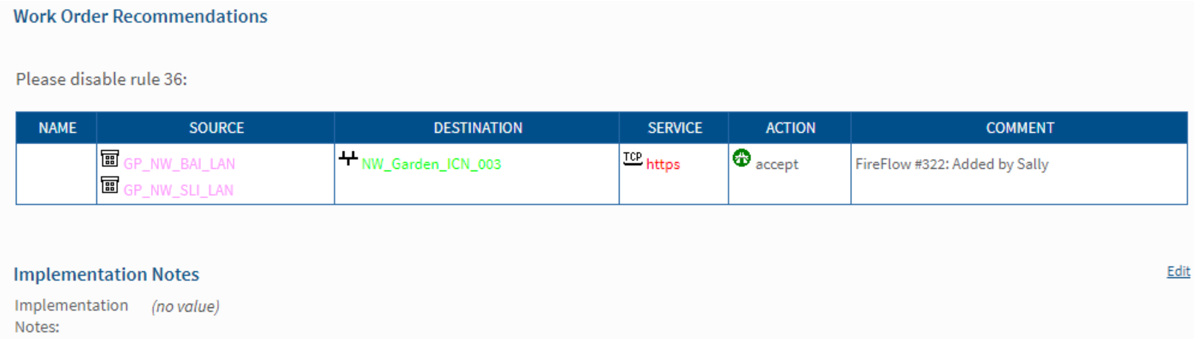
    | Id | Subject | Requestor | Policy to be changed | Device Name | Already Works on Devices | Status | Owner | Created | Last Updated |
    |---|---|---|---|---|---|---|---|---|---|
    | 4023 | (No subject) | ned@company.com | | Flower_ASA | | implement | ned | 2 years ago | 2 years ago |
    | 4024 | (No subject) | ned@company.com | | Iris_Cisco | | implement | ned | 2 years ago | 2 years ago |
    | 4022 | (No subject) | ned@company.com | | Flower_ASA<br>Iris_Cisco | | implement | ned | 2 years ago | 2 years ago |

3. The network operations user then specifies which of the related change requestors (and optionally other users) should receive a notification that the Allow traffic will be deleted.
4. FireFlow sends an email to the selected requestors.
5. The requestors respond via email message.
6. The network operations user does one of the following:
    - Extends the due date of the change request, giving related change requestors more time to respond.
    - Certifies the traffic, sending the change request on to the Resolved stage.
    - Plans the traffic's removal, sending the change request on to the next stage.

## Implement

In the Implement stage, the network operations user plans and executes request implementation. This stage consists of the following steps:

1. FireFlow creates a work order and displays a list of recommendations for implementing the requested change.



Work Order Recommendations

Please disable rule 36:

| NAME | SOURCE | DESTINATION | SERVICE | ACTION | COMMENT |
|---|---|---|---|---|---|
| | GP_NW_BAI_LAN<br>GP_NW_SLI_LAN | NW_Garden_ICN_003 | TCP https | accept | FireFlow #322: Added by Sally |

Implementation Notes

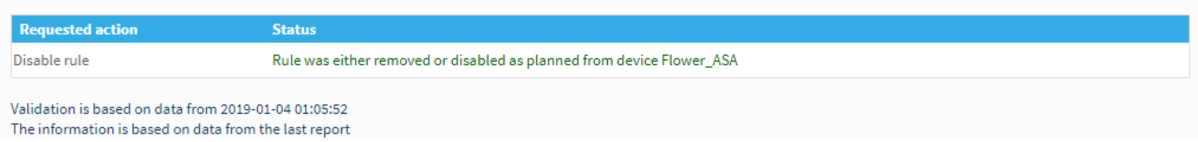
Implementation Notes: *(no value)*

2. The network operations user edits the work order, by adding notes to the work order.
3. The network operations user implements the requested changes on the device or policy according to the work order, by using the relevant management system (for example, Check Point Dashboard or Juniper NSM) to implement the changes.
4. The network operation user sends the change request on to the next stage.

## Validate

In the Validate stage, the network operation user validates the implemented removal of the Allow traffic against the recertification request. This stage consists of the following steps:

1. The network operations user validates the implemented Allow traffic removal against the change request.



| Requested action | Status |
|---|---|
| Disable rule | Rule was either removed or disabled as planned from device Flower_ASA |

Validation is based on data from 2019-01-04 01:05:52
The information is based on data from the last report

2. If validation indicates that the traffic is still allowed, then the network operations user re-initiates the Implement stage.
3. Once the Allow traffic's removal has been successfully validated, the network operations user resolves the change request.

At this point, the change request's lifecycle has effectively ended, and no further user action is required. However, the change request remains available in the system for auditing purposes, as described in the final stages.

### Resolved

Once the Allow traffic has been certified or the recertification request has been validated, the change request enters the Resolved stage.

### Audit

The Audit stage for rule removal request lifecycles is identical to the Audit stage for traffic change request lifecycles. See Audit (see Audit).

## Object change workflow

This topic describes the events that occur in each stage in a default object change workflow.

> **Note:** FireFlow is fully configurable, and your system may differ.

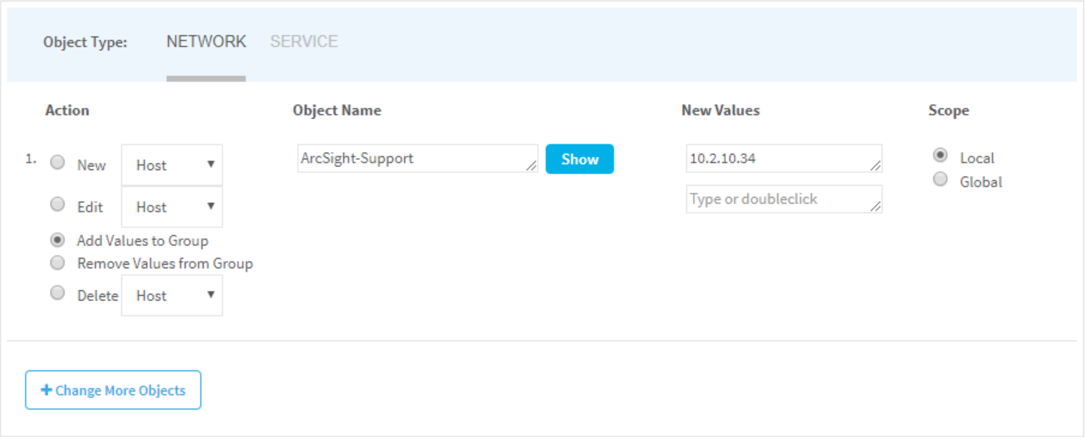
### Request

In the Request stage, a privileged user submits a request for a device object change, initiating the FireFlow change request lifecycle. This stage consists of the following steps:

1. The requesting privileged user selects a template on which to base their request.
2. If the template specifies a workflow, FireFlow assigns the request to that workflow.
3. The requesting privileged user submits the request to FireFlow.

   The request includes information about a device object to create, delete, or modify.

   For example, the requesting privileged user may submit the following request:



Object Type: NETWORK SERVICE

| | Action | | Object Name | | New Values | Scope |
|---|---|---|---|---|---|---|
| 1. | ○ New | Host ▾ | ArcSight-Support | Show | 10.2.10.34 | ● Local |
| | ○ Edit | Host ▾ | | | Type or doubleclick | ○ Global |
| | ● Add Values to Group | | | | | |
| | ○ Remove Values from Group | | | | | |
| | ○ Delete | Host ▾ | | | | |

+ Change More Objects

> **Note:** Check Point devices have a more extensive list of possible actions.

4. FireFlow receives the request information and creates a *change request*.
5. If a workflow has not yet been assigned, FireFlow assigns a workflow. For more details, see Request templates and workflows.
6. The *default assignee* of the role handling new change requests (by default, the Network Operations role) is assigned as the change request's *owner*.
7. FireFlow sends an email message informing the requesting privileged user that the change request was created, and specifying the change request ID in the format [FireFlow #<*number*>], for example [FireFlow #49].

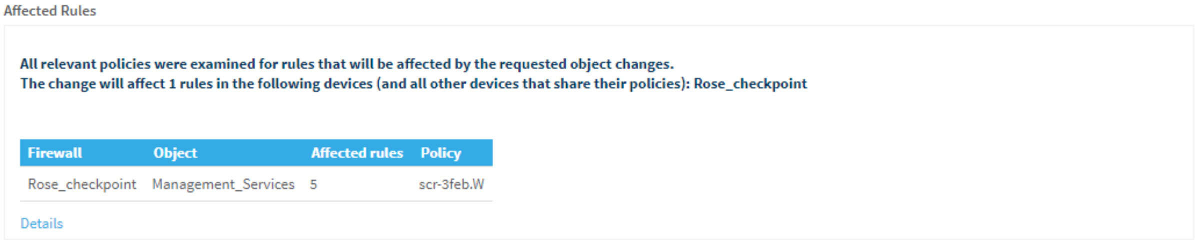
## Plan

In the Plan stage, a user with the network operations role plots out the technical changes needed in order to satisfy the change request. This stage consists of the following steps:

1. The change request may change ownership in one of the following ways:
   - The change request owner assigns it to a user with network operations role.
   - A network operations user chooses to take responsibility for the change request.
2. FireFlow initiates a search for rules that would be affected by the requested object

change.

FireFlow returns a list of affected rules:



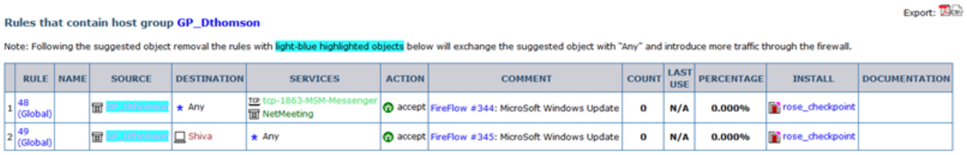
Affected Rules

All relevant policies were examined for rules that will be affected by the requested object changes.
The change will affect 1 rules in the following devices (and all other devices that share their policies): Rose_checkpoint

| Firewall | Object | Affected rules | Policy |
|---|---|---|---|
| Rose_checkpoint | Management_Services | 5 | scr-3feb.W |

Details

You can view details by clicking the details link:



Export:

Rules that contain host group GP_Dthomson

Note: Following the suggested object removal the rules with light-blue highlighted objects below will exchange the suggested object with "Any" and introduce more traffic through the firewall.

| | RULE | NAME | SOURCE | DESTINATION | SERVICES | ACTION | COMMENT | COUNT | LAST USE | PERCENTAGE | INSTALL | DOCUMENTATION |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 48 (Global) | | GP_Dthomson | ★ Any | tcp-1863-MSM-Messenger<br>NetMeeting | accept | FireFlow #344: MicroSoft Windows Update | 0 | N/A | 0.000% | rose_checkpoint | |
| 2 | 49 (Global) | | GP_Dthomson | Shiva | ★ Any | accept | FireFlow #345: MicroSoft Windows Update | 0 | N/A | 0.000% | rose_checkpoint | |

## Approve

The Approve stage consists of the following steps:

1. The *default assignee* of the role handling change requests in the Approve stage (by default, the Information Security role) is assigned as the change request's owner.
2. The change request may change ownership in one of the following ways:
   - The change request owner assigns it to a user with the information security role.
   - An information security user chooses to take responsibility for the change request.
3. The information security user does one of the following:
   - Approves the change request and sends it on to the next stage.
   - Rejects the change request. In this case the change request returns to the start of the Approve stage.
   - Rejects and closes the change request. In this case, an email message is sent

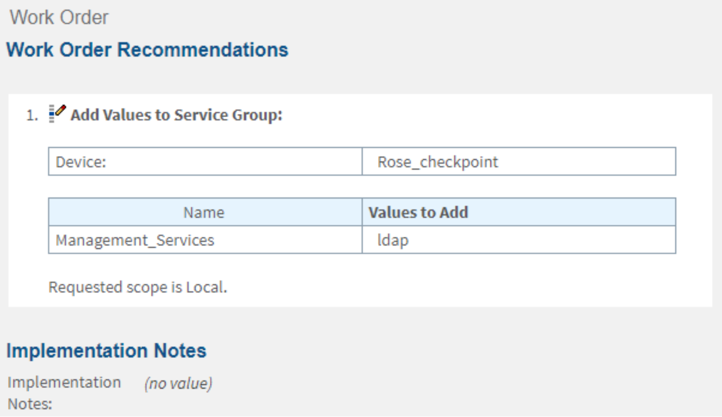
to the requesting privileged user, indicating that the request is denied.

- Contacts the requestor and asks for more information.

## Implement

In the Implement stage, the network operations user plans and executes request implementation. This stage consists of the following steps:

1. The change request's ownership is returned to the network operations user.
2. FireFlow creates a work order and displays a list of recommendations for implementing the requested change.



Work Order

**Work Order Recommendations**

1. **Add Values to Service Group:**

| | |
|---|---|
| Device: | Rose_checkpoint |

| Name | Values to Add |
|---|---|
| Management_Services | ldap |

Requested scope is Local.

**Implementation Notes**

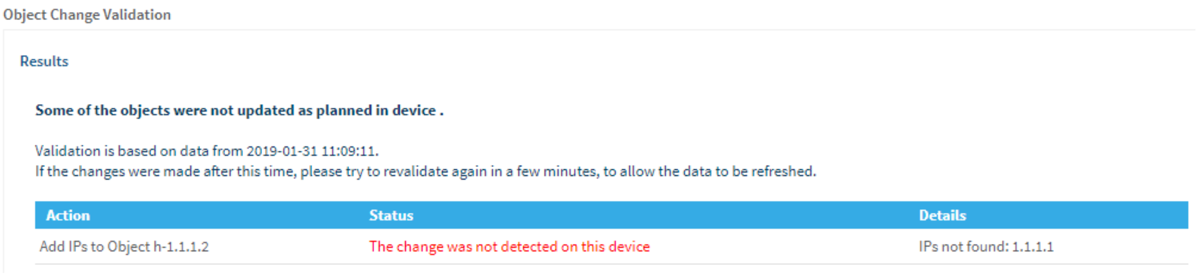
Implementation Notes: *(no value)*

3. The network operations user edits the work order, by adding notes to the work order.
4. The network operations user implements the requested changes on the security device according to the work order, by using the relevant management system (for example, Check Point Dashboard or Juniper NSM) to implement the changes.
5. The network operation user sends the change request on to the next stage.

## Validate

In the Validate stage, the network operation user validates the implemented device object changes against the change request. This stage consists of the following steps:

1. The network operations user validates the implemented device policy changes against the change request.



Object Change Validation

Results

**Some of the objects were not updated as planned in device .**

Validation is based on data from 2019-01-31 11:09:11.
If the changes were made after this time, please try to revalidate again in a few minutes, to allow the data to be refreshed.

| Action | Status | Details |
|---|---|---|
| Add IPs to Object h-1.1.1.2 | The change was not detected on this device | IPs not found: 1.1.1.1 |

2. If validation indicates that the implemented changes did *not* achieve the desired result specified in the change request, then the network operations user re-initiates the Implement stage.
3. The network operations user composes an email message in FireFlow, notifying the requestor that the requested changes were implemented.
4. FireFlow sends the email to the requesting privileged user.
5. The network operations user resolves the change request.

At this point, the change request's lifecycle has effectively ended, and no further user action is required. However, the change request remains available in the system for auditing purposes, as described in the final stages.

## Resolved

Once the change request has been validated, it enters the Resolved stage.

## Audit

The Audit stage for object change request lifecycles is identical to the Audit stage for traffic change request lifecycles. See Audit (see Audit).

# Multi-device object change workflow

This topic describes the events that occur in each stage in a default multi-device object change workflow.

**Note:** FireFlow is fully configurable, and your system may differ.

## Request

In the **Request** stage, a privileged user submits a request for a multi-device object change, initiating the FireFlow change request lifecycle.

> **Note:** A multi -device object change request cannot be created in the Web Interface. It can only be created with the FireFlow REST API.
>
> If licensed, AppChange, layered over AppViz can also initiate these change requests when editing an object. This option depends on your AppViz configuration.

This stage consists of the following steps:

1. The requesting privileged user initiates the request via a REST call, directly or from AppViz.

   The request includes information about a device object to create, delete, or modify.
2. FireFlow receives the request information and creates a *change request*.
3. The *default assignee* of the role handling new change requests (by default, the Network Operations role) is assigned as the change request's *owner*.
4. FireFlow sends an email message informing the requesting privileged user that the change request was created, and specifying the change request ID in the format **[FireFlow #<*number*>]**, for example **[FireFlow #49]**.

The change request ID number additionally appears in the response of the REST call.

## Plan

Multi device object change requests automatically continue through the plan stage to the approve stage.

## Approve

The Approve stage consists of the following steps:

1. The *default assignee* of the role handling change requests in the Approve stage (by default, the Information Security role) is assigned as the change request's owner.
2. The change request may change ownership in one of the following ways:
   - The change request owner assigns it to a user with the information security role.
   - An information security user chooses to take responsibility for the change request.
3. FireFlow initiates a search for rules that would be affected by the requested object change.

   FireFlow returns a list of affected rules:
4. The information security user does one of the following:
   - Approves the change request and sends it on to the next stage.
   - Rejects the change request. In this case the change request returns to the start of the Approve stage.
   - Rejects and closes the change request. In this case, an email message is sent to the requesting privileged user, indicating that the request is denied.
   - Contacts the requestor and asks for more information.

## Implement

The Implement stage for multi-device object change requests is similar to that of single-device object change requests, with the addition of ActiveChange support, depending on the device type.

For more details, see Implement changes with ActiveChange and the AlgoSec support matrix.

## Validate

In the Validate stage, the network operation user validates the implemented device object changes against the change request. This stage consists of the following steps:

1. The network operations user validates the implemented device policy changes against the change request.
2. If validation indicates that the implemented changes did *not* achieve the desired result specified in the change request, then the network operations user re-initiates the Implement stage.
3. The network operations user composes an email message in FireFlow, notifying the requestor that the requested changes were implemented.
4. FireFlow sends the email to the requesting privileged user.
5. The network operations user resolves the change request.

At this point, the change request's lifecycle has effectively ended, and no further user action is required. However, the change request remains available in the system for auditing purposes, as described in the final stages.

### Resolved

Once the change request has been validated, it enters the Resolved stage.

### Audit

The Audit stage for object change request lifecycles is identical to the Audit stage for traffic change request lifecycles. See Audit (see Audit).

## Rule removal workflow

This topic describes the events that occur in each stage in a default rule removal change workflow.

> **Note:** FireFlow is fully configurable, and your system may differ.

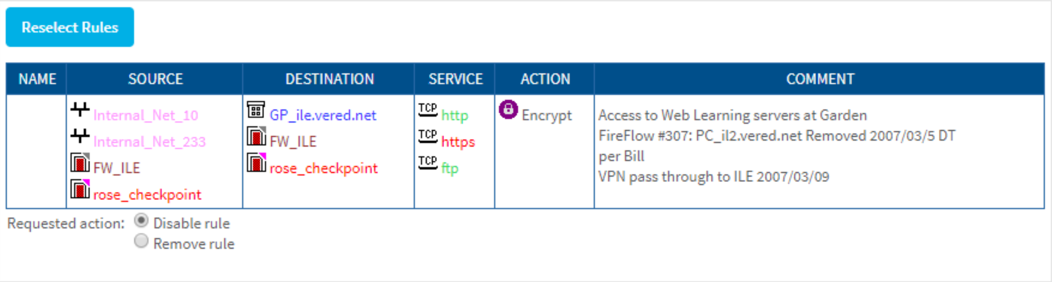
### Request

In the Request stage, a privileged user submits a request to remove or disable one or more device rules, initiating the FireFlow change request lifecycle.

This stage consists of the following steps:

1. The requesting privileged user selects a template on which to base their request.
2. If the template specifies a workflow, FireFlow assigns the request to that workflow.
3. The requesting privileged user submits the request to FireFlow.

   The request includes information about one or more device rules to remove or disable. For example, the requestor may submit the following request:

   | NAME | SOURCE | DESTINATION | SERVICE | ACTION | COMMENT |
   |---|---|---|---|---|---|
   | | Internal_Net_10<br>Internal_Net_233<br>FW_ILE<br>rose_checkpoint | GP_ile.vered.net<br>FW_ILE<br>rose_checkpoint | TCP http<br>TCP https<br>TCP ftp | Encrypt | Access to Web Learning servers at Garden<br>FireFlow #307: PC_il2.vered.net Removed 2007/03/5 DT per Bill<br>VPN pass through to ILE 2007/03/09 |

   Requested action: ● Disable rule  
   ○ Remove rule

4. FireFlow receives the request information and creates a *change request*.
5. If a workflow has not yet been assigned, FireFlow assigns a workflow. For more details, see Request templates and workflows.
6. The *default assignee* of the role handling new change requests (by default, the Network Operations role) is assigned as the change request's *owner*.
7. FireFlow sends an email message informing the requesting privileged user that the change request was created, and specifying the change request ID in the format [FireFlow #<*number*>], for example [FireFlow #49].

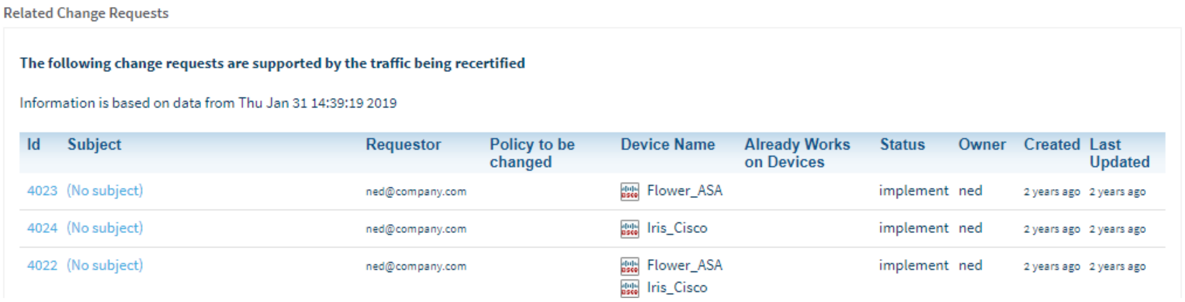
## Approve

In the Approve stage, the network operations user determines the network issues entailed in satisfying the request. This stage consists of the following steps:

1. The change request may change ownership in one of the following ways:
   - The change request owner assigns it to a user with the network operations role.
   - A network operations user chooses to take responsibility for the change request.
2. The network operations user initiates a search for change requests whose traffic

intersects that of the selected device rule.

FireFlow returns a list of related change requests:



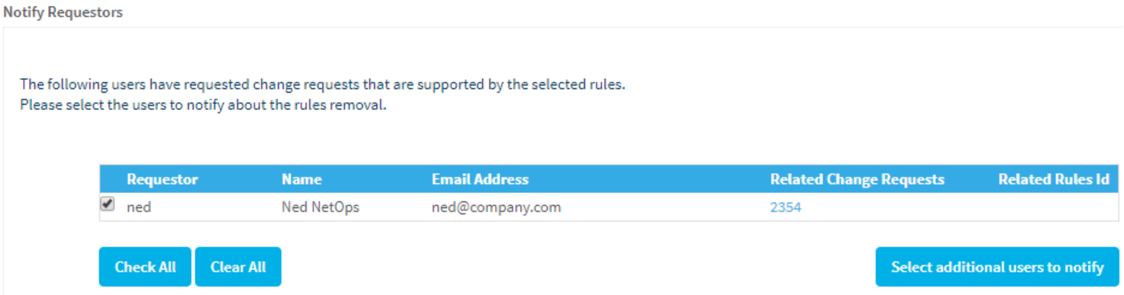
Related Change Requests

**The following change requests are supported by the traffic being recertified**

Information is based on data from Thu Jan 31 14:39:19 2019

| Id | Subject | Requestor | Policy to be changed | Device Name | Already Works on Devices | Status | Owner | Created | Last Updated |
|---|---|---|---|---|---|---|---|---|---|
| 4023 | (No subject) | ned@company.com | | Flower_ASA | | implement | ned | 2 years ago | 2 years ago |
| 4024 | (No subject) | ned@company.com | | Iris_Cisco | | implement | ned | 2 years ago | 2 years ago |
| 4022 | (No subject) | ned@company.com | | Flower_ASA<br>Iris_Cisco | | implement | ned | 2 years ago | 2 years ago |

3. The network operations user then specifies which of the related change requestors (and optionally other users) should receive a notification that the rule will be deleted.



Notify Requestors

The following users have requested change requests that are supported by the selected rules.
Please select the users to notify about the rules removal.

| | Requestor | Name | Email Address | Related Change Requests | Related Rules Id |
|---|---|---|---|---|---|
| ☑ | ned | Ned NetOps | ned@company.com | 2354 | |

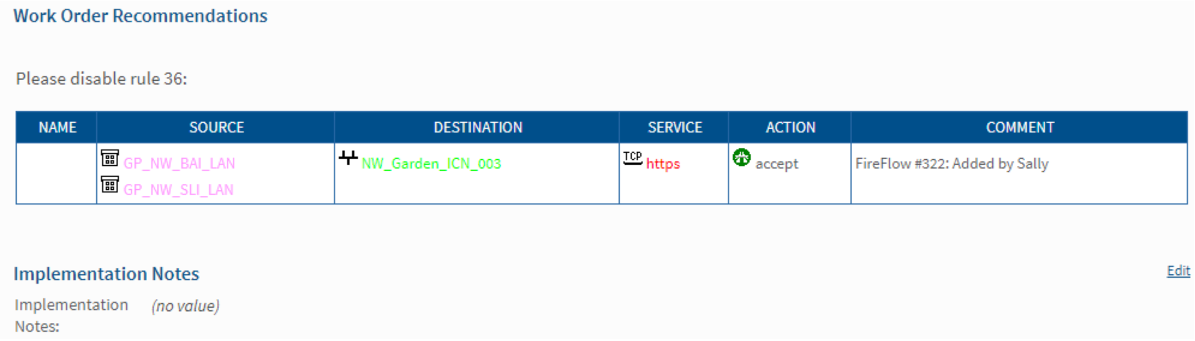
4. FireFlow sends an email to the selected requestors.
5. The requestors respond via an email message or the web interface.
6. The network operations user does one of the following:
   - Approves the change request and sends it on to the next stage.
   - Rejects and closes the change request. In this case, an email message is sent to the requesting privileged user, indicating that the request is denied.
   - Contacts the requestor and asks for more information.
   - Extends the due date of the change request, giving users more time to respond.

## Implement

In the Implement stage, the network operations user plans and executes request implementation.

This stage consists of the following steps:

1. FireFlow creates a work order and displays a list of recommendations for implementing the requested change.



**Work Order Recommendations**

Please disable rule 36:

| NAME | SOURCE | DESTINATION | SERVICE | ACTION | COMMENT |
|---|---|---|---|---|---|
| | GP_NW_BAI_LAN<br>GP_NW_SLI_LAN | NW_Garden_ICN_003 | TCP https | accept | FireFlow #322: Added by Sally |

**Implementation Notes**

Implementation Notes: *(no value)*

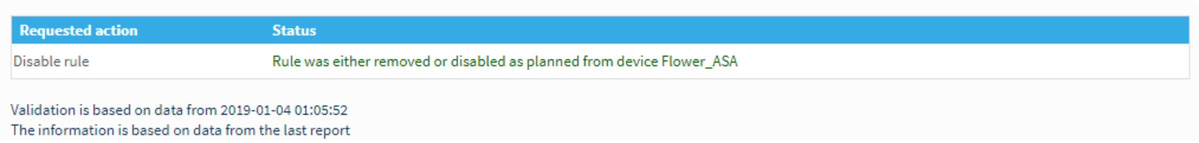
2. The network operations user edits the work order, by adding notes to the work order.
3. The network operations user implements the requested changes on the security device according to the work order, by doing one of the following:
   - The user manually implements the changes or implements the changes using the relevant management system (for example, Check Point Dashboard or Juniper NSM).
   - The user implements the changes from FireFlow using ActiveChange.

     **Note:** In order to use ActiveChange, it must be licensed and enabled. For more details, see Implement changes with ActiveChange.
4. The network operation user sends the change request on to the next stage.

## Validate

In the Validate stage, the network operation user validates the implemented rule removal/disablement against the change request. This stage consists of the following steps:

1. The network operations user validates the implemented rule removal/disablement against the change request.



| Requested action | Status |
|---|---|
| Disable rule | Rule was either removed or disabled as planned from device Flower_ASA |

Validation is based on data from 2019-01-04 01:05:52
The information is based on data from the last report

2. If validation indicates that the specified rule was not removed/disabled, then the network operations user re-initiates the Implement stage.
3. Once the rule removal/disablement has been successfully validated, the network operations user resolves the change request.

At this point, the change request's lifecycle has effectively ended, and no further user action is required. However, the change request remains available in the system for auditing purposes, as described in the final stages.

### Resolved

Once the change request has been validated, it enters the Resolved stage.

### Audit

The Audit stage for rule removal request lifecycles is identical to the Audit stage for traffic change request lifecycles. See Audit (see Audit).

## Rule modification workflow

This topic describes the events that occur in each stage in a default rule modification change workflow.

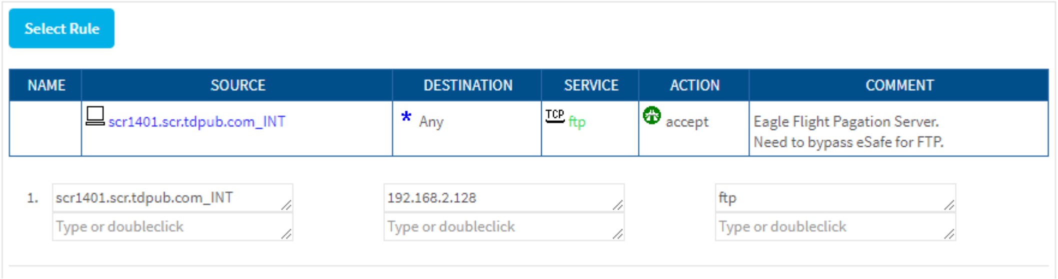
**Note:** FireFlow is fully configurable, and your system may differ.

### Request

In the Request stage, a privileged user submits a request to modify a device rule, initiating the FireFlow change request lifecycle. This stage consists of the following steps:

1. The requesting privileged user selects a template on which to base their request.
2. If the template specifies a workflow, FireFlow assigns the request to that workflow.
3. The requesting privileged user submits the request to FireFlow.

   The request includes information about which device rule to modify, and how it should be modified. For example, the requestor may submit the following request:

   Select Rule

   | NAME | SOURCE | DESTINATION | SERVICE | ACTION | COMMENT |
   |---|---|---|---|---|---|
   |  | scr1401.scr.tdpub.com_INT | * Any | TCP ftp | accept | Eagle Flight Pagation Server.<br>Need to bypass eSafe for FTP. |

   |  |  |  |  |
   |---|---|---|---|
   | 1. | scr1401.scr.tdpub.com_INT | 192.168.2.128 | ftp |
   |  | Type or doubleclick | Type or doubleclick | Type or doubleclick |

4. FireFlow receives the request information and creates a *change request*.
5. If a workflow has not yet been assigned, FireFlow assigns a workflow. For more details, see Request templates and workflows.
6. The *default assignee* of the role handling new change requests (by default, the Network Operations role) is assigned as the change request's *owner*.
7. FireFlow sends an email message informing the requesting privileged user that the change request was created, and specifying the change request ID in the format [FireFlow #<*number*>], for example [FireFlow #49].

## Approve

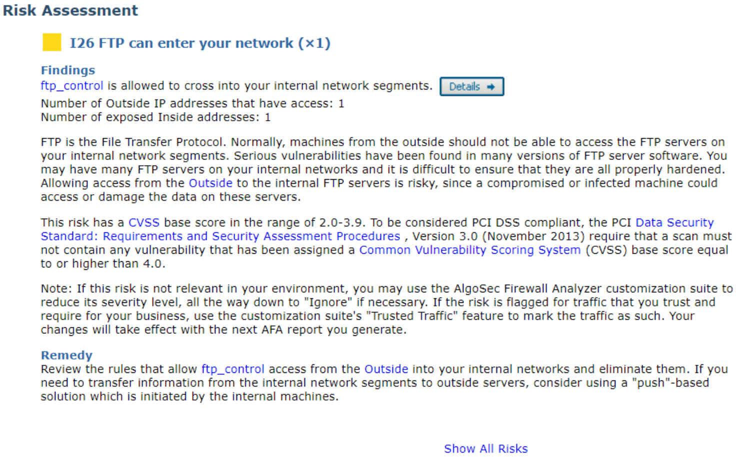
In the Approve stage, a user with the information security role determines the security risks entailed in satisfying the request. This stage consists of the following steps:

1. The *default assignee* of the role handling change requests in the Approve stage (by default, the Information Security role) is assigned as the change request's owner.
2. The change request may change ownership in one of the following ways:
   - The change request owner assigns it to a user with the information security role.

- An information security user chooses to take responsibility for the change request.

3. If the change request includes an "Allow" action, FireFlow initiates a risk check, to determine whether implementing the requested Allow traffic change would introduce risks.

   FireFlow returns the number and severity of risks detected. The user can view a risk assessment of each risk:



Risk Assessment

🟨 I26 FTP can enter your network (×1)

Findings

ftp_control is allowed to cross into your internal network segments.

Number of Outside IP addresses that have access: 1
Number of exposed Inside addresses: 1

FTP is the File Transfer Protocol. Normally, machines from the outside should not be able to access the FTP servers on your internal network segments. Serious vulnerabilities have been found in many versions of FTP server software. You may have many FTP servers on your internal networks and it is difficult to ensure that they are all properly hardened. Allowing access from the Outside to the internal FTP servers is risky, since a compromised or infected machine could access or damage the data on these servers.

This risk has a CVSS base score in the range of 2.0-3.9. To be considered PCI DSS compliant, the PCI Data Security Standard: Requirements and Security Assessment Procedures , Version 3.0 (November 2013) require that a scan must not contain any vulnerability that has been assigned a Common Vulnerability Scoring System (CVSS) base score equal to or higher than 4.0.

Note: If this risk is not relevant in your environment, you may use the AlgoSec Firewall Analyzer customization suite to reduce its severity level, all the way down to "Ignore" if necessary. If the risk is flagged for traffic that you trust and require for your business, use the customization suite's "Trusted Traffic" feature to mark the traffic as such. Your changes will take effect with the next AFA report you generate.

Remedy

Review the rules that allow ftp_control access from the Outside into your internal networks and eliminate them. If you need to transfer information from the internal network segments to outside servers, consider using a "push"-based solution which is initiated by the internal machines.

4. If the change request includes a "Drop" action, the following things happen:

   a. The network operations user initiates a search for change requests change requests whose traffic will be blocked by the "Drop" action.

   b. FireFlow returns a list of related change requests.

   c. The network operations user then specifies which of the related change requestors (and optionally other users) should receive a notification that the traffic will be blocked.

   d. FireFlow sends an email to the selected requestors.

   e. The requestors respond via email message or Web interface.

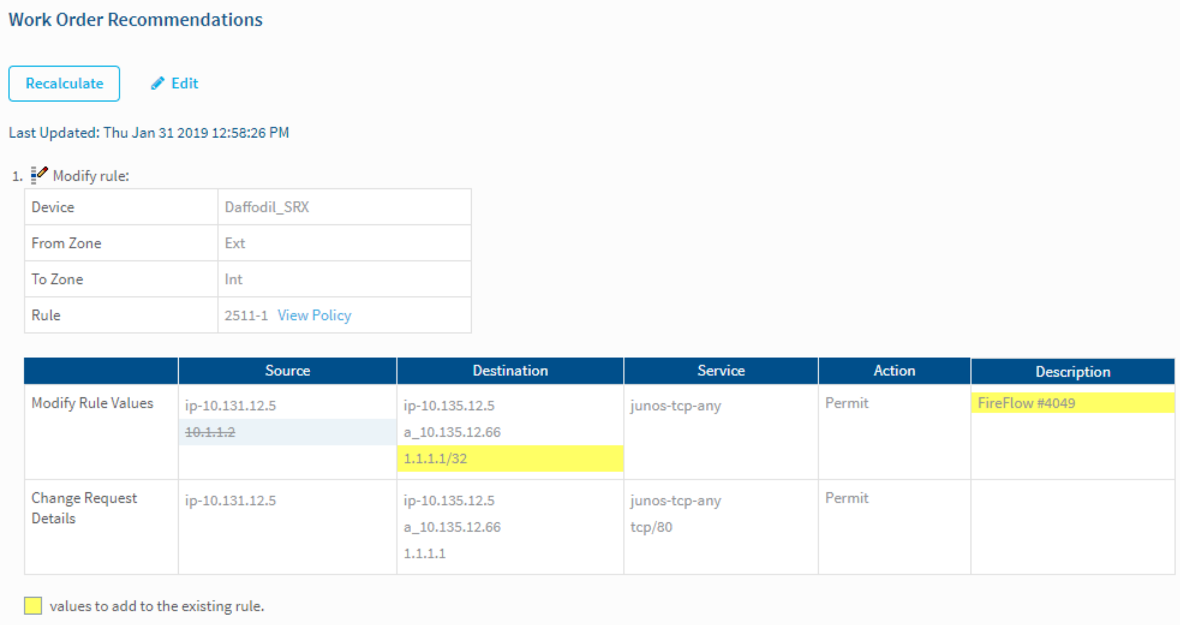
5. The information security user does one of the following:

- Approves the change request and sends it on to the next stage.
- Rejects the change request and returns it to the Plan stage.
- Rejects and closes the change request. In this case, an email message is sent to the requestor, indicating that the request is denied.
- Contacts the requestor and asks for more information.

## Implement

In the Implement stage, the network operations user plans and executes request implementation. This stage consists of the following steps:

1. FireFlow creates a work order and displays a list of recommendations for implementing the requested change.



Work Order Recommendations

Last Updated: Thu Jan 31 2019 12:58:26 PM

1. Modify rule:

| | |
|---|---|
| Device | Daffodil_SRX |
| From Zone | Ext |
| To Zone | Int |
| Rule | 2511-1 View Policy |

| | Source | Destination | Service | Action | Description |
|---|---|---|---|---|---|
| Modify Rule Values | ip-10.131.12.5<br>~~10.1.1.2~~ | ip-10.135.12.5<br>a_10.135.12.66<br>1.1.1.1/32 | junos-tcp-any | Permit | FireFlow #4049 |
| Change Request Details | ip-10.131.12.5 | ip-10.135.12.5<br>a_10.135.12.66<br>1.1.1.1 | junos-tcp-any<br>tcp/80 | Permit | |

🟨 values to add to the existing rule.

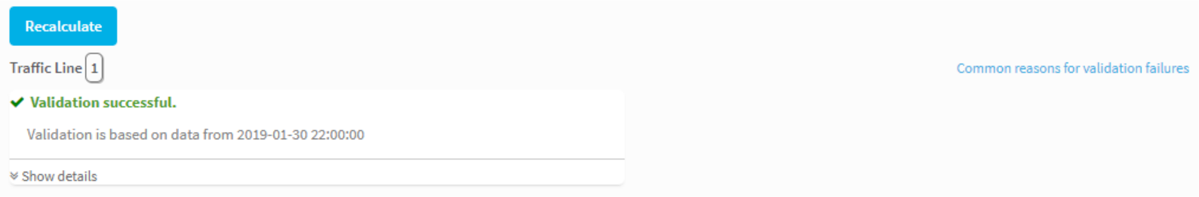
2. If the rule has changed while the change request was being processed, the network operations user will have the option to re-plan. Re-planning updates the rule values in FireFlow.
3. The network operations user edits the work order, by adding notes to the work order.

4. The network operations user implements the requested changes on the security device according to the work order, by using the relevant management system (for example, Check Point Dashboard or Juniper NSM) to implement the changes.
5. The network operation user sends the change request on to the next stage.

## Validate

In the Validate stage, the network operation user validates the implemented rule modification against the change request. This stage consists of the following steps:

1. The network operations user validates the implemented rule modification against the change request.



✓ Validation successful.

Validation is based on data from 2019-01-30 22:00:00

2. If validation indicates that the specified rule was not modified, then the network operations user re-initiates the Implement stage.
3. Once the rule modification has been successfully validated, the network operations user resolves the change request.

At this point, the change request's lifecycle has effectively ended, and no further user action is required. However, the change request remains available in the system for auditing purposes, as described in the final stages.

## Match

According to a configurable schedule, FireFlow automatically checks all devices for rule changes and determines the following:

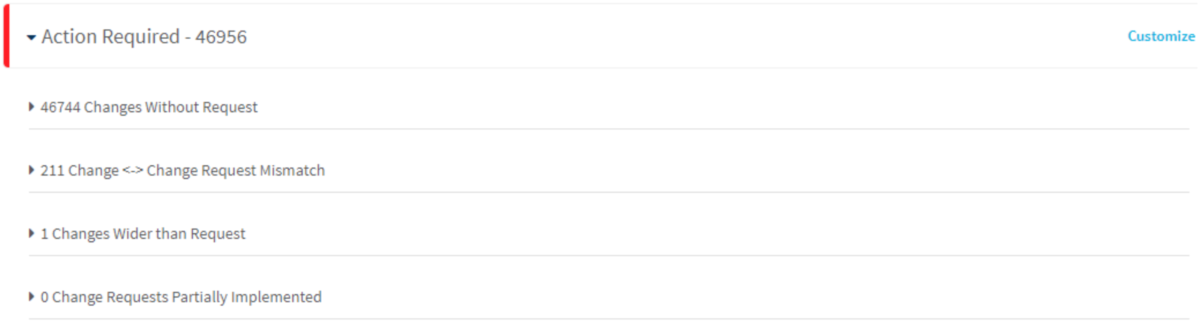
- Each change is associated with a change request.
- Each change request is associated with a change.
- Each change is associated with the *correct* change request.

- The scope of each change matches the approved scope in the associated change request.

If there are no problems with a given change request, FireFlow automatically marks it as matched.

For control purposes, an information security user periodically checks that all change requests were matched successfully, and resolves any problems that FireFlow may have detected during auto matching. The Match stage consists of the following steps:

1. The information security user checks whether FireFlow detected any matching problems with the validated change requests in the system.



Action Required - 46956

46744 Changes Without Request

211 Change <-> Change Request Mismatch

1 Changes Wider than Request

0 Change Requests Partially Implemented

2. If a problem is detected for a change request, the information security user does one of the following:
   - Re-opens the change request
   - Manually approves the mismatch

**Note:** It is recommended to perform these steps on a weekly or monthly basis.

## Resolved

Once the change request has been validated, it enters the Resolved stage.

## Audit

The Audit stage for rule modification request lifecycles is identical to the Audit stage for traffic change request lifecycles. See Audit (see Audit).

# Web filtering change workflow

This topic describes the events that occur in each stage in a default web filtering change workflow.

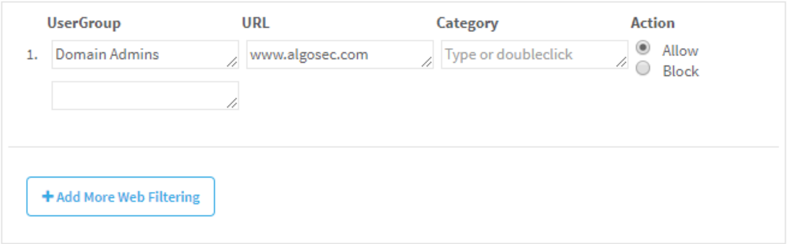
> **Note:** FireFlow is fully configurable, and your system may differ.

## Request

In the Request stage, a requestor submits a request to filter a URL, initiating the FireFlow change request lifecycle. This stage consists of the following steps:

1. The requestor selects a template on which to base their request.
2. If the template specifies a workflow, FireFlow assigns the request to that workflow.
3. The requestor submits the request to FireFlow.

   The request includes information about the relevant user group, URL, category, and action for the Web filtering rule. For example, the requestor may submit the following request:

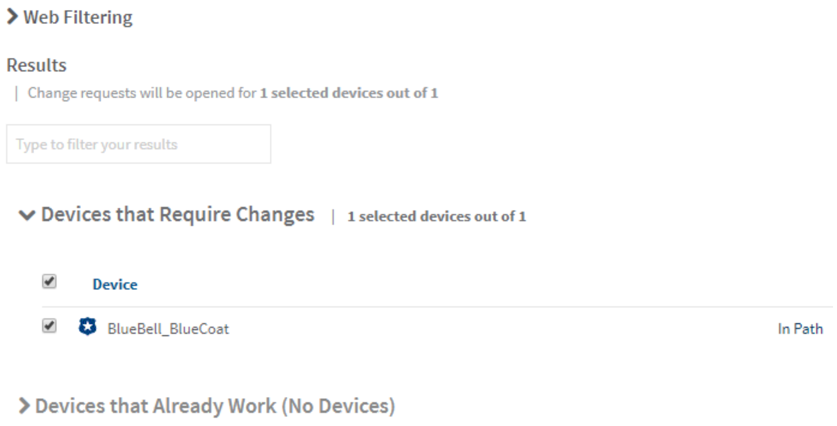
   |  | UserGroup | URL | Category | Action |
   |---|---|---|---|---|
   | 1. | Domain Admins | www.algosec.com | Type or doubleclick | ● Allow<br>○ Block |

4. FireFlow receives the request information and creates a *change request*.
5. If a workflow has not yet been assigned, FireFlow assigns a workflow. For more details, see Request templates and workflows.
6. The *default assignee* of the role handling new change requests (by default, the Network Operations role) is assigned as the change request's *owner*.
7. FireFlow sends an email message informing the requestor that the change request was created, and specifying the change request ID in the format [FireFlow #<*number*>], for example [FireFlow #49].

## Plan

In the Plan stage, a user with the network operations role plots out the technical changes needed in order to satisfy the change request. This stage consists of the following steps:

1. The change request may change ownership in one of the following ways:
    - The change request owner assigns it to a user with the network operations role.
    - A network operations user chooses to take responsibility for the change request.
2. FireFlow initiates a query to identify relevant devices.
3. The network operations user uses FireFlow to confirm which devices are relevant to the requested change.



> Web Filtering
Results
Type to filter your results
> Devices that Already Work (No Devices)

| Change requests will be opened for **1 selected devices out of 1**

Devices that Require Changes | 1 selected devices out of 1

| ☑ | Device | |
|---|---|---|
| ☑ | BlueBell_BlueCoat | In Path |

4. If the network user modified the Web filtering change request, FireFlow tests whether the requested URL is already allowed/denied to the specified users/user groups. If the URL is already allowed/denied, the network operations user closes the change request, and FireFlow sends an email message to the requestor indicating that the change request was closed.
5. If there is more than one device that is relevant to the change, the network operations user selects the devices on which to implement the change.
6. The network operation user sends the change request on to the next stage.

7. If the network operations user selected multiple devices, FireFlow will generate a sub-request for each.

## Approve

The Approve stage consists of the following steps:

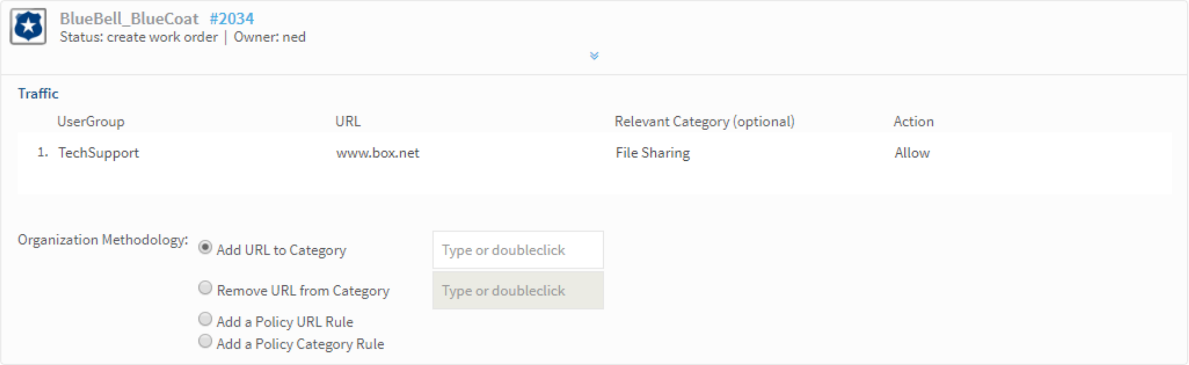
1. The *default assignee* of the role handling change requests in the Approve stage (by default, the Information Security role) is assigned as the change request's owner.
2. The change request may change ownership in one of the following ways:
   - The change request owner assigns it to a user with the information security role.
   - An information security user chooses to take responsibility for the change request.
3. The information security user does one of the following:
   - Approves the change request and sends it on to the next stage.
   - Rejects the change request. In this case the change request returns to the start of the Approve stage.
   - Contacts the requestor and asks for more information.

## Implement

In the Implement stage, the network operations user plans and executes request implementation. If the request was created for multiple devices, this stage must be performed separately for each sub-request.

This stage consists of the following steps:

1. The change request's ownership is returned to the network operations user.
2. The network operations user chooses an organizational methodology to use for implementing the requested change.



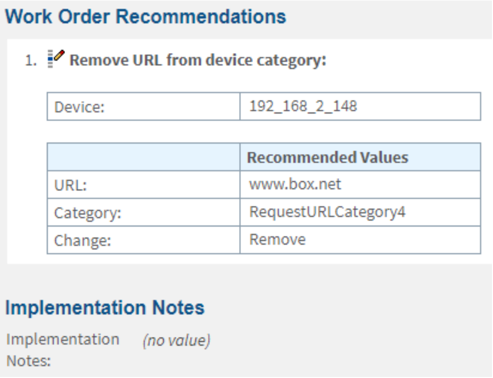
BlueBell_BlueCoat #2034
Status: create work order | Owner: ned

Traffic

|  | UserGroup | URL | Relevant Category (optional) | Action |
|---|---|---|---|---|
| 1. | TechSupport | www.box.net | File Sharing | Allow |

Organization Methodology:
● Add URL to Category — Type or doubleclick
○ Remove URL from Category — Type or doubleclick
○ Add a Policy URL Rule
○ Add a Policy Category Rule

3. FireFlow creates a work order and displays a list of recommendations for implementing the requested change.



Work Order Recommendations

1. Remove URL from device category:

|  |  |
|---|---|
| Device: | 192_168_2_148 |

|  | Recommended Values |
|---|---|
| URL: | www.box.net |
| Category: | RequestURLCategory4 |
| Change: | Remove |

Implementation Notes

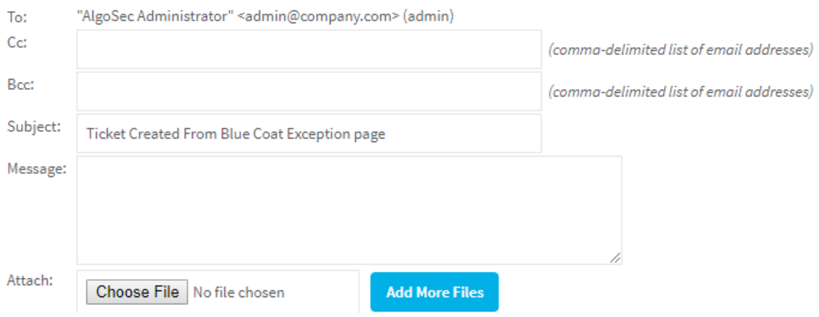
Implementation Notes: *(no value)*

4. The network operations user edits the work order, by adding notes to the work order.
5. The network operations user implements the requested changes on the security device according to the work order.
6. The network operation user sends the change request on to the next stage.

## Validate

In the Validate stage, the network operation user validates the implemented device policy changes against the change request. The requestor then checks that the request was implemented, and the network operations user resolves the change request. This stage consists of the following steps:

1. The network operations user composes an email message in FireFlow, notifying the requestor that the requested changes were implemented.



To: "AlgoSec Administrator" <admin@company.com> (admin)

Cc: (comma-delimited list of email addresses)

Bcc: (comma-delimited list of email addresses)

Subject: Ticket Created From Blue Coat Exception page

Message:

Attach: No file chosen

2. FireFlow sends the email to the requestor.
3. The requestor checks that the requested change was implemented and the desired result was achieved.
4. One of the following things happens:
   - If the desired result was not achieved, the requestor responds via an email message or via the Web interface, and the network operations user then re-initiates the implementation stage.
   - If the desired result was achieved, the requestor responds via an email message or via the Web interface, and the network operations user then resolves the change request.
   - If the requestor does not respond, the network operations user can choose to resolve the change request anyway.

At this point, the change request's lifecycle has effectively ended, and no further user action is required. However, the change request remains available in the system for auditing purposes, as described in the final stages.

## Resolved

Once the change request has been matched to the relevant change(s), it enters the Resolved stage.

## Audit

The Audit stage for Web filtering change request lifecycles is identical to the Audit stage for traffic change request lifecycles. See Audit (see Audit).

# Request changes

**Relevant for: All FireFlow users**

This topic provides a high level description of the various methods available for creating new change requests.

As the change request is processed, FireFlow will send you notification emails. For more details, see Respond to change requests.

**Tip:** By default, many request fields are optional. We recommend entering values for as many fields as possible to enable the team to process your request efficiently.

## Request changes via FireFlow

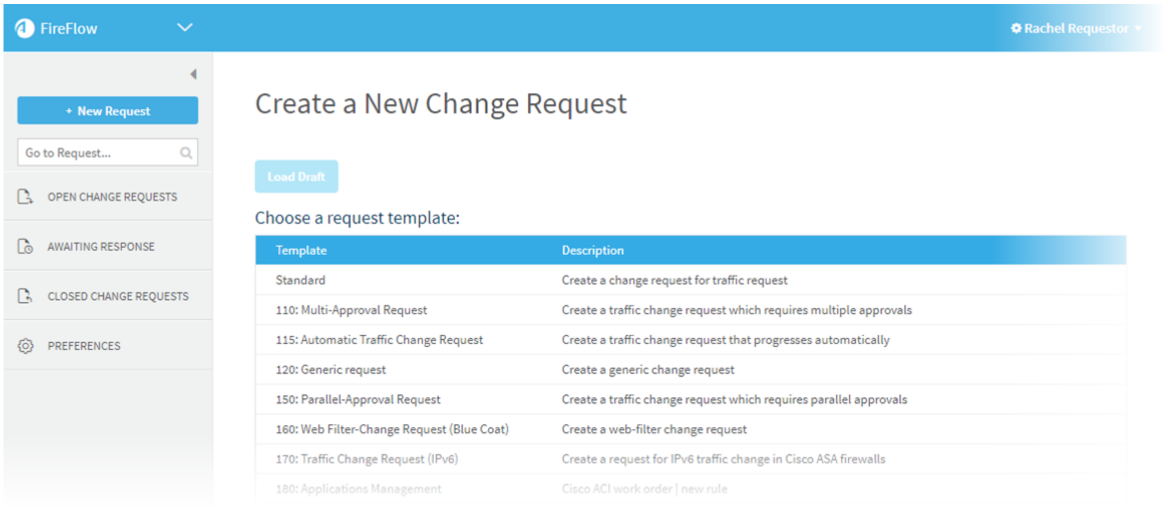
All FireFlow users can log in a submit a change request directly from FireFlow. The user interface will look different for FireFlow requestor users, displaying only the options available to them.

### Do the following:

To submit a new change request, do the following:

1. In FireFlow, at the top left, click **+ New Request**. FireFlow displays a list of templates to choose from.

   For example:



Create a New Change Request

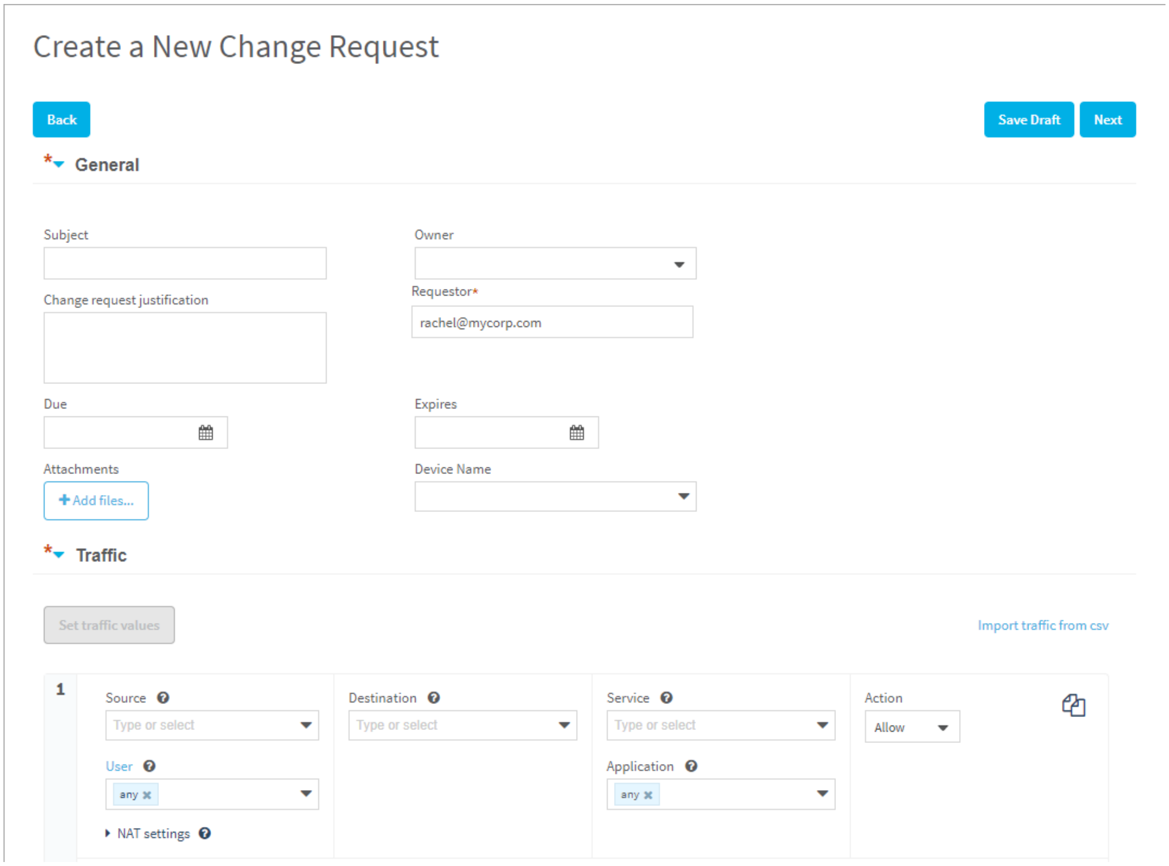
Choose a request template:

| Template | Description |
|---|---|
| Standard | Create a change request for traffic request |
| 110: Multi-Approval Request | Create a traffic change request which requires multiple approvals |
| 115: Automatic Traffic Change Request | Create a traffic change request that progresses automatically |
| 120: Generic request | Create a generic change request |
| 150: Parallel-Approval Request | Create a traffic change request which requires parallel approvals |
| 160: Web Filter-Change Request (Blue Coat) | Create a web-filter change request |
| 170: Traffic Change Request (IPv6) | Create a request for IPv6 traffic change in Cisco ASA firewalls |
| 180: Applications Management | Cisco ACI work order \| new rule |

2. To load a recent draft, click **Load Draft** above the list of templates. Otherwise, click the template you want to use.

   The **Create a New Change Request** page appears, displaying the fields configured for the selected template.

   For example:



Create a New Change Request

Requestor*
rachel@mycorp.com

User
any

Application
any

Action
Allow

3. Enter the field values as needed.

   - All **Traffic** fields are mandatory, as indicated by a red asterisk.
   - IPv4 and IPv6 traffic cannot be mixed in the same traffic request.

### Upload a request spreadsheet

FireFlow enables you to upload a spreadsheet with request data. By default, change requests submitted via spreadsheet use the **120: Generic Request** template.

Do the following:

a. Prepare your file. Supported file types include:

   - **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)

   Sample files are saved to your FireFlow machine at **/usr/share/fireflow/local/extras**.

   In the file, **Source**, **Destination**, **Protocol**, and **Port** columns are mandatory.

b. In the **Create a New Change Request** page, click **Add Files** to attach the spreadsheet to your request.

> **Note:** By default, FireFlow creates a separate change request from each traffic line in the spreadsheet file. Your system may differ. For details, contact your FireFlow administrator.

For more details, see Change request field references.

4. To save a draft and continue later, click **Save Draft**, and then click **OK**.

> **Note:** FireFlow supports one draft per user. New drafts overwrite previous draft versions.

To create your request, click **Next**.

FireFlow creates your request and displays the request ID number linked from the top-right of your screen. Click the linked number to view the change request.

FireFlow also sends you an email notification and checks your request.

- **If the traffic already works**, FireFlow automatically closes the request and sends you another confirmation email.
- **If the request requires changes**, FireFlow pushes the request through the workflow configured for your request template.

For more details, see View change requests.

## Duplicate a change request in FireFlow

To create a change request that is similar to an existing one, duplicate the exiting change request, making changes as needed.

### Do the following:

1. In FireFlow, navigate to the change request you want to duplicate. For details, see View change requests.
2. At the top of the page, click ≡, and then click **Duplicate**.

   The **Create a New Change Request** page appears, with the original request's details and subject.
3. Modify the values as needed, and click **Create**.

   For details, see Change request field references.

3. Modify the fields as desired, using the information in Requestor Create Change Request Fields (see Change request field references).
4. Click **Create**.

FireFlow creates your request and sends you an email confirmation. At the same time, FireFlow checks your request and does one of the following:

- **If the traffic already works**, FireFlow automatically closes the request and sends you another confirmation email.

- **If the request requires changes**, FireFlow pushes the request through the workflow configured for your request template.

## Request a change via the no-login request form

FireFlow's no-login request form enables you to submit a request without logging in to FireFlow.

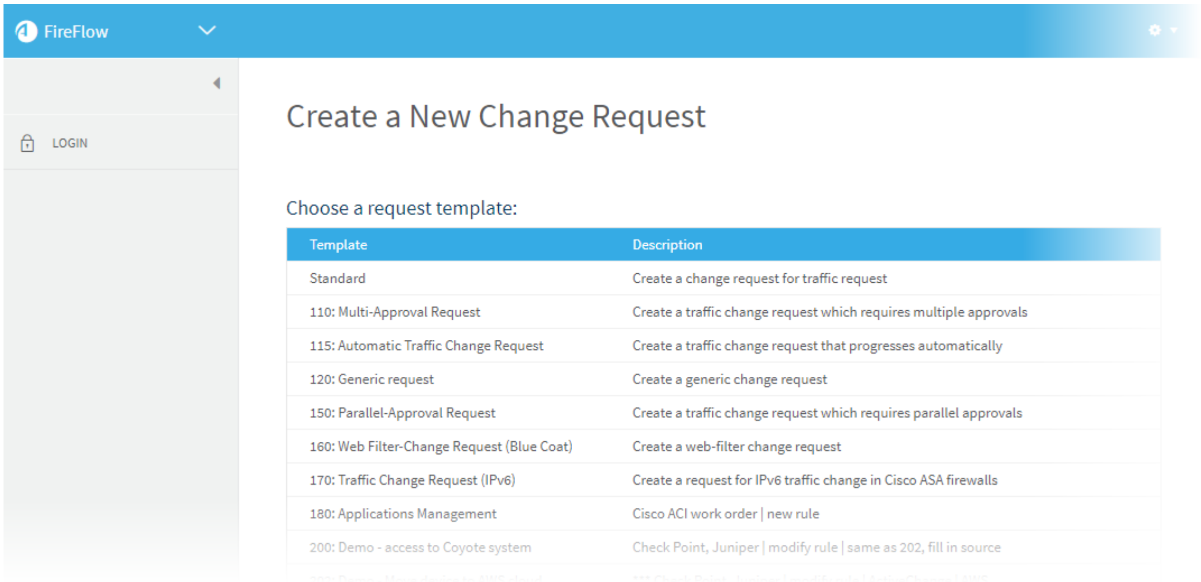
> **Note:** This method is only available if configured for your system. For more details, contact your FireFlow administrator.

### Do the following:

1. In your browser's **Address** field, enter **https://<fireflow server>/FireFlow/NewTicket**

   where **<FireFlow_server>** is the FireFlow server URL.

   he **Create a New Change Request** page is displayed with a list of templates. For example:

   Create a New Change Request

   Choose a request template:

   | Template | Description |
   |---|---|
   | Standard | Create a change request for traffic request |
   | 110: Multi-Approval Request | Create a traffic change request which requires multiple approvals |
   | 115: Automatic Traffic Change Request | Create a traffic change request that progresses automatically |
   | 120: Generic request | Create a generic change request |
   | 150: Parallel-Approval Request | Create a traffic change request which requires parallel approvals |
   | 160: Web Filter-Change Request (Blue Coat) | Create a web-filter change request |
   | 170: Traffic Change Request (IPv6) | Create a request for IPv6 traffic change in Cisco ASA firewalls |
   | 180: Applications Management | Cisco ACI work order \| new rule |
   | 200: Demo - access to Coyote system | Check Point, Juniper \| modify rule \| same as 202, fill in source |
   | 202: Demo - Move device to AWS cloud | *** Check Point, Juniper \| modify rule \| ActiveChange \| AWS |

2. Click the name of the template you want to use. For more details, see [Request templates and workflows](). If you have questions about custom templates or

workflows, contact your FireFlow administrator.

The FireFlow **Create a New Change Request** page is displayed.

3. Complete the fields as required. For details, see Change request field references
4. Click **Next** to create your request.

FireFlow creates your request and sends you an email confirmation. At the same time, FireFlow checks your request and does one of the following:

- **If the traffic already works**, FireFlow automatically closes the request and sends you another confirmation email.
- **If the request requires changes**, FireFlow pushes the request through the workflow configured for your request template.

## Request a change by email

Send an email to FireFlow with the details of your change request.

**Note:** This method is only available if configured for your system. For more details, contact your FireFlow administrator.

### Do the following:

1. Create a new email to the FireFlow system email address. For details, contact your FireFlow administrator.
2. Include the following line anywhere in your email:

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

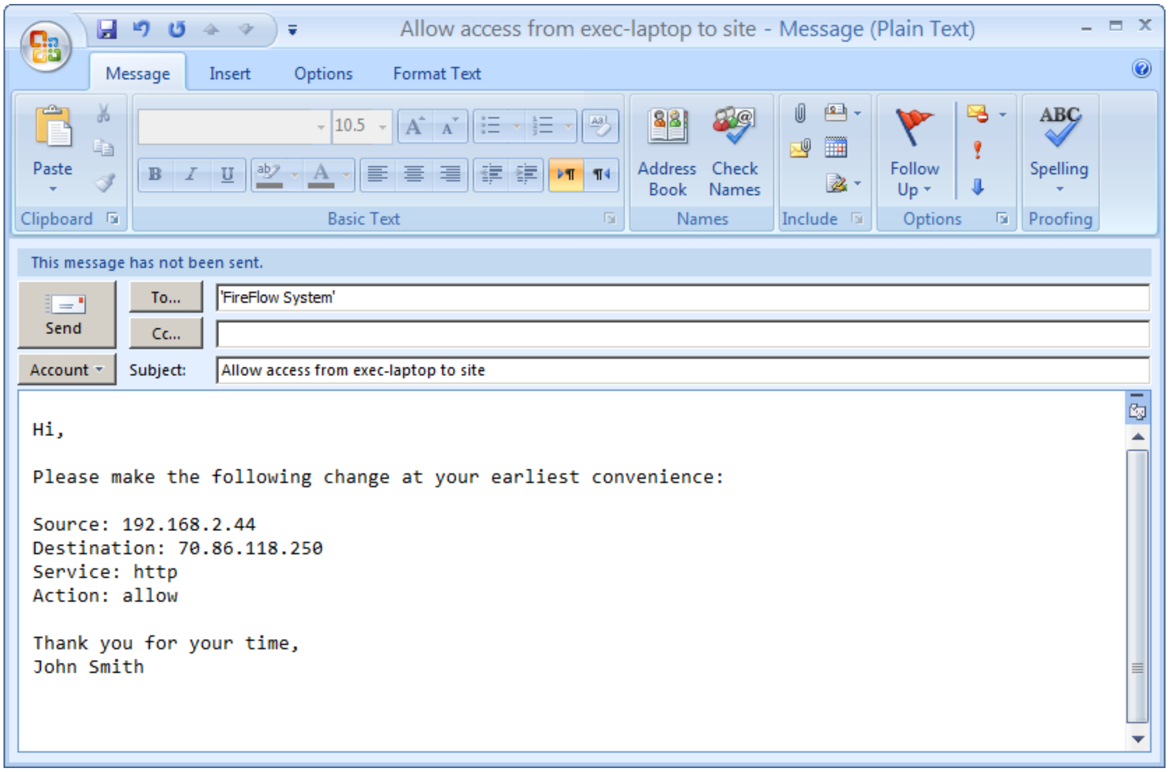
   where:

   - **<source>** is an IP address, IP range, network or device object.
   - **<destination>** is an IP address, IP range, network or device object.
   - **<service>** is the device service or port.

- **<action>** is the device action to perform for the connection:
  - **allow**. Allow the connection.
  - **block**. Block the connection.

> **Note:** This syntax is the default FireFlow syntax for emailing change requests. Your system may be configured differently.
>
> For details, contact your FireFlow administrator.

For example:



This message has not been sent.

To... 'FireFlow System'

Subject: Allow access from exec-laptop to site

```
Hi,

Please make the following change at your earliest convenience:

Source: 192.168.2.44
Destination: 70.86.118.250
Service: http
Action: allow

Thank you for your time,
John Smith
```

FireFlow creates your request and sends you an email confirmation. Your email text and any technical details specified is added to the change history.

At the same time, FireFlow checks your request and does one of the following:

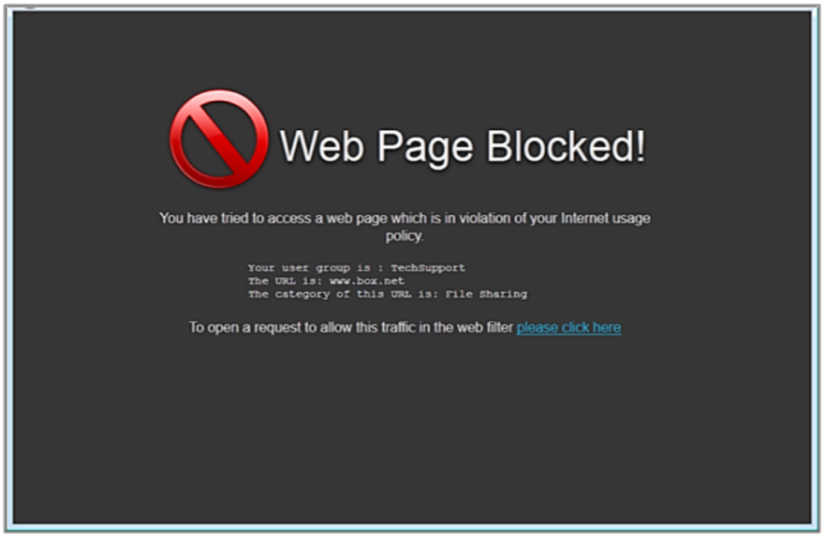
- **If the traffic already works**, FireFlow automatically closes the request and sends you another confirmation email.

- **If the request requires changes**, FireFlow pushes the request through the workflow configured for your request template.

## Request a change from the Symantec Blue Coat **Blocked** page

If you attempt to access a URL that is blocked by the Symantec Blue Coat device's web filtering policy, the **Blocked** page enables you to submit a change request directly.

For example:



Web Page Blocked!

You have tried to access a web page which is in violation of your Internet usage policy.

```
Your user group is : TechSupport
The URL is: www.box.net
The category of this URL is: File Sharing
```

To open a request to allow this traffic in the web filter please click here

### Do the following:

1. Click the link on the page, such as **please click here**, or **Autocreate Change Request**, depending on configuration.

   FireFlow displays the **Create a New Change Request** page.

2. Complete the fields as needed. For details, see Web-filter change request fields.

3. Click **Create**.

FireFlow creates your request and sends you an email confirmation. At the same time, FireFlow checks your request and does one of the following:

- **If the traffic already works**, FireFlow automatically closes the request and sends you another confirmation email.
- **If the request requires changes**, FireFlow pushes the request through the workflow configured for your request template.

# Change request field references

**Relevant for: All FireFlow users**

This topic describes the fields available in FireFlowchange requests.

## Generic change request fields

| Name | Description |
|---|---|
| **Subject** | Type a title for your request and for the change request that will be generated.<br>**Note:** This field is optional. |
| **Due** | Specify the date by which this change request should be resolved, by doing one of the following:<br>• Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>• Type the desired date in the field provided. You can use most relative and absolute formats, for example `yyyy-mm-dd`, `mm/dd/yyyy`, `Mon dd yyyy`, “next week”, and “now + 3 days”.<br>**Note:** This field is optional. |
| **Describe the issue** | Type a free text description of the issue.<br>This description will be reviewed by the network operations and information security users who handle your change request. It will also be added to the change request history.<br>**Note:** This field is optional. |

| Name | Description |
|---|---|
| **Attach File** | To attach a file to your request, do one of the following:<br>• Type the path to the file in the field provided.<br>• Click **Browse**, browse to the desired file, and click **Open**.<br>If you are using the **120: Generic Request template** or any custom template that allows creating change requests from files, FireFlow will create a change request from an attached spreadsheet file. For more information on creating change requests from file, see Creating Change Requests from File.<br>• To add more files, click **Add More Files**.<br>**Note:** This field is optional. |
| **Requestor** | In the Requestors Web Interface, this field displays your email address and is read-only.<br>**Note:** In the No-Login Web Form, you must type your email address. |
| **Expires** | Specify the date on which this change request will expire, by doing one of the following:<br>• Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>• Type the desired date in the field provided.<br>FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**.<br>**Note:** This field is optional. |

| Name | Description |
|---|---|
| **External change request id** | If you have already opened a change request for this request in an external change management system that is integrated with FireFlow, type the change request's ID number.<br>The FireFlow change request generated for your request will be linked to the external system change request.<br>**Note:** This field is optional. |
| **Workflow** | The change request's workflow.<br>**Note:** This field is read-only. |
| **From Template** | The change request's template.<br>**Note:** This field is read-only. |

## Traffic-based change request fields

| Name | Description |
|---|---|
| **Requestor** | In the Requestors Web Interface, this field displays your email address and is read-only.<br>**Note:** In the No-Login Web Form, you must type your email address. |
| **Subject** | Type a title for your request and for the change request that will be generated.<br>**Note:** This field is optional. |

| Name | Description |
|---|---|
| **Due** | Specify the date by which this change request should be resolved, by doing one of the following:<br>- Click 📅 , and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>- Type the desired date in the field provided.<br>FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**.<br>**Note:** This field is optional. |
| **Expires** | Specify the date on which this change request will expire, by doing one of the following:<br>- Click 📅 , and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>- Type the desired date in the field provided. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**.<br>**Note:** This field is optional. |
| **Request** | Due to system customizations, this area may include fields that are not described below. Some possible additional fields are described below. For additional information, consult with your FireFlow administrator. |
| **Source** | Specify the traffic source(s). For details, see Change request wizards.<br>**Note:** You can optionally input variables into traffic fields, and these variables will be set to the desired value once you submit the change request. For details, see Variables in traffic fields. |

| Name | Description |
|---|---|
| **User** | Enter one or more (comma separated) user names and/or groups. The default value is **Any**.<br>This field is only relevant for Check Point and Palo Alto devices. |
| **Destination** | Specify the traffic destination(s). For details, see Change request wizards.<br>**Note:** You can optionally input variables into traffic fields, and these variables will be set to the desired value once you submit the change request. For details, see Variables in traffic fields. |
| **Service** | Specify the traffic service(s). For details, see Change request wizards.<br>**Note:** You can optionally input variables into traffic fields, and these variables will be set to the desired value once you submit the change request. For details, see Variables in traffic fields.<br>**Note:** For traffic that affects Check Point devices, you must specify a service that is supported by the authentication method. For information on supported services for each method, refer to Check Point documentation. |
| **Application** | Specify the application(s). For details, see Change request wizards.<br>The default value is **Any**.<br>This field is only relevant for Palo Alto devices. |
| **Action** | Choose the device action to perform for the connection. This can be either of the following:<br>• **Allow:** Allow the connection.<br>• **Drop:** Block the connection.<br>• **Note:** When using the Traffic Change Request (IPv6) workflow, only traffic with "Allow" actions is supported. |

| Name | Description |
|---|---|
| **Show NAT** | Click this option to display Network Address Translation (NAT) and Port Address Translation (PAT) for the defined traffic.<br>The **Source NAT**, **Destination NAT**, **Port Translation**, and **NAT Type** fields appear.<br>Depending on system customizations, the **Source after NAT**, **Destination after NAT**, and **Port after Translation** fields may appear as well. |
| **Hide NAT** | Click this option to hide the NAT and PAT fields. |
| **Source NAT** | Type the source NAT value, if the connection's source should be translated.<br>**Note:** If the **Source after NAT** field appears below this field, then you must type the source NAT value *before* translation. |
| **Source after NAT** | Type the source NAT value after translation, if the connection's source should be translated. |
| **Destination NAT** | Type the destination NAT value, if the connection's destination should be translated.<br>**Note:** If the **Destination after NAT** field appears below this field, then you must type the destination NAT value *before* translation. |
| **Destination after NAT** | Type the destination NAT value after translation, if the connection's destination should be translated. |
| **Port Translation** | Type the port value, if the connection's port should be translated.<br>**Note:** If the **Port after Translation** field appears below this field, then you must type the port value *before* translation. |
| **Port after Translation** | Type the port value after translation, if the connection's port should be translated. |
| **NAT Type** | Specify the type of NAT (**Static** or **Dynamic**).<br>**Note:** If you filled in the **Source NAT**, **Destination NAT**, and/or **Port Translation** fields, then you must specify the NAT type. |

| Name | Description |
|---|---|
| **Add More Traffic** | To add more traffic to the request, click this option and complete the fields. |
| **Set traffic values** | Click this button to set traffic values for variables you have put in the source, destination or service fields.<br>For details, see Variables in traffic fields. |
| **Import traffic from csv** | Click this link to import a CSV file of traffic lines. Select the CSV file from your computer.<br>**Required Headers:**<br>- Source<br>- Destination<br>- Service<br>**Optional Headers:**<br>- User. If this header is not present, the value defaults to "any".<br>- Application. If this value is not present, the value defaults to "any".<br>- Action. If this header is not present, the value defaults to "allow".<br>Any other headers included in the CSV file are ignored.<br>**Note:** All headers are not case sensitive.<br>Multiple entries (such as IP addressees, ranges, or networks) that appear in a single cell must be separated by commas within the cell. |
| ⧉ | To replicate a traffic line (add a new traffic line with the same traffic as in the current traffic line), click this option and modify the fields as desired. |
| 🗑 | To remove additional traffic from the request, click this option next to the desired traffic. |
| **More** | |

| Name | Description |
|---|---|
| **External change request id** | If you have already opened a change request for this request in an external change management system that is integrated with FireFlow, type the change request's ID number.<br>The FireFlow change request generated for your request will be linked to the external system change request.<br>**Note:** This field is optional. |

## IPv6 traffic change request fields

| Name | Description |
|---|---|
| **Requestor** | In the Requestors Web Interface, this field displays your email address and is read-only.<br>**Note:** In the No-Login Web Form, you must type your email address. |
| **Subject** | Type a title for your request and for the change request that will be generated.<br>**Note:** This field is optional. |
| **Due** | Specify the date by which this change request should be resolved, by doing one of the following:<br>• Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>• Type the desired date in the field provided. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**.<br>**Note:** This field is optional. |

| Name | Description |
|---|---|
| **Expires** | Specify the date on which this change request will expire, by doing one of the following:<br>• Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>• Type the desired date in the field provided. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**.<br>**Note:** This field is optional. |
| **Request** | Use this area to specify the traffic changes you would like.<br>By default, when submitting a traffic change request, this area includes the following fields for defining traffic: **Source**, **Destination**, **Service**, **Action**, **Show NAT**, **Hide NAT**, **Source NAT**, **Destination NAT**, **Port Translation**, **NAT Type**, **Add More Traffic**, and 🗑 .<br>Due to system customizations, this area may differ in the following ways:<br>• NAT fields may not appear.<br>• The following additional NAT fields may appear: **Source after NAT**, **Destination after NAT**, **Port after Translation**.<br>• The **Source**, **Destination**, and/or **Service** fields may be followed by a custom field. For information about these fields, consult with your FireFlow administrator.<br>• Each row of traffic may be followed by a custom field. For information about these fields, consult with your FireFlow administrator. |

| Name | Description |
|---|---|
| **Source** | Do one of the following:<br>• Type the IP address, IP range, network, or device object.<br>• Use the **Choose Source Wizard**. For details, see Change request wizards.<br>**Note:** Only IPv6 addresses are supported. You cannot mix IPv6 and IPv4 addresses in the same workflow. |
| **Destination** | Do one of the following:<br>• Type the IP address, IP range, network, device object.<br>• Use the **Choose Destination Wizard**. For details, see Change request wizards.<br>**Note:** Only IPv6 addresses are supported. You cannot mix IPv6 and IPv4 addresses in the same workflow. |
| **Service** | Do one of the following:<br>• Type the device service or port for the connection (for example "http" or "tcp/123"). For more details, see Traffic-based change request fields.<br>For information on how to use non-TCP/UDP/ICMP protocols, Supported layer 3 protocols.<br>• Use the **Choose Service Wizard**. For details, see Change request wizards. |
| **Action** | Choose the device action to perform for the connection. This can be either of the following:<br>• **Allow:** Allow the connection.<br>• **Drop:** Block the connection. |

| Name | Description |
|---|---|
| **Show NAT** | Click this option to display Network Address Translation (NAT) and Port Address Translation (PAT) for the defined traffic.<br>The **Source NAT**, **Destination NAT**, **Port Translation**, and **NAT Type** fields appear.<br>**Note:** Depending on system customizations, the **Source after NAT**, **Destination after NAT**, and **Port after Translation** fields may appear as well. |
| **Hide NAT** | Click this option to hide the NAT and PAT fields. |
| **Source NAT** | Type the source NAT value, if the connection’s source should be translated.<br>**Note:** If the **Source after NAT** field appears below this field, then you must type the source NAT value *before* translation. |
| **Source after NAT** | Type the source NAT value after translation, if the connection’s source should be translated. |
| **Destination NAT** | Type the destination NAT value, if the connection’s destination should be translated.<br>**Note:** If the **Destination after NAT** field appears below this field, then you must type the destination NAT value *before* translation. |
| **Destination after NAT** | Type the destination NAT value after translation, if the connection’s destination should be translated. |
| **Port Translation** | Type the port value, if the connection’s port should be translated.<br>**Note:** If the **Port after Translation** field appears below this field, then you must type the port value *before* translation. |
| **Port after Translation** | Type the port value after translation, if the connection’s port should be translated. |

| Name | Description |
|---|---|
| **NAT Type** | Specify the type of NAT (**Static** or **Dynamic**).<br>**Note:** If you filled in the **Source NAT**, **Destination NAT**, and/or **Port Translation** fields, then you must specify the NAT type. |
| **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. |
| **From Template** | The change request's template.<br>**Note:** This field is read-only. |
| **Workflow** | The change request's workflow.<br>**Note:** This field is read-only. |
| **External change request id** | If you have already opened a change request for this request in an external change management system that is integrated with FireFlow, type the change request's ID number.<br>The FireFlow change request generated for your request will be linked to the external system change request.<br>**Note:** This field is optional. |
| **Describe the issue** | Type a free text description of the issue.<br>This description will be reviewed by the network operations and information security users who handle your change request. It will also be added to the change request history.<br>This field is optional. |

| Name | Description |
|---|---|
| **Attach file** | To attach a file to your request, do one of the following:<br>• Type the path to the file in the field provided.<br>• Click **Browse**, browse to the desired file, and click **Open**.<br>To add more files, click **Add More Files**.<br>**Note:** This field is optional. |

## MulticastTraffic change request fields

| Name | Description |
|---|---|
| **General** | To close General section, click in the heading. To reopen, click again. |
| **Owner** | Owner of the request. |
| **Requestor** | In the Requestors Web Interface, this field displays your email address and is read-only.<br>In the No-Login Web Form, you must type your email address. |
| **Subject** | Type a title for your request and for the change request that will be generated.<br>This field is optional. |
| **Due** | Specify the date by which this change request should be resolved, by doing one of the following:<br>• Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>• Type the desired date in the field provided. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**.<br>This field is optional. |

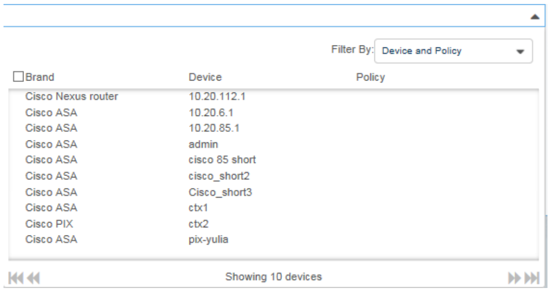
| Name | Description |
|---|---|
| **Expires** | Specify the date on which this change request will expire, by doing one of the following:<br>• Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>• Type the desired date in the field provided. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**.<br>This field is optional. |
| **Traffic** | To close Traffic section, click in the heading. To reopen, click again. |
| **Request** | Use this area to specify the traffic changes you would like.<br>By default, when submitting a traffic change request, this area includes the following fields for defining traffic: **Source**, **Destination**, **Service**, **Action**, **Show NAT**, **Hide NAT**, **Source NAT**, **Destination NAT**, **Port Translation**, **NAT Type**, **Add More Traffic**, and 🗑.<br>Due to system customizations, this area may differ in the following ways:<br>• NAT fields may not appear.<br>• The following additional NAT fields may appear: **Source after NAT**, **Destination after NAT**, **Port after Translation**.<br>• The **Source**, **Destination**, and/or **Service** fields may be followed by a custom field. For information about these fields, consult with your FireFlow administrator.<br>• Each row of traffic may be followed by a custom field. For information about these fields, consult with your FireFlow administrator. |

| Name | Description |
|---|---|
| **Source** | Do one of the following:<br>• Type the IP address, IP range, network, device object, or DNS name of the connection source.<br>• Use the **Choose Source Wizard**, as described in Using the Choose Source/Destination Wizard (see Change request wizards).<br>To enter multiple values, press Enter. A new field appears for this source.<br>**Note:** You cannot mix regular traffic and multicast in the same workflow.<br>When specifying Check Point traffic for which the User Authentication method is used, you can include the user group as part of the source, in the following format:<br>`usergroup@host`<br>Where:<br>• *usergroup* is the user group's name. You may use the **Choose Source Wizard**'s **Device Object** tab to select the user group if desired.<br>**Note:** LDAP user groups are only supported for devices configured to use OPSEC data collection.<br>• *host* is the IP address, IP range, network, device object, or DNS name of the connection source.<br>For example: **group1@1.2.3.4**, **group1@RNDNetwork**, or **group1@Any**.<br>**Note:** Specifying the user group is only supported if the FireFlow default authentication method is User Authentication. Ask your FireFlow administrator for further information. |

| Name | Description |
|---|---|
| **Destination** | Do one of the following:<br>- Type the IP address, IP range, network, device object, or DNS name of the connection destination.<br>- Use the **Choose Destination Wizard**, as described in Using the Choose Source/Destination Wizard (see Change request wizards).<br>To enter multiple values, press **Enter**. A new field appears for this destination.<br>**Note:** You cannot mix regular traffic and multicast in the same workflow. |
| **Service/Application** | Do one of the following:<br>- Type the device service or port for the connection (for example "http" or "tcp/123"). For details, see Supported layer 3 protocols.<br>- Type the name of an application as defined in your Palo Alto or Check Point device.<br>- Use the **Choose Service Wizard**. For details, see Change request wizards.<br>To enter multiple values, press **Enter**. A new field appears for this service.<br>**Note:** When configuring a change request for Check Point traffic, you must specify a service that is supported by the authentication method. For information on supported services for each method, refer to Check Point documentation. |
| **Action** | Choose the device action to perform for the connection. This can be either of the following:<br>- **Allow:** Allow the connection.<br>- **Drop:** Block the connection. |

| Name | Description |
|---|---|
| **NAT settings** | Click this option to display Network Address Translation (NAT) and Port Address Translation (PAT) for the defined traffic.<br>The **Source NAT**, **Destination NAT**, **Port Translation**, and **NAT Type** fields appear.<br>Depending on system customizations, the **Source after NAT**, **Destination after NAT**, and **Port after Translation** fields may appear as well.<br>Click NAT settings again to hide the settings. |
| **Source NAT** | Type the source NAT value, if the connection’s source should be translated.<br>**Note:** If the **Source after NAT** field appears below this field, then you must type the source NAT value *before* translation. |
| **Source after NAT** | Type the source NAT value after translation, if the connection’s source should be translated. |
| **Destination NAT** | Type the destination NAT value, if the connection’s destination should be translated.<br>**Note:** If the **Destination after NAT** field appears below this field, then you must type the destination NAT value *before* translation. |
| **Destination after NAT** | Type the destination NAT value after translation, if the connection’s destination should be translated. |
| **Port Translation** | Type the port value, if the connection’s port should be translated.<br>**Note:** If the **Port after Translation** field appears below this field, then you must type the port value *before* translation. |
| **Port after Translation** | Type the port value after translation, if the connection’s port should be translated. |

| Name | Description |
|---|---|
| **NAT Type** | Specify the type of NAT (**Static** or **Dynamic**).<br>**Note:** If you filled in the **Source NAT**, **Destination NAT**, and/or **Port Translation** fields, then you must specify the NAT type. |
| **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. |
| **More** | To close the More section, click in the heading. To reopen, click again. |
| **External change request id** | If you have already opened a change request for this request in an external change management system that is integrated with FireFlow, type the change request's ID number.<br>The FireFlow change request generated for your request will be linked to the external system change request.<br>This field is optional. |

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td><b>Device Name</b></td><td>
<p>Click in the <b>Device Name</b> box. The device selection dialog box appears with a list of available Cisco devices.</p>

<p>Filter By: Device and Policy</p>
<table>
<tr><th>□Brand</th><th>Device</th><th>Policy</th></tr>
<tr><td>Cisco Nexus router</td><td>10.20.112.1</td><td></td></tr>
<tr><td>Cisco ASA</td><td>10.20.6.1</td><td></td></tr>
<tr><td>Cisco ASA</td><td>10.20.85.1</td><td></td></tr>
<tr><td>Cisco ASA</td><td>admin</td><td></td></tr>
<tr><td>Cisco ASA</td><td>cisco 85 short</td><td></td></tr>
<tr><td>Cisco ASA</td><td>cisco_short2</td><td></td></tr>
<tr><td>Cisco ASA</td><td>Cisco_short3</td><td></td></tr>
<tr><td>Cisco ASA</td><td>ctx1</td><td></td></tr>
<tr><td>Cisco PIX</td><td>ctx2</td><td></td></tr>
<tr><td>Cisco ASA</td><td>pix-yulia</td><td></td></tr>
</table>
<p>Showing 10 devices</p>
<ul>
<li>To filter, in the <b>Filter By</b> list, select <b>Brand</b>, <b>Device</b>, <b>Policy</b>, <b>Device and Policy</b>, or <b>Selected</b>.</li>
<li>To select all devices for a brand, select the <b>Brand</b> check box.</li>
<li>To select, click a device. The device will appear at the top of the box. Click another device to select it. There is no need to hold the CTRL key for multiple selections.</li>
<li>To move forward and backward in the device list, click the ▶▶ and ◀◀ icons.</li>
</ul>
<p>Selected devices appear in the <b>Device Name</b> box.</p>
<p>Click the up arrow to close the dialog box.</p>
</td></tr>
<tr><td><b>Change request justification</b></td><td>
<p>Type a free text description of the issue.</p>
<p>This description will be reviewed by the network operations and information security users who handle your change request. It will also be added to the change request history.</p>
<p>This field is optional.</p>
</td></tr>
<tr><td><b>Attachments</b></td><td>
<p>To add attachments, click <b>Add files</b>. The <b>Choose File to Upload</b> dialog box opens.</p>
<p>Browse to the desired file, and click Open. To select multiple files, press CTRL while selecting.</p>
<p>This field is optional.</p>
</td></tr>
</table>

## Web-filter change request fields

| Name | Description |
|---|---|
| **Requestor** | In the Requestors Web Interface, this field displays your email address and is read-only.<br>In the No-Login Web Form, you must type your email address. |
| **Subject** | Type a title for your request and for the change request that will be generated.<br>This field is optional. |
| **Due** | Specify the date by which this change request should be resolved, by doing one of the following:<br>• Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>• Type the desired date in the field provided. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**.<br>This field is optional. |
| **Expires** | Specify the date on which this change request will expire, by doing one of the following:<br>• Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>• Type the desired date in the field provided. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**.<br>This field is optional. |
| **Request** | Use this area to specify the connection you would like to filter. |

| Name | Description |
|---|---|
| **User Group** | Do one of the following:<br>- Type the name of the user or user group that should be allowed/denied access to a URL.<br>- Use the **Choose User Group Wizard**. For details, see Change request wizards. |
| **URL** | Type the URL to which to allow/deny access. |
| **Category** | Do one of the following:<br>- Type URL's Web filtering category.<br>- Use the **Choose Category Wizard.** For details, see Change request wizards.<br>**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:<br>- **Allow:** Allow the connection.<br>- **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 connections from the request, click this option next to the desired traffic. |
| **From Template** | The change request's template.<br>This field is read-only. |
| **Workflow** | The change request's workflow.<br>This field is read-only. |

| Name | Description |
|---|---|
| **External change request id** | If you have already opened a change request for this request in an external change management system that is integrated with FireFlow, type the change request's ID number.<br>The FireFlow change request generated for your request will be linked to the external system change request.<br>This field is optional. |
| **Describe the issue** | Type a free text description of the issue.<br>This description will be reviewed by the network operations and information security users who handle your change request. It will also be added to the change request history.<br>This field is optional. |
| **Attach file** | To attach a file to your request, do one of the following:<br>• Type the path to the file in the field provided.<br>• Click **Browse**, browse to the desired file, and click **Open**.<br>To add more files, click **Add More Files**.<br>This field is optional. |

## Supported layer 3 protocols

This topic lists the non-TCP/UDP/ICMP protocols that FireFlow supports by default.

| Protocol | FireFlow Defined Service Name | Protocol Number |
|---|---|---|
| IPsec (ESP) | ipsec_50 | 50 |
| IPsec (AH) | ipsec_51 | 51 |
| IPsec (ESP and AH) | ipsec | 50 and 51 |
| GRE | gre | 47 |
| IPv6-ICMP | icmp6 | 58 |
| SKIP | skip | 57 |
| ETHERIP | etherip | 97 |
| PIM | pim | 103 |

**Note:** When using layer 3 protocols in FireFlow, you must use the FireFlow defined service name, not the protocol number. In addition, you may use service objects which contain these protocols.

**Tip:** FireFlow enables administrators to define additional layer 3 protocols for FireFlow support.

## Variables in traffic fields

This procedure describes how to use variables when entering traffic details in a traffic change request.

Variables are supported in any of the traffic lines for the change request.

### Do the following:

1. In the **Source**, **Destination**, **Service**, and/or **Application** field, enter one or more variables using the following syntax:

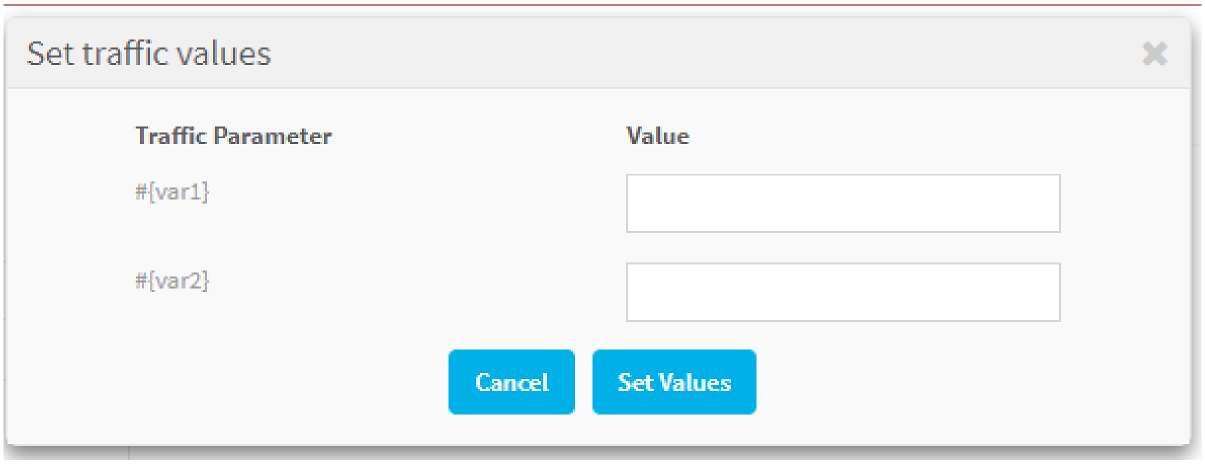
   ```
   #{VariableName}
   ```

   where, **VariableName** is the name you give the variable.

   In the **Traffic** area, the **Set traffic values** button is enabled.

2. Click **Set traffic values**.

   The **Set traffic values** dialog box appears with all of the variables you have used listed under **Traffic Parameter**. For example:



Set traffic values

| Traffic Parameter | Value |
|---|---|
| #{var1} | |
| #{var2} | |

3. Enter the values for each variable you want to use, and click **Set Values**.

When you submit the change request, each variable will be replaced with its designated value.

# Change request wizards

**Relevant for: All FireFlow users**

This topic describes how to use various wizards in the change request forms to help you fid the values you want efficiently.

## Choose Source/Destination wizards

The **Choose Source** and **Choose Destination** wizards help you specify a connection source or destination in a change request.

These wizards differ for IPv4 and IPv6 traffic, and may differ further, depending on your system configuration.

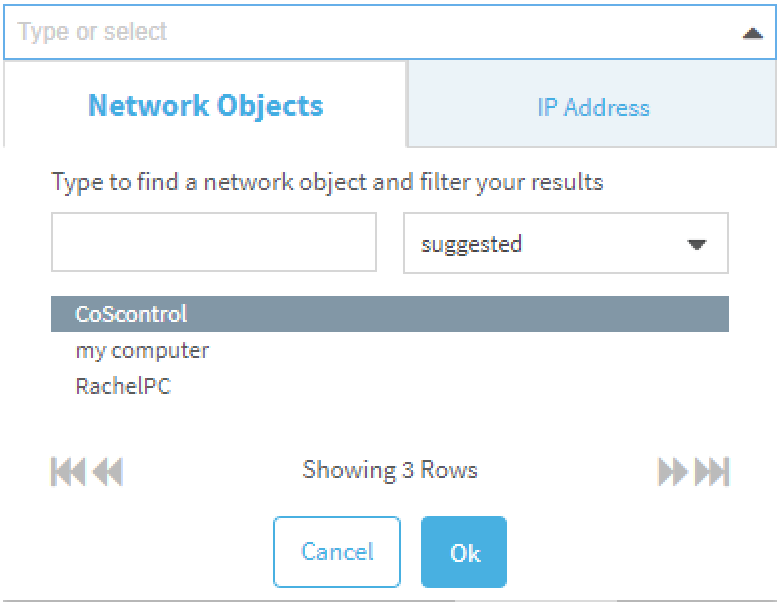
### Choose a source / destination for IPv4 traffic

In your change request form, do the following:

1. In the **Source** or **Destination** field, click ▼ .

   The wizard opens, displaying the **Network Objects** tab.

For example:



Type to find a network object and filter your results

suggested

CoScontrol
my computer
RachelPC

Showing 3 Rows

2. Do one of the following:

| | |
|---|---|
| **Select from a list of device objects or suggestions** | Do the following:<br>a. Click the **Network Objects** tab.<br>b. In the dropdown menu, select the type of network objects you'd like to view.<br>To search, enter any part of the source/destination's name in the search field (case insensitive).<br>All objects containing the string you entered are listed below the search.<br>c. Select an item from the list of suggestions or device objects listed. |
| **Enter a specific value** | Do the following:<br>a. Click the **IP Address** tab.<br>b. Enter the IP address, IP range, CIDR, or Netmask value you want to use as the source/destination. |

3. Click **OK**.

If you entered a value in the **IP Address** tab, the wizard validates the entered value.

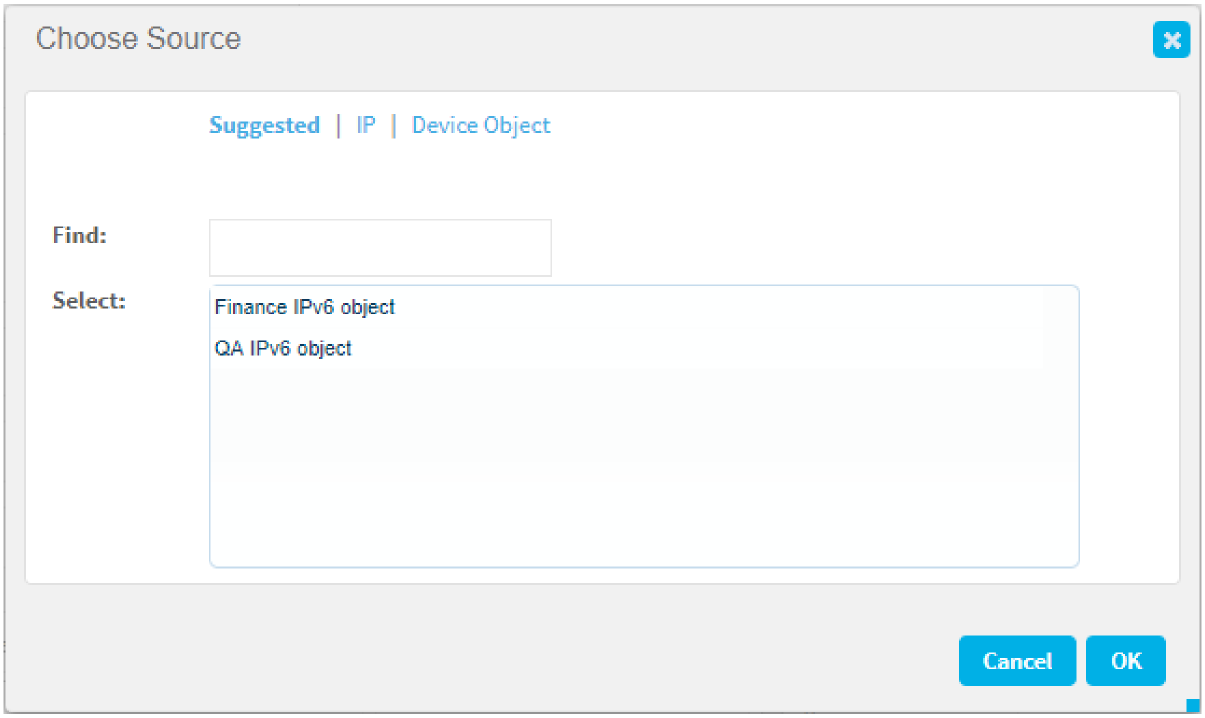
The selected source/destination is displayed in the **Source** or **Destination** field. For example, if you selected **my computer**, your computer's IP address is displayed.

### Choose a source / destination for IPv6 traffic

In your change request form, do the following:

1. Double-click in the **Source** or **Destination** field.

   The **Choose Source Wizard** or **Choose Destination Wizard** opens displaying the **Suggested** tab.



Choose Source

Suggested | IP | Device Object

Find:

Select:

Finance IPv6 object

QA IPv6 object

2. Do one of the following:

| | |
|---|---|
| **Select from a list of device objects or suggestions** | Do the following:<br>- To search for a source/destination, in the **Find** field, enter any part of the source/destination's name (case-insensitive).<br>- In the **Select** list, select the item you want to use as the source/destination. |
| **Enter a specific value** | Do the following:<br>a. Click the **IP** tab.<br>b. Do one of the following:<br>**Specify an IP address**. Click **IP** and enter your IP address.<br>**Specify an IP range.** Click **IP Range** and enter your IP range.<br>**Specify a network**. Click **CIDR** and enter your network value.<br>**Specify any IP address**. Click **Any**. This specifies an IP range **of 0.0.0.0-255.255.255.255.** |
| **Select from all device objects in AFA** | Do the following:<br>a. Click the **Device Object** tab.<br>b. To search for a device object, do the following:<br>○ In the **Search** dropdown list, select the device in which the object is located.<br>○ In the **For** field, enter any part of the object's name.<br>The **Select** list displays all source/destinations containing the string you entered.<br>To navigate between search result pages enter the page number you want to jump to in the **Page** field.<br>c. In the **Select** list, select the desired device object. |

3. Click **OK**.

If you entered a value in the **IP** tab, the wizard validates the entered value.

The selected source/destination is displayed in the **Source** or **Destination** field. For example, if you selected **my computer**, your computer's IP address is displayed.

## Choose Service wizard

The **Choose Service** wizard helps you specify a connection service in a change request.

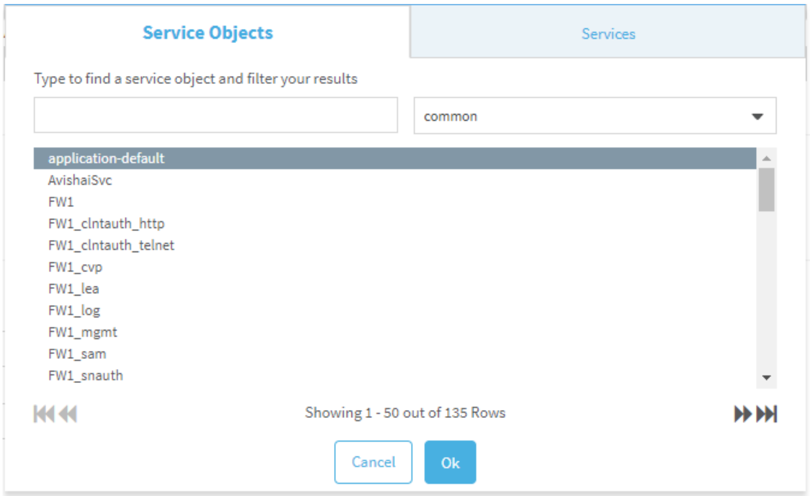
These wizards differ for IPv4 and IPv6 traffic, and may differ further, depending on your system configuration.

### Choose a service for IPv4 traffic

In your change request form, do the following:

1. In the **Service** field, click ▼.

   The **Choose Service Wizard** opens, displaying the **Service Objects** tab and **common** service objects.



Type to find a service object and filter your results

common

application-default
AvishaiSvc
FW1
FW1_clntauth_http
FW1_clntauth_telnet
FW1_cvp
FW1_lea
FW1_log
FW1_mgmt
FW1_sam
FW1_snauth

Showing 1 - 50 out of 135 Rows

2. Do one of the following:

| | |
|---|---|
| **Select the service from a list of services** | Do the following:<br>a. In the dropdown menu, select the type of service you want to view.<br>By default, only common service objects are displayed.<br>b. To search for a service object, enter any part of the object's name in the search field (case insensitive).<br>c. Select the service object you want to use from the list displayed. |
| **Specify a custom service** | Do the following:<br>a. Click the **Services** tab.<br>b. Enter the service in one of the following formats:<br>**protocol/port**, to indicate a single service.<br>**protocol/***, to indicate any port for the specified protocol<br>**protocol/port1-port2**, to indicate a range of ports for a specific protocol<br>*****, to indicate "any" service |

3. Click **OK**.

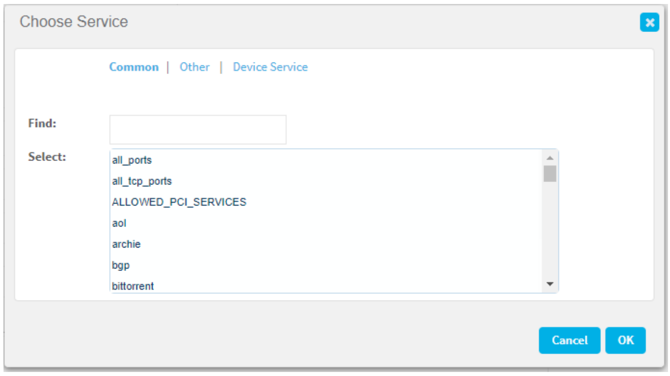
If you entered a custom service, the wizard validates the entered value. The selected service or appears in the **Service** field.

### Choose a service for IPv4 traffic

In your change request form, do the following:

1. Double-click in the **Service** field.

   The **Choose Service Wizard** opens displaying the **Common** tab.



Choose Service

Common | Other | Device Service

Find:

Select:

all_ports
all_tcp_ports
ALLOWED_PCI_SERVICES
aol
archie
bgp
bittorrent

2. Do one of the following:

| | |
|---|---|
| **Select the service from a list of services defined in AFA** | Do the following:<br>◦ To search for an service, in the **Find** field, enter any part of the object's name in the search field (case insensitive).<br>◦ In the **Select** list, select the service you want to use. |
| **Specify a custom service** | Do the following:<br>a. Click the **Other** tab.<br>b. In the **Protocol** area, select a specific protocol, or select **Any**.<br>c. In the **Port** area, do one of the following:<br>Select **Single** to specify a single destination port. Enter the port number.<br>Select **Range** to specify a destination port range. Enter the port range.<br>Select **Any** to specify any destination port. |

| | |
|---|---|
| **Select a service from a list of services defined on devices** | Do the following:<br>a. Click the **Device Service** tab.<br>b. In the **Search** area, select a device from the dropdown list.<br>c. To search for a specific service defined on the device, in the **For** field, enter any part of the service's name (case-insensitive), and then click **Go**.<br>d. In the **Select** list, select the desired service.<br>**Note:** This feature is only supported for service's whose protocol is TCP, UDP, or ICMP. If a service is selected with another protocol, the change request will not open. |

3. Click **OK**.

If you entered a port number or range, the wizard validates the entered value. The selected service appears in the **Service** field.

## Choose Application wizard

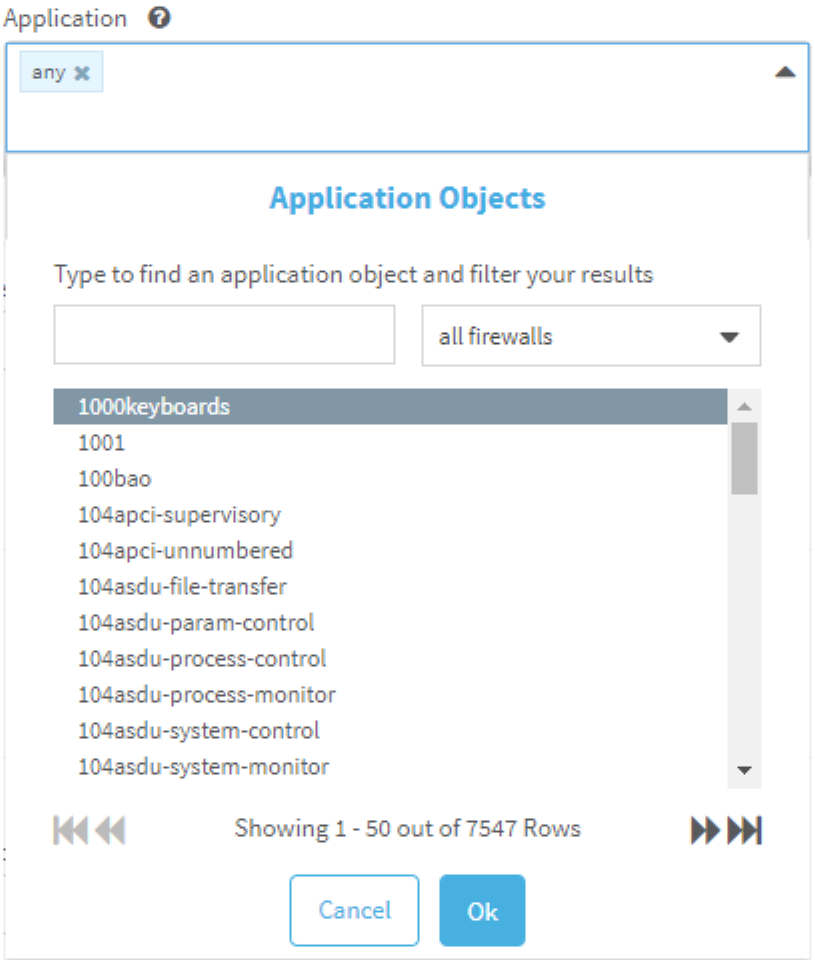
The **Choose Application** wizard helps you define an application for your change request.

This wizard appears depending on your system configuration, and only when there are Palo Alto devices defined in AFA.

### Do the following:

1. In your change request form, in the **Application** field, click ▼.

   The Application wizard is displayed.



Application

any

Application Objects

Type to find an application object and filter your results

all firewalls

1000keyboards
1001
100bao
104apci-supervisory
104apci-unnumbered
104asdu-file-transfer
104asdu-param-control
104asdu-process-control
104asdu-process-monitor
104asdu-system-control
104asdu-system-monitor

Showing 1 - 50 out of 7547 Rows

2. Select the application you want to use from the list of items displayed.

   Filter the items displayed by doing any of the following:

   - In the dropdown menu, select the device or device group on which the application is defined.
   - Search for an application by entering any part of the application's name in the field (case-insensitive).

3. Click **OK**.

The application appears in the **Application** field.

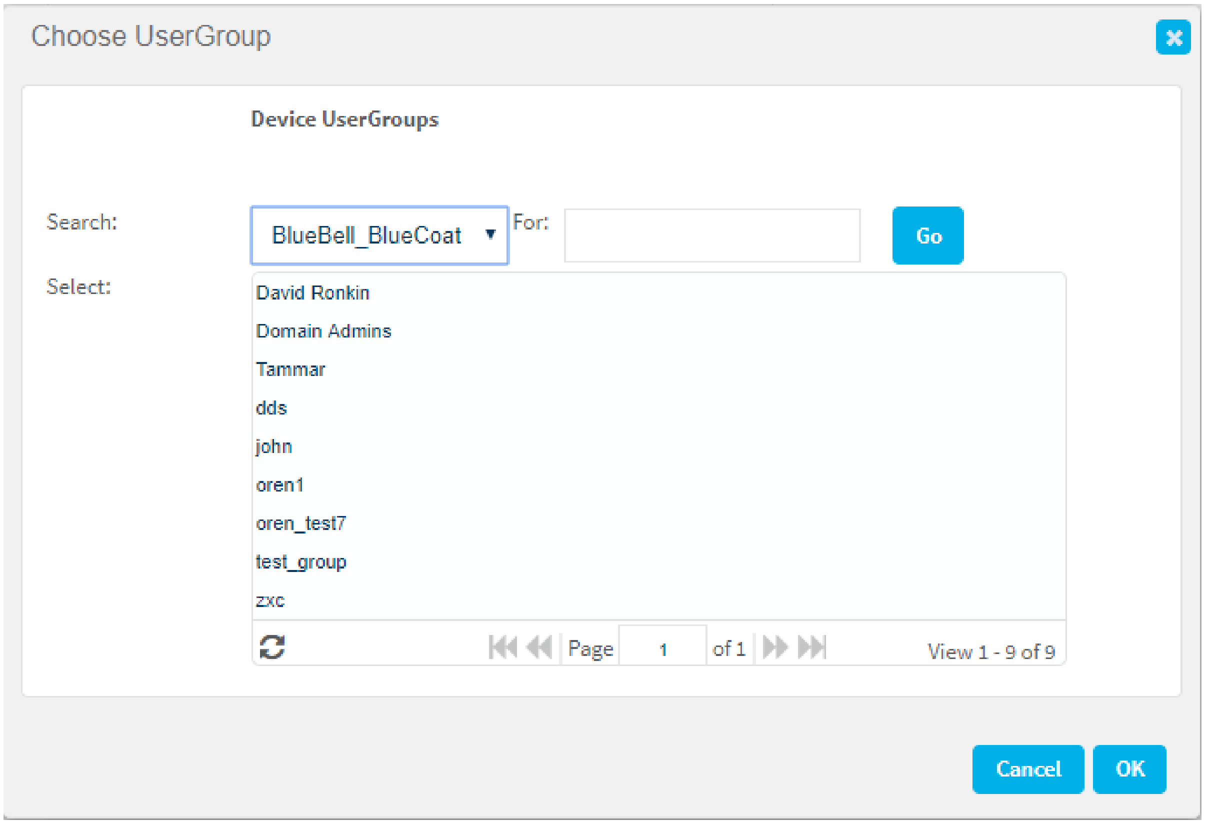
## Choose User Group wizard

The **Choose UserGroup** wizard helps you select a user group from all groups in a device's security policy, and is available for Web Filtering requests only.

### Do the following:

1. In your change request form, double-click in the **User Group** field.

   The **Choose User Group Wizard** opens.



Choose UserGroup

Device UserGroups

Search: BlueBell_BlueCoat For:

Select:

David Ronkin
Domain Admins
Tammar
dds
john
oren1
oren_test7
test_group
zxc

2. In the **Search** field, select the desired device.

   > **Note:** This field displays only Symantec Blue Coat device names.

   (Optional) To search for a user group, in the **For** field, type any part of the user group's name, and click **Go**. To navigate between search result pages, in the **Page** field, type the desired page number, then press **Enter**.

3. In the **Select** list, select the desired user group.
4. Click **OK**.

The selected user group is displayed in the **User Group** field.

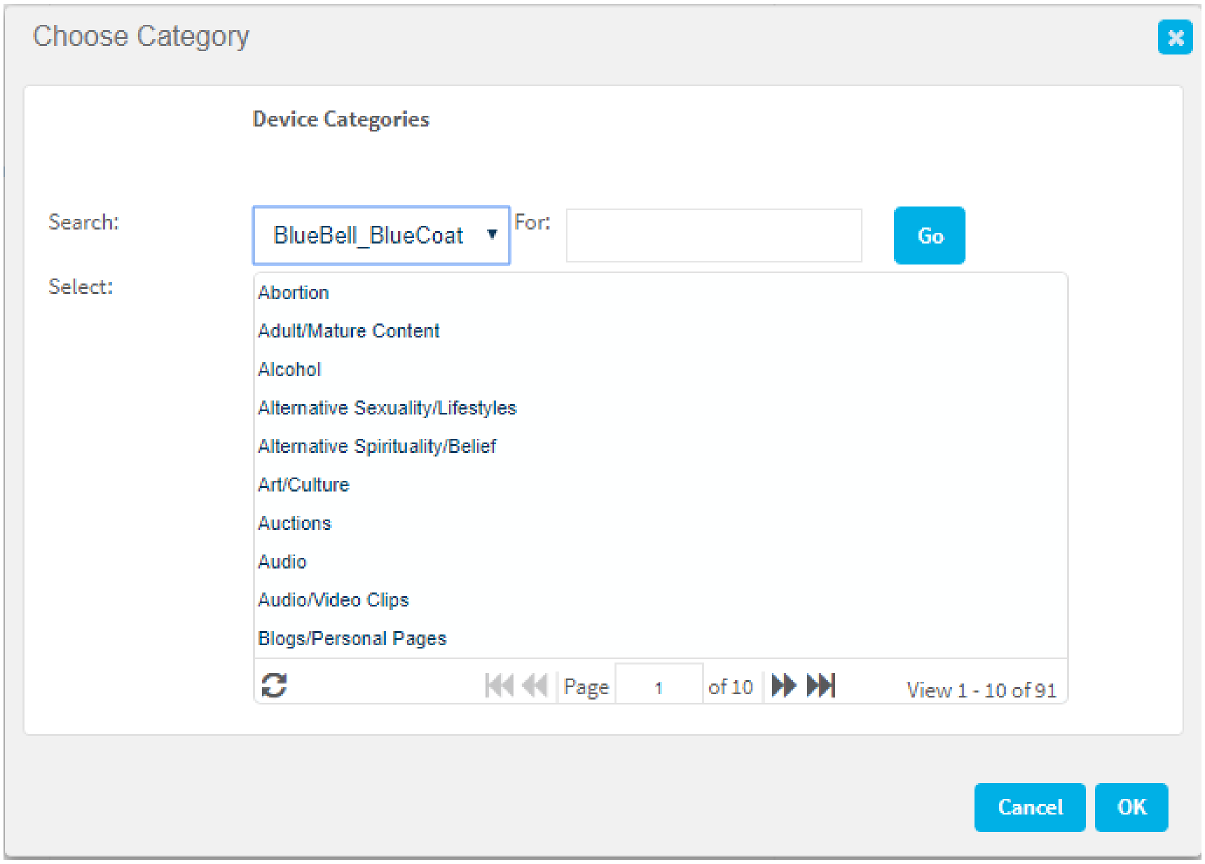
## Choose Category wizard

The **Choose Category Wizard** enables you to select a Web filtering category by selecting the category from a list of all categories that exist on a device.

### Do the following:

1. In your change request form, double-click in the **Category** field.

   The **Choose Category Wizard** opens.



Choose Category

Device Categories

Search: BlueBell_BlueCoat

For:

Select:

Abortion
Adult/Mature Content
Alcohol
Alternative Sexuality/Lifestyles
Alternative Spirituality/Belief
Art/Culture
Auctions
Audio
Audio/Video Clips
Blogs/Personal Pages

2. In the **Search** field, select the desired device.

> **Note:** This field displays only Symantec Blue Coat device names.

(Optional) To search for a category group, in the **For** field, type any part of the category's name, and click **Go**. To navigate between search result pages, in the **Page** field, type the desired page number, then press **Enter**.

3. In the **Select** list, select the desired category.
4. Click **OK**.

The selected category is displayed in the **Category** field.

## Select Devices wizard

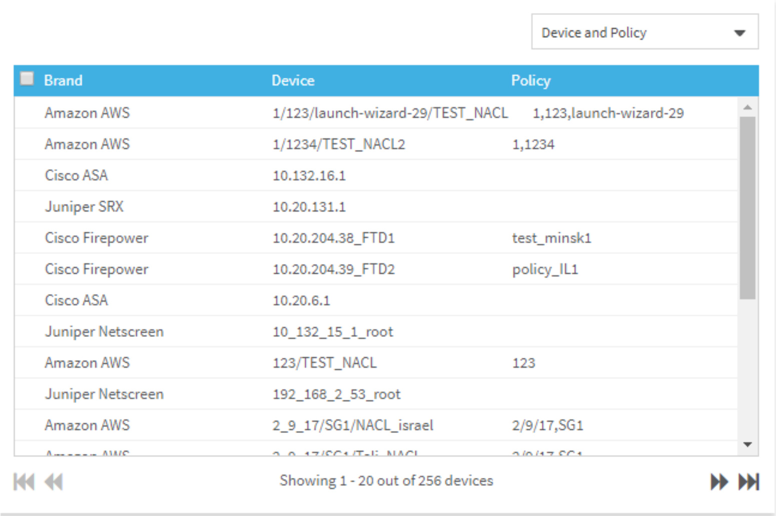
The Select Devices wizard enables you to quickly and easily select a single device or multiple devices.

> **Note:** For more details, see Amazon Web Services and Microsoft Azure "Devices".

### Do the following:

1. Click in a field to select a device.

   The Select Devices wizard appears.



| □ Brand | Device | Policy |
|---|---|---|
| Amazon AWS | 1/123/launch-wizard-29/TEST_NACL | 1,123,launch-wizard-29 |
| Amazon AWS | 1/1234/TEST_NACL2 | 1,1234 |
| Cisco ASA | 10.132.16.1 | |
| Juniper SRX | 10.20.131.1 | |
| Cisco Firepower | 10.20.204.38_FTD1 | test_minsk1 |
| Cisco Firepower | 10.20.204.39_FTD2 | policy_IL1 |
| Cisco ASA | 10.20.6.1 | |
| Juniper Netscreen | 10_132_15_1_root | |
| Amazon AWS | 123/TEST_NACL | 123 |
| Juniper Netscreen | 192_168_2_53_root | |
| Amazon AWS | 2_9_17/SG1/NACL_israel | 2/9/17,SG1 |
| Amazon AWS | 2_9_17/SG1/Tali_NACL | 2/9/17,SG1 |

Showing 1 - 20 out of 256 devices

2. Select a device by doing one of the following:

    - **Click a device.** Click the arrows at the bottom of the dialog to page through the list to find the one you want.

    - **Search for a device**. Do the following:

        a. In the **Filter By** dropdown, select the filter criteria you want to use.

        The following fields are available for filtering in the device selection wizard:

        | | |
        |---|---|
        | **Name and Policy** | Filter by both the device name and policy name. |
        | **Name** | Filter by the device name. |
        | **Policy** | Filter by the policy name. |
        | **Brand** | Filter by the brand name. |
        | **Selected** | Show only selected devices. |

        b. In the textbox, enter your search criteria. The filter runs as you enter text.

        Click the arrow buttons at the bottom of the dialog to page through the list. Click a device to select it.

        > **Tip:** Select all filtered devices by selecting the checkbox to the left of the **Brand** column. This is only supported for scenarios when multiple device selection is supported.

3. To remove a device from the selected devices, click **x**.

4. Click outside of the wizard to add the selected devices to the field.

    The selected devices are added to the field.

### Amazon Web Services and Microsoft Azure "Devices"

FireFlow handles Amazon Web Services (AWS) and Microsoft Azure "devices" as follows:

- The "device" will always be the security "security set". A security set is a group of instances/VMs with the exact same security group(s) and network ACLs applied to them. Therefore, every instance/VM in a security set has identical security policies.
- When modifying traffic for a security set, FireFlow automatically selects the optimal security group to modify in **Initial Planning**. The security group is selected based on rule capacity and the lowest number of affected instances/VMs.

  In Initial Planning, you can manually change the security group to modify, just like you can manually change which devices are relevant to modify for a change request. For more details, see Initial planning.

# Initial planning

**Relevant for: Network operators**

This section describes how network operators can perform initial planning for traffic change requests or Web filtering change requests.

Initial planning includes defining the requested change's details, determining whether the change is necessary, and specifying the affected devices on which the requested change should be implemented.

If you select multiple devices or policies, FireFlow creates multiple requests with the same details for each device or policy.

**Tip:** We recommend enabling real-time monitoring before planning changes to ensure that the latest data is used to plan the change.

**Note:** A change request's stage is indicated by the Change Request Lifecycle Status Bar. For details, see View change requests.

▶ Auto-Confirm Devices in the Plan Stage: Watch to learn how to automatically confirm devices in the Plan stage of a change request.

## Plan traffic changes

Usually, traffic changes are requested to allow traffic, and FireFlow detects the devices blocking the specified traffic. In the event that a change includes a request to drop traffic, FireFlow detects the devices allowing the specified traffic. The following procedure relates mainly to requests for allowing traffic, but it is also relevant to requests for blocking traffic.

## Do the following:

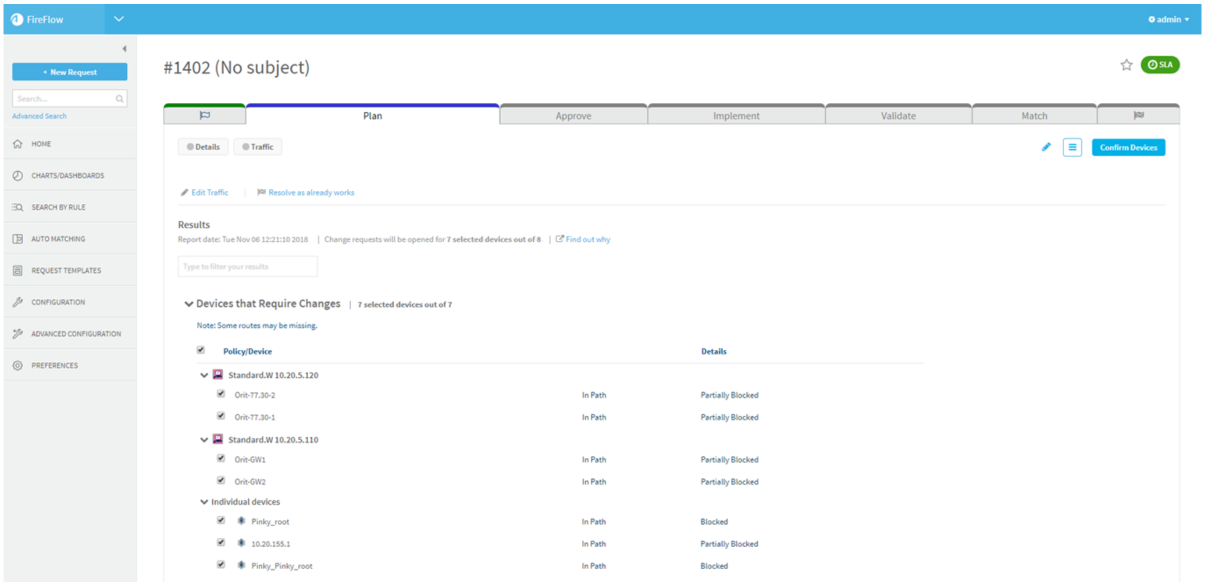
1. View the change request. For details, see View change requests.
2. If you were not assigned this change request, click **Take Ownership** at the top of the page.

   You are now the change request's owner.

   > **Note:** This button only appears if you were *not* assigned this change request.

3. If the Initial Plan results are outdated, recalculate the initial plan by clicking **Recalculate Initial Plan**.

   The change request appears displaying its initial plan **Results**.

   #1402 (No subject)

   Results

   Report date: Tue Nov 06 12:21:10 2018 | Change requests will be opened for **7 selected devices out of 8** | Find out why

   Devices that Require Changes | **7 selected devices out of 7**

   Note: Some routes may be missing.

   | ☑ Policy/Device | | Details |
   |---|---|---|
   | Standard.W 10.20.5.120 | | |
   | ☑ Orit-77.30-2 | In Path | Partially Blocked |
   | ☑ Orit-77.30-1 | In Path | Partially Blocked |
   | Standard.W 10.20.5.110 | | |
   | ☑ Orit-GW1 | In Path | Partially Blocked |
   | ☑ Orit-GW2 | In Path | Partially Blocked |
   | Individual devices | | |
   | ☑ Pinky_root | In Path | Blocked |
   | ☑ 10.20.155.1 | In Path | Partially Blocked |
   | ☑ Pinky_Pinky_root | In Path | Blocked |

   In the **Results** area, each device or policy relevant for the change request appears. The **Details** column indicates whether the specified traffic is blocked or partially allowed. If the change request includes both "Allow" and "Drop" actions, the connectivity details appear in the **Traffic to be allowed** and **Traffic to be blocked** columns.

**Note:** If initial plan failed on one or more devices, a notification appears with a link to find out why.

### Policy-based change requests

FireFlow uses policy-based change requests for Palo Alto Networks Panorama, Check Point, Fortinet Fortimanager, and Junos Space Security Director. During initial planning, FireFlow will suggest relevant policies (the policies on the relevant devices).

- FireFlow will always recommend the highest level policy under the global policy.
- Additionally, FireFlow will recommend installing the change on all devices with the policy.

If desired, you can set FireFlow to only install changes on the relevant devices or simply to always use device-based change requests.

### AWS and Azure "device" handling

FireFlow does not support AWS for drop traffic change requests.

For more details, see Amazon Web Services and Microsoft Azure "Devices".

### Disaster recovery devices

If FireFlow suggests (or you manually select) devices that are a part of a Disaster Recovery (DR) set, an additional column appears, indicating which devices were found in path and which were added because of their inclusion in the DR set.

### NAT traffic changes

If the change request includes traffic with NAT, the **Results** table includes a **NAT** column to indicate which devices have at least one NAT rule. In addition, the **NAT Settings** link appears above the results area, allowing you to specify when translation is done by the device.

By default, if the change request already works, FireFlow will automatically close it. However, if handling of NAT-only traffic changes is configured, FireFlow will keep the change request open and use the NAT values in the risk check and work order.

#### Palo Alto Networks Panorama devices

For Palo Alto Networks Panorama devices, FireFlow will always recommend changing the lowest device group. If a higher level device group blocks the traffic the change request is attempting to allow, the traffic will still not be allowed after the work order is implemented. To allow the traffic you must manually change the higher level device group.

#### Cisco Firepower devices

For Cisco Firepower devices, FireFlow will always recommend implementing changes at the lowest policy level.

4. Do any of the following as needed:

   #### Modify selected devices/policies

   If desired, modify the selected devices/policies, by doing one or more of the following:

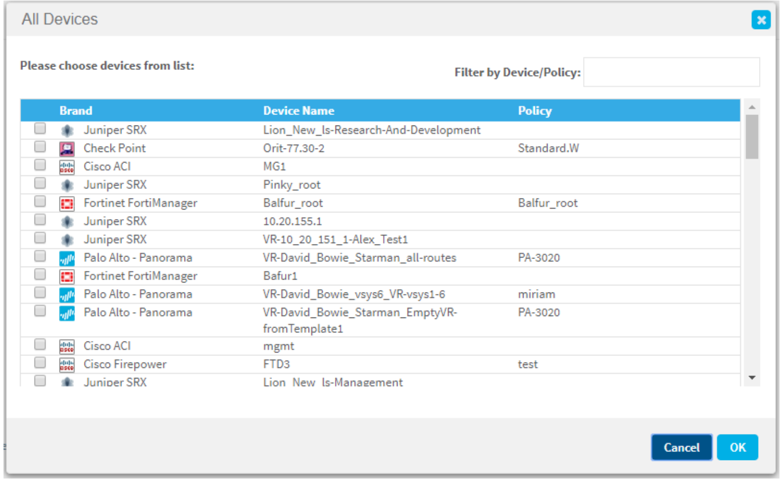
   - In the **Results** area, select the devices on which to implement the change.

     If more than one device or policy is selected, a request will be created for each device or policy.

   - To specify a device that does not appear in the **Results** area, do the following:

     a. Click **Add More Devices**.

        The **All Devices** dialog box appears.



All Devices

Please choose devices from list:

Filter by Device/Policy:

| | Brand | Device Name | Policy |
|---|---|---|---|
| □ | Juniper SRX | Lion_New_ls-Research-And-Development | |
| □ | Check Point | Orit-77.30-2 | Standard.W |
| □ | Cisco ACI | MG1 | |
| □ | Juniper SRX | Pinky_root | |
| □ | Fortinet FortiManager | Balfur_root | Balfur_root |
| □ | Juniper SRX | 10.20.155.1 | |
| □ | Juniper SRX | VR-10_20_151_1-Alex_Test1 | |
| □ | Palo Alto - Panorama | VR-David_Bowie_Starman_all-routes | PA-3020 |
| □ | Fortinet FortiManager | Bafur1 | |
| □ | Palo Alto - Panorama | VR-David_Bowie_vsys6_VR-vsys1-6 | miriam |
| □ | Palo Alto - Panorama | VR-David_Bowie_Starman_EmptyVR-fromTemplate1 | PA-3020 |
| □ | Cisco ACI | mgmt | |
| □ | Cisco Firepower | FTD3 | test |
| □ | Juniper SRX | Lion_New_ls-Management | |

b. Select the desired device(s) for the change request by doing the following:

   - For all device brands other than AWS or Azure, select the check box for the desired device(s).
   - For AWS or Azure, do the following:

     i. Select the desired security set(s).

     ii. In the **Policy Name** column, select the security group.

        If multiple devices or policies are selected, a request will be created for each device or policy.

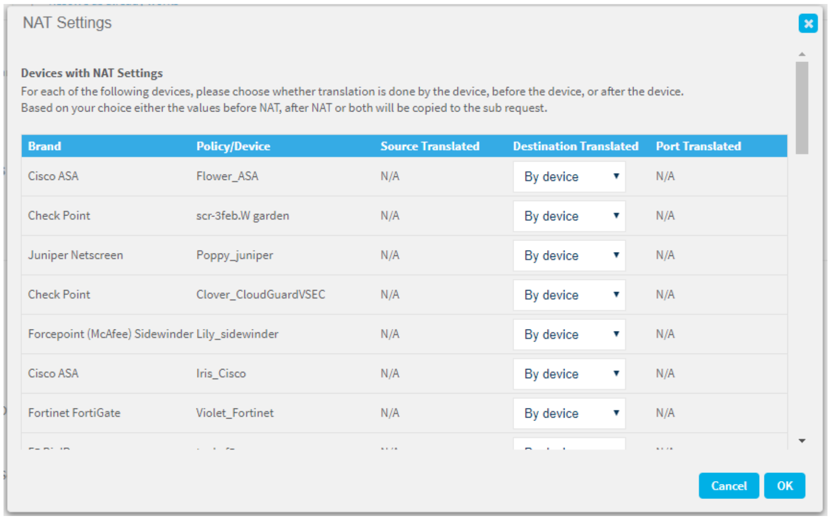
     iii. Click **OK**.

### Edit NAT settings

For change requests including traffic with NAT, do the following to edit the NAT settings that FireFlow will use throughout the change request's lifecycle:

a. Click **NAT Settings**.

   The **NAT Settings** window is displayed.



NAT Settings

**Devices with NAT Settings**

For each of the following devices, please choose whether translation is done by the device, before the device, or after the device.
Based on your choice either the values before NAT, after NAT or both will be copied to the sub request.

| Brand | Policy/Device | Source Translated | Destination Translated | Port Translated |
|---|---|---|---|---|
| Cisco ASA | Flower_ASA | N/A | By device ▾ | N/A |
| Check Point | scr-3feb.W garden | N/A | By device ▾ | N/A |
| Juniper Netscreen | Poppy_juniper | N/A | By device ▾ | N/A |
| Check Point | Clover_CloudGuardVSEC | N/A | By device ▾ | N/A |
| Forcepoint (McAfee) Sidewinder | Lily_sidewinder | N/A | By device ▾ | N/A |
| Cisco ASA | Iris_Cisco | N/A | By device ▾ | N/A |
| Fortinet FortiGate | Violet_Fortinet | N/A | By device ▾ | N/A |

b. For each device with NAT settings (that is, the device has at least one NAT rule), select where the source, destination or port was translated:

- **Before device:** The translation is performed before this device.
- **By device:** The translation is performed by this device.
- **After device:** The translation is performed after this device.

c. For each device without NAT settings, select where the source, destination or port was translated:

- **Before device:** The translation is performed before this device.
- **After device:** The translation is performed after this device.

d. Click **OK**.

> **Note:** If you define a new device in AFA that performs NAT or you add a NAT rule to a device that previously had no NAT rules, you must analyze the device before FireFlow can provide accurate default values.

### Modify traffic

If you want to modify the traffic, do the following:

a. In the **Traffic** area, modify the traffic fields as desired. For details, see [Change request field references](#).

b. Click **Save and Recalculate**.

   FireFlow indicates the differences between the traffic and the installed policy.

c. Click **Start Initial Plan**.

   FireFlow recalculates the initial plan, based on the new traffic.

### Recalculate initial planning on a different device group

Do the following:

a. In the **Already works** area, select the desired device group in the drop-down menu.

b. Click **Save and Recalculate**.

   FireFlow examines the selected devices' latest installed policies.

c. If the requested traffic is already allowed, click the **Resolve as already works** link at the top of the page.

### Contact the requestor

If the traffic details are incomplete, contact the requestor for additional details. For details, see [Respond to change requests](#).

### View a detailed report about affected devices

To view a detailed report on the device(s) that will be affected by the requested change, at the top of the results area, click Find out why .

The traffic simulation query report provided by AFA opens in a new window, including all of the relevant devices for the change request. You can drill down to view the relevant device rules in the affected device(s).

> **Note:** This report (not including the network map) is also available when viewing the change request. For more details, see View change requests.

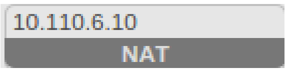
5. Click **Confirm Devices**.

   If multiple devices were selected, FireFlow creates a change request for each device and policy (sub-requests).

   The change request moves to the Approve stage.

> **Note:** If desired, you can enable asynchronous sub-request creation. This enables you to complete other tasks while FireFlow creates sub-requests for each device or policy relevant to the change request.

### NAT traffic changes

If the initial plan identified that NAT rules are already in place and that NAT is taking place in one or more devices in the path of the requested traffic, then the traffic of devices that are located after the NAT took place in the path will be modified accordingly. You will see the following label next to the traffic of that device to indicate that NAT took place .

For change requests requesting traffic with NAT, requests will include only the relevant addresses. A request for a device that is located before NAT will only include the before translation address, a request for a device that is located after NAT will only include the after translation address, and the request for a device that performs NAT will include the before translation and after translation addresses.

## Plan web filtering changes

Here is a description of how to plan Web Filtering changes.

## Do the following:

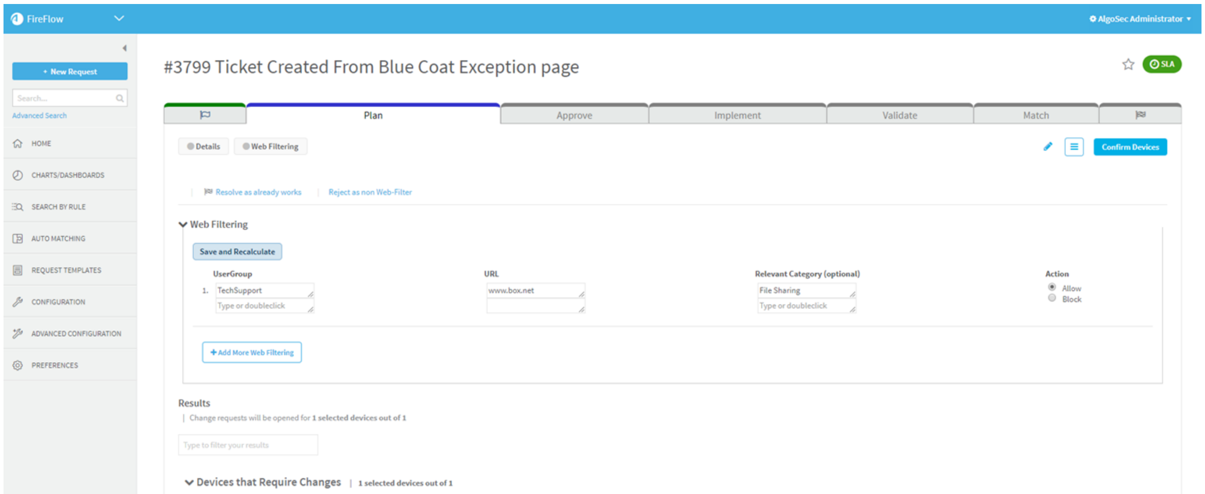
1. View the change request. For details, see View change requests.
2. If you were not assigned this change request, click **Take Ownership** at the top of the page.

   You are now the change request's owner.

   > **Note:** This button only appears if you were *not* assigned this change request.

3. Click **Initial Plan**.

   The **Web Filtering** and **Results** areas appear.

   #3799 Ticket Created From Blue Coat Exception page

   Web Filtering

   | | UserGroup | URL | Relevant Category (optional) | Action |
   |---|---|---|---|---|
   | 1. | TechSupport | www.box.net | File Sharing | ● Allow<br>○ Block |
   | | Type or doubleclick | | Type or doubleclick | |

   Results

   Change requests will be opened for **1 selected devices out of 1**

   Devices that Require Changes | 1 selected devices out of 1

4. In the **Results** area, specify the devices that are relevant to this request, by doing any of the following:

   - Select the check box next to its name to select an individual device in the list.
   - Select the check box on the heading line to select all devices in the list.
   - Clear the check box on the heading line to select none of the devices in the list.

   If more than one device or policy is selected, a request will be created for each device or policy.

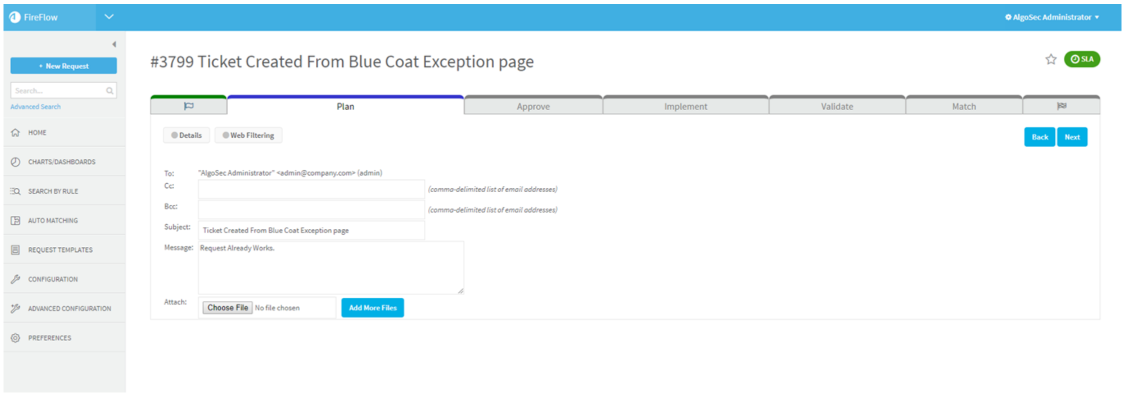
5. If the change request already works, do the following:

a. Click **Resolve as already works**.

A confirmation message appears.

b. Click **OK**.

The **Request Already Works** message page appears.



#3799 Ticket Created From Blue Coat Exception page

To: "AlgoSec Administrator" <admin@company.com> (admin)

Cc: (comma-delimited list of email addresses)

Bcc: (comma-delimited list of email addresses)

Subject: Ticket Created From Blue Coat Exception page

Message: Request Already Works.

Attach: No file chosen

c. Configure the fields as needed. For details, see Respond to change requests.

d. Click **Next**.

The change request is resolved.

6. If the problem that prompted the requestor to submit this change request was not caused by Web Filtering, do the following:

   a. Click **Reject as non Web-Filter**.

   A confirmation message appears.

   b. Click **OK**.

   The change request is rejected and closed.

7. If you are not satisfied with the results and want to modify the Web filtering details or the device group, in the **Modify Traffic** area, modify the Web filtering fields as desired.

   For more details, see Change request field references.

8. Click **Next**.

The change request proceeds to the Approve stage.

If you have the network operations role only (and not the information security role), the **Home** page is displayed.

## Select devices manually

Network operation users working with IPv6 or multicast traffic change requests may need to select devices manually.

If multiple devices or policies are chosen, FireFlow creates a request with the same technical details for each device or policy.

**Tip:** Even if the user who submitted the change request specified devices, this action allows the privileged user to modify the selected devices.

**Note:** Only Cisco IOS/ASA devices are supported for IPv6 workflows. All types of Cisco devices are supported for Multicast workflow.

### Do the following:

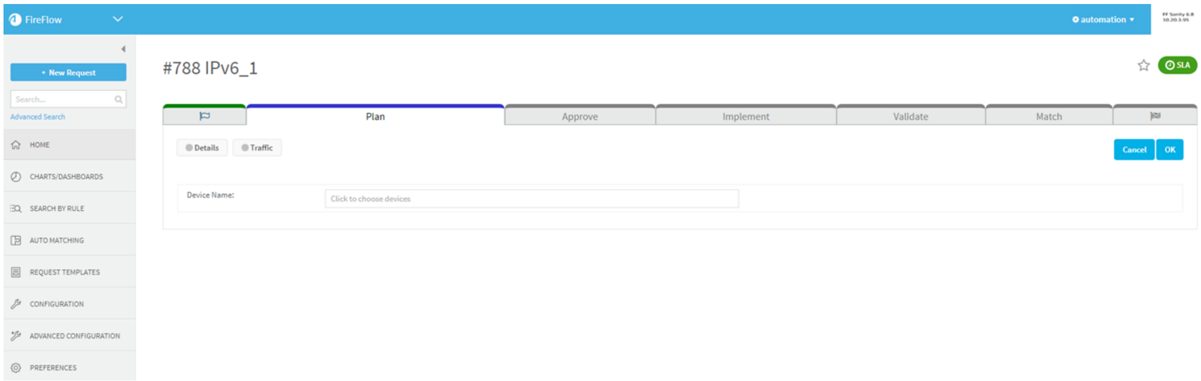
1. View the change request. For more details, see View change requests.
2. If you were not assigned this change request, click **Take Ownership** at the top of the page.

   You are now the change request's owner.

   **Note:** This button only appears if you were *not* assigned this change request.

3. At the top of the page, click **Choose Devices**.

   The **Device Name** field appears.



4. Click in the **Device Name** field.

   The Select Devices Wizard appears. For details, see Change request wizards.

5. Click **OK**.

# Approve planned changes

**Relevant for: Privileged users**

This topic describes the procedures you may perform during the a change request's **Approve** stage.

> **Note:** At several points, you may need to notify requestors about updates made.
>
> For details, see Manage requestor notifications.

## Find affected rules

This procedure explains how information security users can find device rules that are affected by a change request.

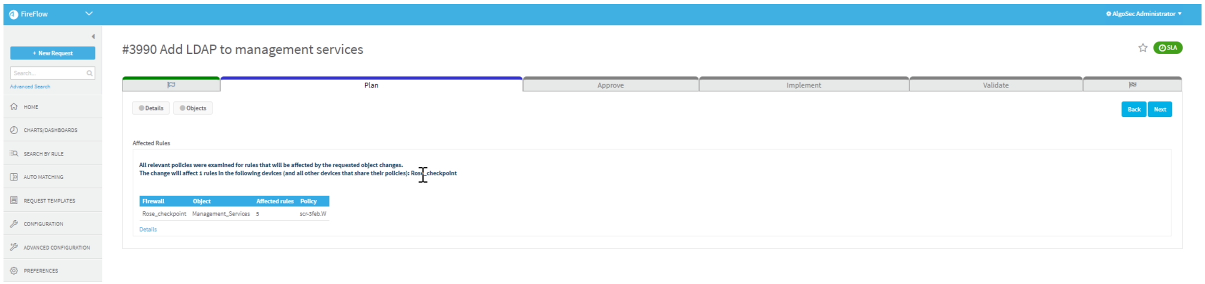
This may be performed as part of the Plan or Approve stage, depending on whether the change request is for single or multiple devices.

> **Note:** To determine a change request's stage, view the change request. The stage is indicated by the Change Request Lifecycle Status Bar. For details, see View change requests.

### Do the following:

1. View the change request. For details, see View change requests.
2. Do one of the following:
    - For single device object change requests, at the top of the page, click **Find Affected Rules**.
    - For multi-device object change requests, click **Find Affected Rules** for every sub request.

   The **Affected Rules** page appears displaying the number of device rules affected, as well as the affected rules per object.



#3990 Add LDAP to management services

Affected Rules

All relevant policies were examined for rules that will be affected by the requested object changes.
The change will affect 1 rules in the following devices (and all other devices that share their policies): Rose_checkpoint

| Firewall | Object | Affected rules | Policy |
|---|---|---|---|
| Rose_checkpoint | Management_Services | 5 | scr-3feb.W |

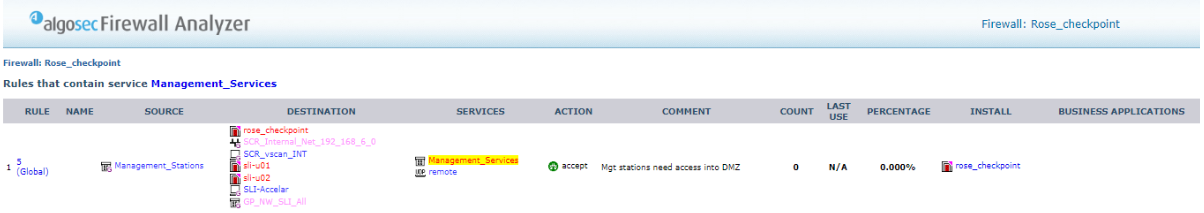
Details

**Note:** For Check Point devices, FireFlow finds affected rules on all devices where the object exists. Specifically, object change requests for objects defined on the CMA show affected rules on all policies of devices below that CMA, and object change requests for objects defined on the MDSM show affected rules on all policies of devices below any of the CMAs.

For Multi Device Object Change requests, the **Affected Rules** area displays full details about the rules.

3. To view the affected rules' details when using the single device object change workflow, in the **Affected Rules** area, click the **Details** link.

   A window opens displaying the rules' details.



Firewall: Rose_checkpoint

Rules that contain service Management_Services

| RULE | NAME | SOURCE | DESTINATION | SERVICES | ACTION | COMMENT | COUNT | LAST USE | PERCENTAGE | INSTALL | BUSINESS APPLICATIONS |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 5<br>(Global) | Management_Stations | rose_checkpoint<br>SCR_Internal_Net_192_168_6_0<br>SCR_vscan_INT<br>sli-u01<br>sli-u02<br>SLI-Accelar<br>GP_NW_SLI_All | Management_Services<br>remote | accept | Mgt stations need access into DMZ | 0 | N/A | 0.000% | rose_checkpoint | |

- Yellow highlighting indicates which objects contain the object(s) relevant to the change request.
- Light-blue highlighting indicates where an object slated to be deleted will be replaced by "Any". Examine rules with objects highlighted in light-blue to prevent security holes.

> **Note:** Light-blue highlighting is only relevant when deleting objects from Check Point devices.

4. In the **Affected Rules** page, click **Next**.

To continue with the change request, see Approve, reject, or return to planning.

# Certify or plan traffic removal

Once you have received responses from the related change requestors, you must decide whether to certify the Allow traffic or plan its removal.

This topic describes how network operation users can certify or plan traffic removal for recertification requests in the Approve stage.

> **Note:** To determine a change request's stage, view the change request. The stage is indicated by the Change Request Lifecycle Status Bar. For details, see View change requests.

## Do one of the following:

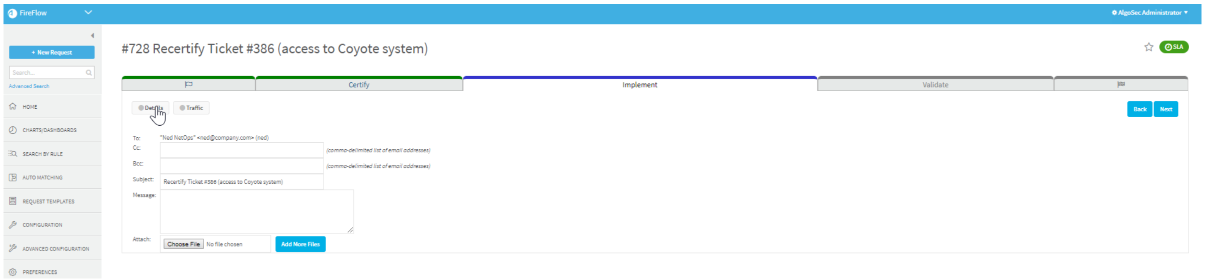
### Certify traffic

Certify the Allow traffic if the related change requestors' responses indicate that the Allow traffic should not be removed.

1. View the change request. For details, see View change requests.
2. Click ≡ , and then click **Traffic is Needed**.

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

   The Certify Change Request page is displayed.



#728 Recertify Ticket #386 (access to Coyote system)

To: "Ned NetOps" <ned@company.com> (ned)

Cc: (comma-delimited list of email addresses)

Bcc: (comma-delimited list of email addresses)

Subject: Recertify Ticket #386 (access to Coyote system)

Message:

Attach: No file chosen

4. Complete the fields as needed. For details, see Respond to change requests.
5. Click **Next**.

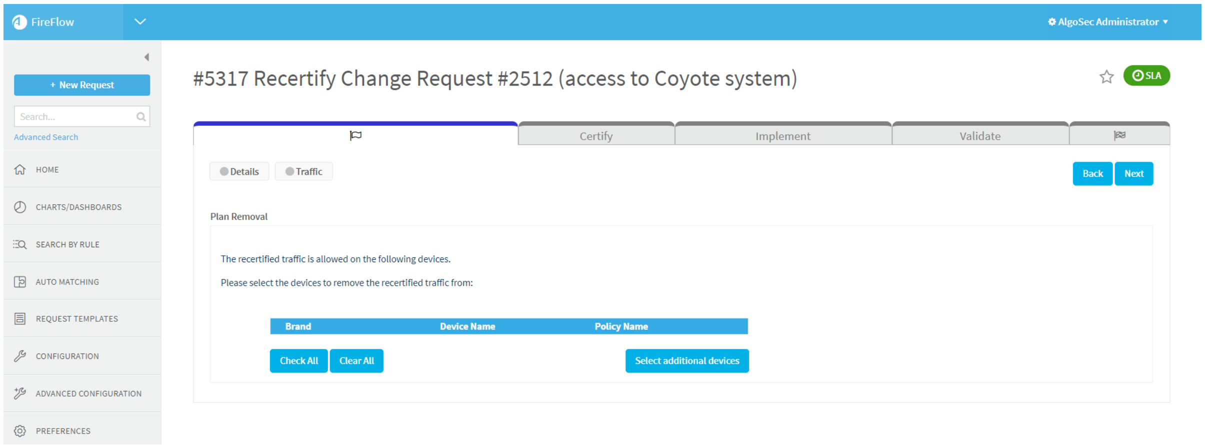
The email message is sent to the requestor, the change request is resolved, and the HOME page appears.

### Plan traffic removal

Plan traffic removal when the related change requestors' responses indicate that the Allow traffic should be removed.

1. View the change request. For details, see View change requests.
2. Click ☰ , and then click **Plan Removal**.

   The Plan Removal page appears displaying a list of devices on which the traffic is allowed.



#5317 Recertify Change Request #2512 (access to Coyote system)

Plan Removal

The recertified traffic is allowed on the following devices.

Please select the devices to remove the recertified traffic from:

| Brand | Device Name | Policy Name |
|---|---|---|

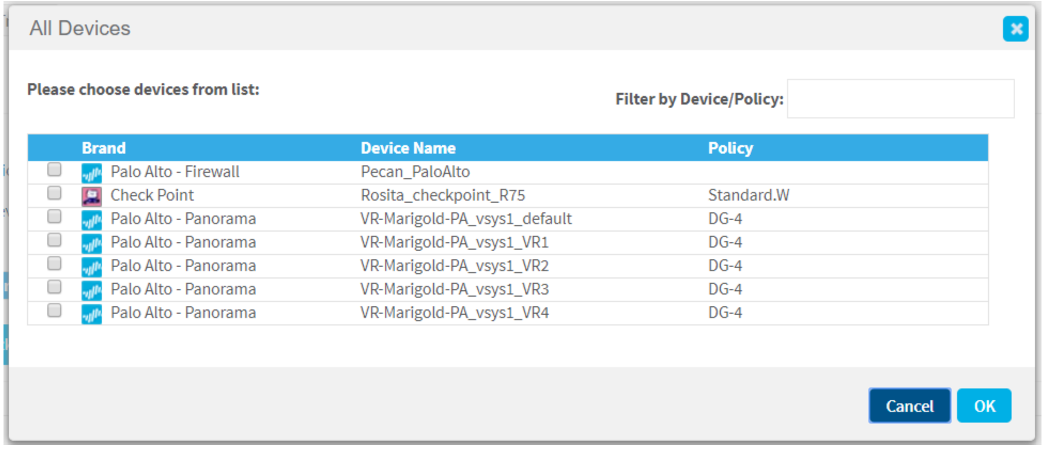
3. Specify the devices from which the Allow traffic should be removed, by doing any of

the following:

- To select an individual device in the list, select the check box next to its name.
- Click **Check All** to select all devices in the list.
- Click **Clear All** to select none of the devices in the list.
- To specify additional devices that are not listed, do the following:

  a. Click **Select additional devices**.

     The **All Devices** dialog box opens with a list of all devices in the FireFlow system.



All Devices

Please choose devices from list:

Filter by Device/Policy:

| | Brand | Device Name | Policy |
|---|---|---|---|
| □ | Palo Alto - Firewall | Pecan_PaloAlto | |
| □ | Check Point | Rosita_checkpoint_R75 | Standard.W |
| □ | Palo Alto - Panorama | VR-Marigold-PA_vsys1_default | DG-4 |
| □ | Palo Alto - Panorama | VR-Marigold-PA_vsys1_VR1 | DG-4 |
| □ | Palo Alto - Panorama | VR-Marigold-PA_vsys1_VR2 | DG-4 |
| □ | Palo Alto - Panorama | VR-Marigold-PA_vsys1_VR3 | DG-4 |
| □ | Palo Alto - Panorama | VR-Marigold-PA_vsys1_VR4 | DG-4 |

  b. Select the check boxes next to the desired device(s).

  c. Click **OK**.

     The selected devices appear in the list of devices from which to remove the Allow traffic, with an asterisk next to their name.

  d. Click **Next**.

     The recertification request proceeds to the Implement stage.

A request is opened for each of the selected devices.

## Perform a manual risk check

This section explains how information security users can perform a manual risk check for generic change requests in the **Approve** stage.

> **Note:** To determine a change request's stage, view the change request. The stage is indicated by the Change Request Lifecycle Status Bar. For details, see View change requests.

After a generic change request has been created, it starts the Approve stage of the FireFlow change request lifecycle. In this stage, you perform a manual check for risks entailed in implementing the requested change.

You must then decide whether to return the change request to the Plan stage for further planning, reject and close the change request, or approve it.

### Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click **Manual Check**.

   A confirmation message appears.
3. Click **OK**.
4. Examine the change request, and determine whether implementing it would involve risks.

## Approve, reject, or return to planning

This topic explains network operation or information security users can approve, reject, or return a change request to the **Plan** stage.

> **Note:** To determine a change request's stage, view the change request. The stage is indicated by the Change Request Lifecycle Status Bar. For details, see View change requests.

## Request handling per request type

The following table describes how you might want to handle requests of different types at the Approve stage in your workflow.

| Change request type | Description |
|---|---|
| **Object change requests, including multi-device**<br>**Traffic change requests with drop actions only** | When working with an object change request or a traffic change request with only "Drop" action(s), once you have examined the affected rules results or notified requestors of related change requests, you must decide whether to:<br>• Return the change request to the Plan stage for further planning<br>• Reject and close the change request<br>• Approve the change request |
| **Traffic change requests with an allow action** | When working with a traffic change request with an "Allow" action (with the exception of IPv6 traffic), you must examine the risk check results before you approve the change request.<br>Examining the risk check will:<br>• Follow initial planning if the change request you are working with has only "Allow" actions<br>• Follow notifying requestors of related change requests if the change request you are working with also has "Drop" action(s)<br>After you have examined the risks, you must decide whether to:<br>• Return the change request to the Plan stage for further planning<br>• Reject and close the change request<br>• Approve the change request |
| **IPv6 traffic change requests** | When working with IPv6 traffic change requests you must decide whether to:<br>• Reject and close the change request<br>• Approve the change request |

| Change request type | Description |
|---|---|
| **Rule removal requests** | When working with a rule removal request, once you have received responses from the related change requestors, you must decide whether to:<br>• Reject and close the change request<br>• Approve the change request |
| **Rule modification requests** | When working with a rule modification request, you must first decide whether to modify the change request. If you decide to do so, you must examine the risk check results.<br>You must then decide whether to:<br>• Reject and close the change request<br>• Approve the change request |
| **Web filtering change request** | When working with a Web filtering change request, you must decide whether to:<br>• Return the change request to the Plan stage<br>• Approve the change request |

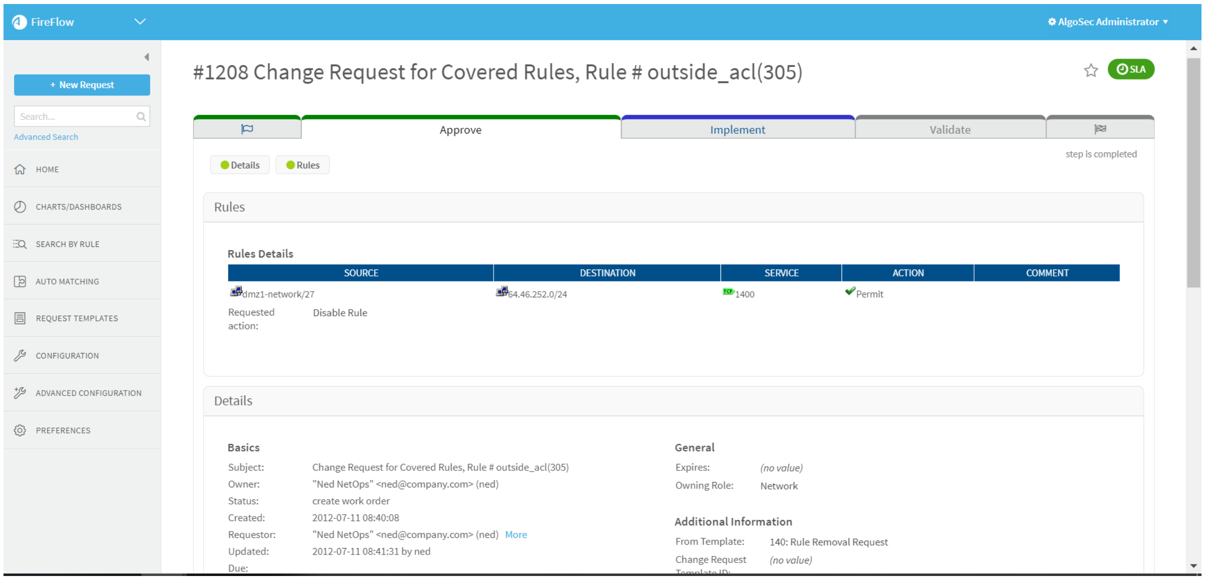
Do any of the following:

### Modify a rule modification request

This procedure describes how to modify a rule modification request.

1. View the change request. For details, see View change requests.
2. At the top of the page, click ✏.

   The details of the rule modification request are displayed in an editable format.



#1208 Change Request for Covered Rules, Rule # outside_acl(305)

Rules

Rules Details

| SOURCE | DESTINATION | SERVICE | ACTION | COMMENT |
|---|---|---|---|---|
| dmz1-network/27 | 64.46.252.0/24 | TCP 1400 | ✓ Permit | |

Requested action: Disable Rule

Details

Basics

Subject: Change Request for Covered Rules, Rule # outside_acl(305)
Owner: "Ned NetOps" <ned@company.com> (ned)
Status: create work order
Created: 2012-07-11 08:40:08
Requestor: "Ned NetOps" <ned@company.com> (ned) More
Updated: 2012-07-11 08:41:31 by ned
Due:

General

Expires: *(no value)*
Owning Role: Network

Additional Information

From Template: 140: Rule Removal Request
Change Request Template ID: *(no value)*

3. Modify the **Source**, **Destination**, and/or **Service/Application** fields as desired.
4. Click **Ok**.

The change request is modified.

### Examine risk check results

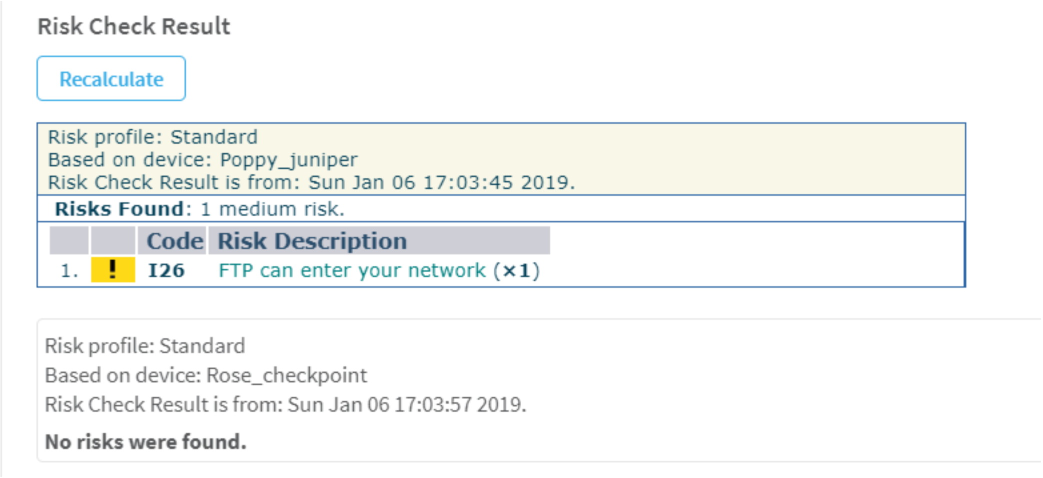
> **Note:** The method FireFlow uses to choose devices to perform risk checks on requests and their devices or policies can be customized by an administrator.

Do the following:

1. View the change request. For details, see View change requests.
2. If the risk check is not available, refresh the risk calculation by clicking **Recalculate**.

   > **Note:** You will also want to recalculate the risk check in the following rare cases: if you edited the risk profile in AFA, the routing of the device changed, or you changed the assignment of interfaces to zones in AFA for any of the devices.

FireFlow analyzes the device data, and the risk check results appear in the **Risk Check Result** area.



Risk Check Result

Risk profile: Standard
Based on device: Poppy_juniper
Risk Check Result is from: Sun Jan 06 17:03:45 2019.

**Risks Found**: 1 medium risk.

| | | Code | Risk Description |
|---|---|---|---|
| 1. | ! | I26 | FTP can enter your network (×1) |

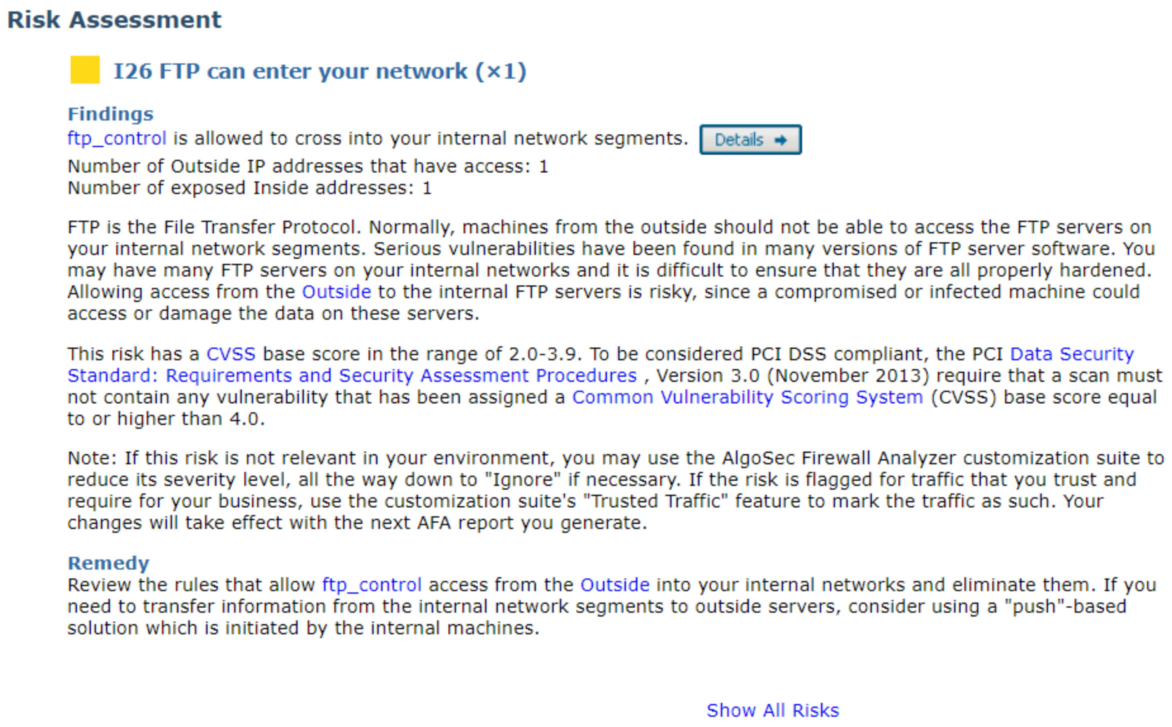
Risk profile: Standard
Based on device: Rose_checkpoint
Risk Check Result is from: Sun Jan 06 17:03:57 2019.

**No risks were found.**

The **Risk Check Result** area displays the number and severity of risks detected, followed by the date and time at which the device data that was used in the risk check was gathered.

3. To view a risk assessment, click on the desired risk.

   An assessment of the risk opens in a new window.



Risk Assessment

🟨 I26 FTP can enter your network (×1)

Findings

ftp_control is allowed to cross into your internal network segments.

Number of Outside IP addresses that have access: 1
Number of exposed Inside addresses: 1

FTP is the File Transfer Protocol. Normally, machines from the outside should not be able to access the FTP servers on your internal network segments. Serious vulnerabilities have been found in many versions of FTP server software. You may have many FTP servers on your internal networks and it is difficult to ensure that they are all properly hardened. Allowing access from the Outside to the internal FTP servers is risky, since a compromised or infected machine could access or damage the data on these servers.

This risk has a CVSS base score in the range of 2.0-3.9. To be considered PCI DSS compliant, the PCI Data Security Standard: Requirements and Security Assessment Procedures , Version 3.0 (November 2013) require that a scan must not contain any vulnerability that has been assigned a Common Vulnerability Scoring System (CVSS) base score equal to or higher than 4.0.

Note: If this risk is not relevant in your environment, you may use the AlgoSec Firewall Analyzer customization suite to reduce its severity level, all the way down to "Ignore" if necessary. If the risk is flagged for traffic that you trust and require for your business, use the customization suite's "Trusted Traffic" feature to mark the traffic as such. Your changes will take effect with the next AFA report you generate.

Remedy

Review the rules that allow ftp_control access from the Outside into your internal networks and eliminate them. If you need to transfer information from the internal network segments to outside servers, consider using a "push"-based solution which is initiated by the internal machines.

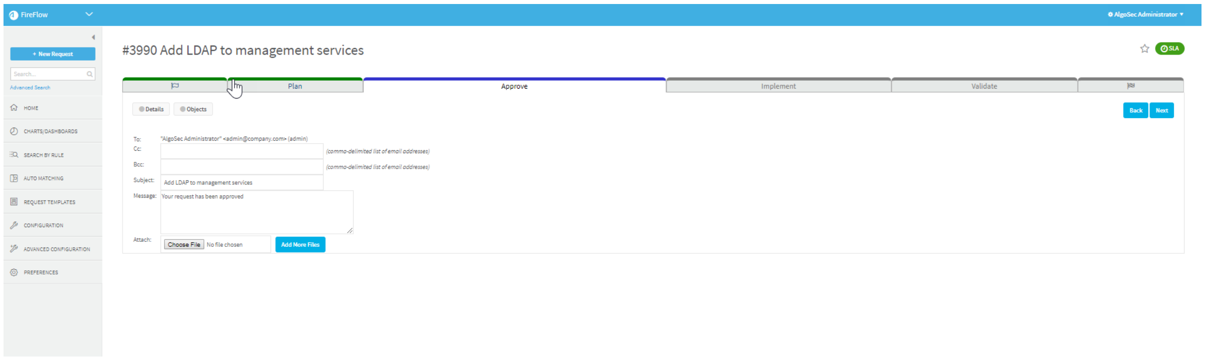
## Approve a change request

Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click **Approve**.

   The Approve Change Request page appears.

   > **Note:** For IPv6 traffic requests, and for other traffic requests using the Basic workflow, an email is automatically sent to the requestor after the change request is approved. After the change request is approved, it proceeds straight to the implement stage.



#3990 Add LDAP to management services

To: "AlgoSec Administrator" <admin@company.com> (admin)

Cc: (comma-delimited list of email addresses)

Bcc: (comma-delimited list of email addresses)

Subject: Add LDAP to management services

Message: Your request has been approved

Attach: No file chosen

3. Complete the fields as needed. For details, see Respond to change requests.
4. Click **Next**.

The change request proceeds to the Implement stage. See Implementing Changes (see Implement changes).

The email message is sent to the requestor.

If you have the network operations role only (and not the information security role), or if the change request is not for a specific device or policy, the **Home** page appears.

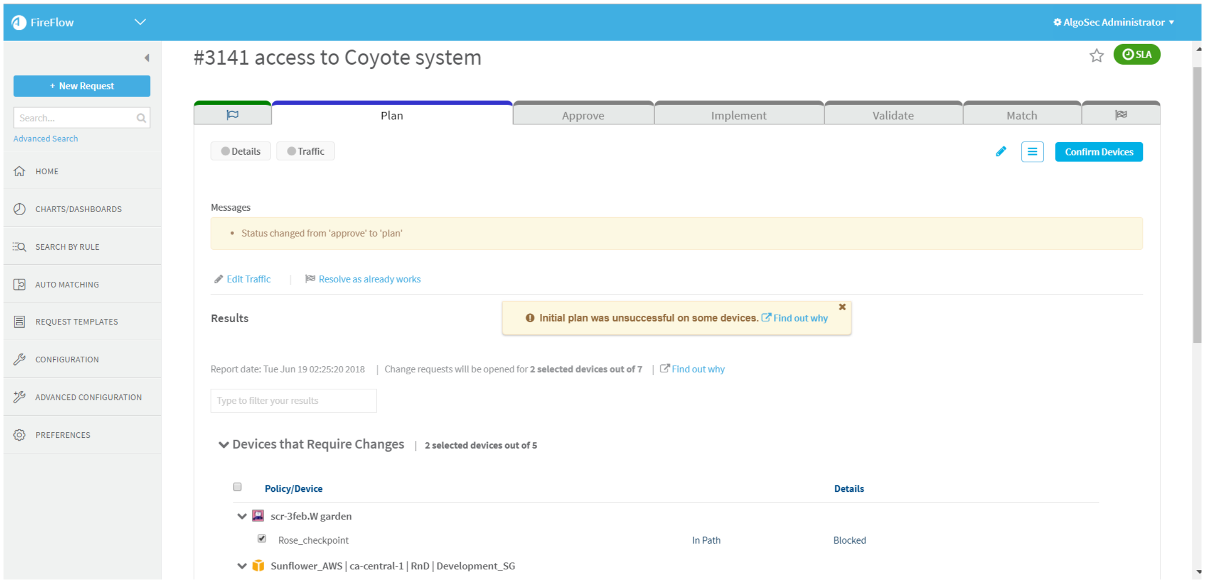
### Return a change request to the Plan stage

If you determine that the change request requires modifications, you can return it to the Plan stage. Here is a description of how this is done.

Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click **Reject**.

   The Reject Change Request page appears.



#3141 access to Coyote system

Messages

- Status changed from 'approve' to 'plan'

Results

Initial plan was unsuccessful on some devices. Find out why

Report date: Tue Jun 19 02:25:20 2018 | Change requests will be opened for **2 selected devices out of 7** | Find out why

Devices that Require Changes | **2 selected devices out of 5**

| □ Policy/Device | | Details |
|---|---|---|
| scr-3feb.W garden | | |
| ☑ Rose_checkpoint | In Path | Blocked |
| Sunflower_AWS \| ca-central-1 \| RnD \| Development_SG | | |

3. Complete the fields as needed. For details, see Respond to change requests.
4. Click **Next**.

The change request is returned to the Plan stage for re-planning.

If you have the network operations role only (and not the information security role), the **Home** page appears.

### Reject and close a change request

If you determine that the change request should not be implemented, you can reject and close it.

Do the following:

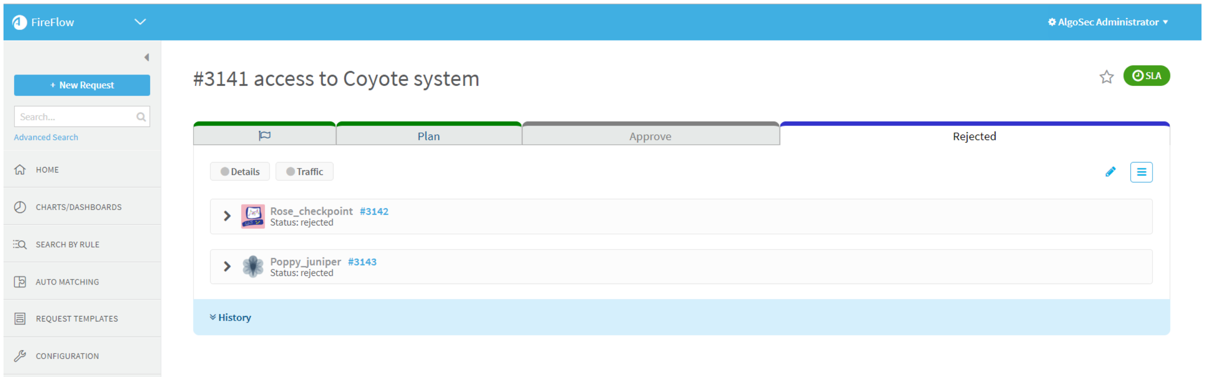
1. View the change request. For details, see View change requests.
2. At the top of the page, do one of the following:
   - For rule removal requests, click **Reject**.
   - For other change request types, click ☰, and then click **Reject & Close**.

> **Note:** The list of option available in the drop-down list may be changed by an administrator, by editing a workflow's available actions.

A confirmation message appears.

3. Click **OK**.

   The Reject Change Request page appears.



#3141 access to Coyote system

Rose_checkpoint #3142
Status: rejected

Poppy_juniper #3143
Status: rejected

4. Complete the fields as needed. For details, see Respond to change requests.
5. Click **Next**.

The email message is sent to the requestor, and the change request is closed.

## ➔ See also:

- Manage requestor notifications

# Manage requestor notifications

### Relevant for: Network operation users

This topic describes how to manage requestor notifications for change requests in the **Approve** stage, such as traffic change requests with a "Drop" action, rule removal requests, rule modification requests, or re-certification requests.

> **Note:** To determine a change request's stage, view the change request. The stage is

indicated by the Change Request Lifecycle Status Bar. For details, see View change requests.

## Request handling per type

You may need to notify requestors as follows, depending on the request type:

| Request type | Description |
|---|---|
| **Traffic change requests with a Drop action** | In a traffic change request with a "Drop" action, a rule removal request, or a rule modification request, you can search for change requests whose requested traffic will consequently be blocked. You must then notify the requestors of these change requests that the traffic is slated to be blocked. The requestors have until the change request's due date to respond.<br>For rule removal requests, you also have the option to extend the due date. If desired, you can view responses received from requestors or re-notify the requestors at any time.<br>Once you have received the requestors' responses, the change request advances to the Approve stage. |
| **Rule removal requests** | |
| **Rule modification requests** | |
| **Re-certification requests** | In a re-certification request, you can search for change requests whose traffic intersects that of the Allow traffic that was added by the expired change request.<br>You must then notify the requestors of these change requests that the Allow traffic is slated for removal.<br>The requestors have until the recertification request's due date to respond.<br>If desired, you can extend the due date, view responses received from requestors, or re-notify the requestors at any time.<br>Once you have received the requestors' responses, you must decide whether to certify the Allow traffic or plan its removal. |

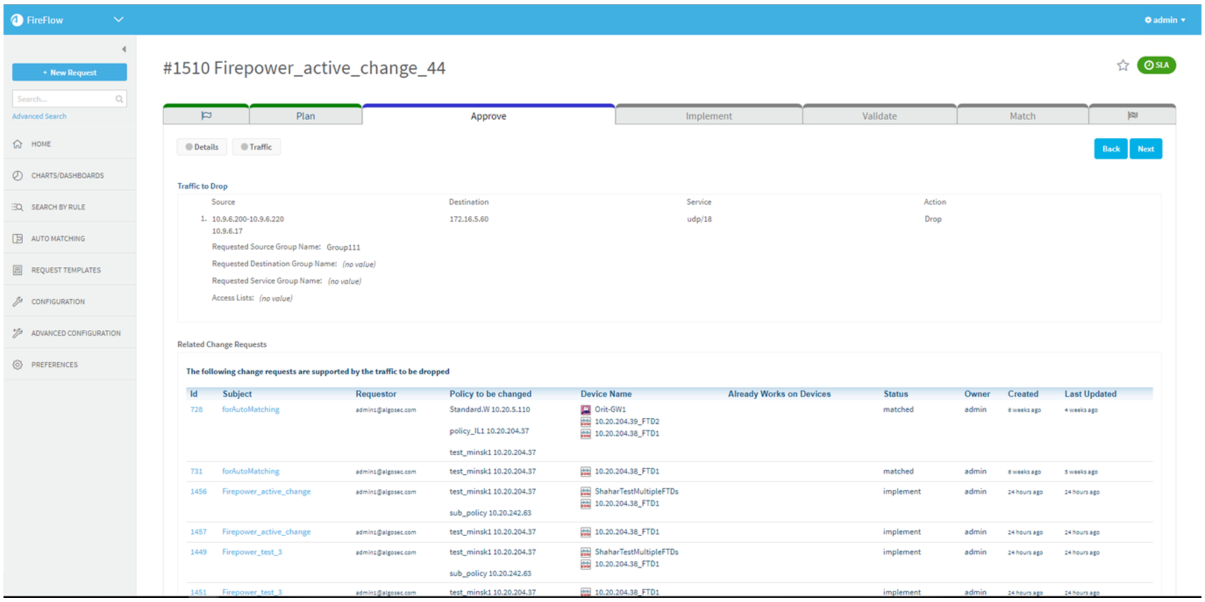
## Find related change requests

### Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click **Find Related Change Requests**.

   The **Related Change Requests** appear.

   For traffic change requests with a "Drop" action, the page displays the details of the "Allow" traffic that is to be blocked, followed by a list of change requests related to the rule.

   #1510 Firepower_active_change_44

   Traffic to Drop

   | | Source | Destination | Service | Action |
   |---|---|---|---|---|
   | 1. | 10.9.6.200-10.9.6.220<br>10.9.6.17 | 172.16.5.60 | udp/18 | Drop |

   Requested Source Group Name: Group111

   Requested Destination Group Name: *(no value)*

   Requested Service Group Name: *(no value)*

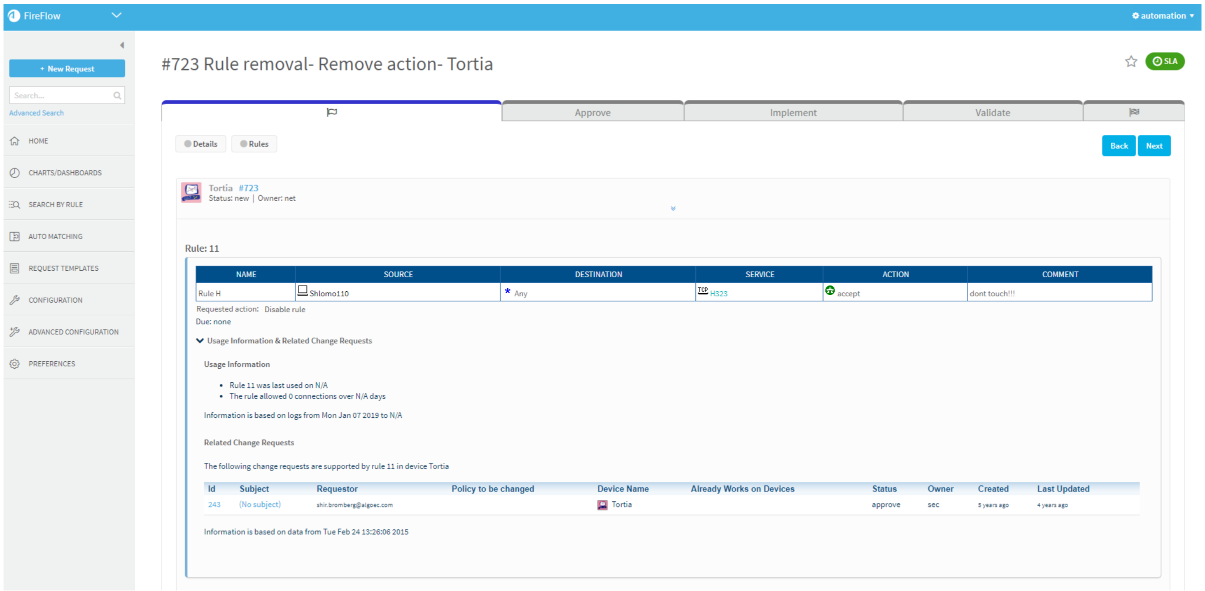
   Access Lists: *(no value)*

   Related Change Requests

   The following change requests are supported by the traffic to be dropped

   | Id | Subject | Requestor | Policy to be changed | Device Name | Already Works on Devices | Status | Owner | Created | Last Updated |
   |---|---|---|---|---|---|---|---|---|---|
   | 728 | forAutoMatching | admin1@algosec.com | Standard.W 10.20.5.110<br>policy_IL1 10.20.204.37<br>test_minsk1 10.20.204.37 | Orit-GW1<br>10.20.204.39_FTD2<br>10.20.204.38_FTD1 | | matched | admin | 6 weeks ago | 4 weeks ago |
   | 731 | forAutoMatching | admin1@algosec.com | test_minsk1 10.20.204.37 | 10.20.204.38_FTD1 | | matched | admin | 6 weeks ago | 5 weeks ago |
   | 1456 | Firepower_active_change | admin1@algosec.com | test_minsk1 10.20.204.37<br>sub_policy 10.20.242.63 | ShaharTestMultipleFTDs<br>10.20.204.38_FTD1 | | implement | admin | 24 hours ago | 24 hours ago |
   | 1457 | Firepower_active_change | admin1@algosec.com | test_minsk1 10.20.204.37 | 10.20.204.38_FTD1 | | implement | admin | 24 hours ago | 24 hours ago |
   | 1449 | Firepower_test_3 | admin1@algosec.com | test_minsk1 10.20.204.37<br>sub_policy 10.20.242.63 | ShaharTestMultipleFTDs<br>10.20.204.38_FTD1 | | implement | admin | 24 hours ago | 24 hours ago |
   | 1451 | Firepower_test_3 | admin1@algosec.com | test_minsk1 10.20.204.37 | 10.20.204.38_FTD1 | | implement | admin | 24 hours ago | 24 hours ago |

   For rule removal requests, the page displays the rule details, information on the rule's usage, and a list of change requests related to the rule.



#723 Rule removal- Remove action- Tortia

Tortia #723
Status: new | Owner: net

Rule: 11

| NAME | SOURCE | DESTINATION | SERVICE | ACTION | COMMENT |
|---|---|---|---|---|---|
| Rule H | Shlomo110 | * Any | TCP H323 | accept | dont touch!!! |

Requested action: Disable rule
Due: none

Usage Information & Related Change Requests

Usage Information

- Rule 11 was last used on N/A
- The rule allowed 0 connections over N/A days

Information is based on logs from Mon Jan 07 2019 to N/A

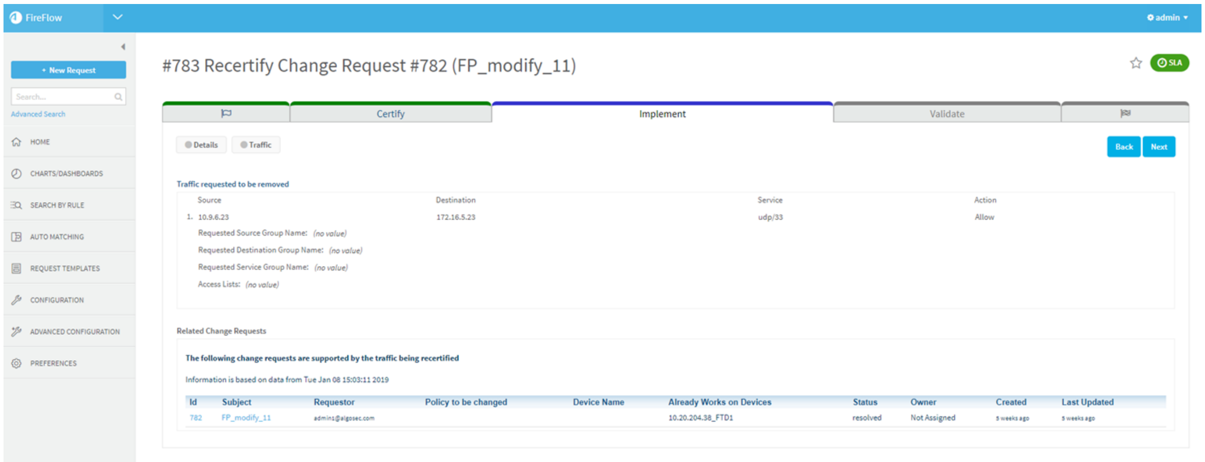
Related Change Requests

The following change requests are supported by rule 11 in device Tortia

| Id | Subject | Requestor | Policy to be changed | Device Name | Already Works on Devices | Status | Owner | Created | Last Updated |
|---|---|---|---|---|---|---|---|---|---|
| 243 | (No subject) | shir.bromberg@algoec.com | | Tortia | | approve | sec | 5 years ago | 4 years ago |

Information is based on data from Tue Feb 24 13:26:06 2015

For recertification requests, the page displays the details of the Allow traffic that is to be removed, followed by a list of change requests related to the rule.



#783 Recertify Change Request #782 (FP_modify_11)

Traffic requested to be removed

| | Source | Destination | Service | Action |
|---|---|---|---|---|
| 1. | 10.9.6.23 | 172.16.5.23 | udp/33 | Allow |

Requested Source Group Name: *(no value)*
Requested Destination Group Name: *(no value)*
Requested Service Group Name: *(no value)*
Access Lists: *(no value)*

Related Change Requests

**The following change requests are supported by the traffic being recertified**

Information is based on data from Tue Jan 08 15:03:11 2019

| Id | Subject | Requestor | Policy to be changed | Device Name | Already Works on Devices | Status | Owner | Created | Last Updated |
|---|---|---|---|---|---|---|---|---|---|
| 782 | FP_modify_11 | admin1@algosec.com | | | 10.20.204.38_FTD1 | resolved | Not Assigned | 5 weeks ago | 5 weeks ago |

3. To view an individual change request, click on the change request's name.
4. In the related change requests page, click **Next**.

The change request is displayed with the related change requests results.

## Notify requestors of related change requests

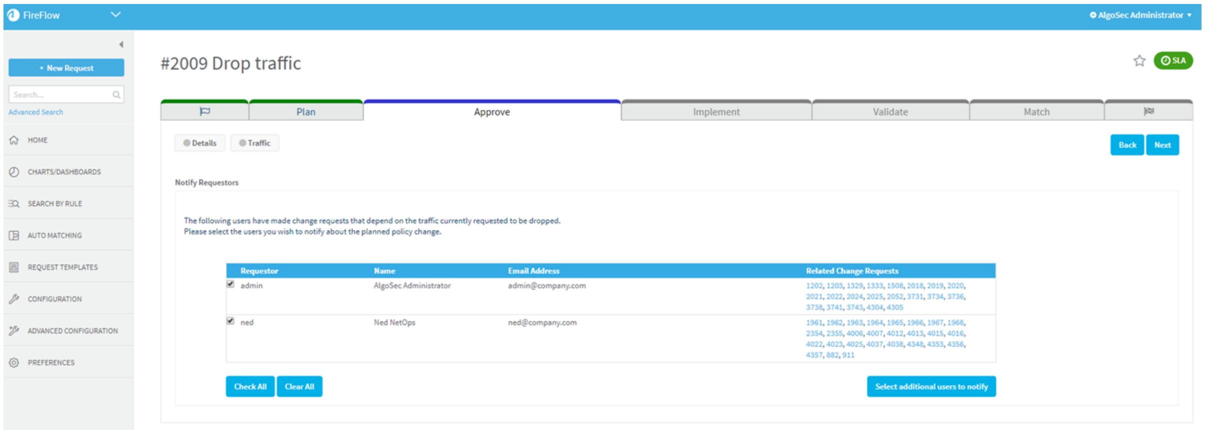
The following procedures describe how to notify requestors of related change requests:

### Drop traffic, rule removal, and rule modification requests

Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click **Notify Rule Requestors**.

   The **Notify Requestors** page appears displaying all requestors of related change requests.

   #2009 Drop traffic

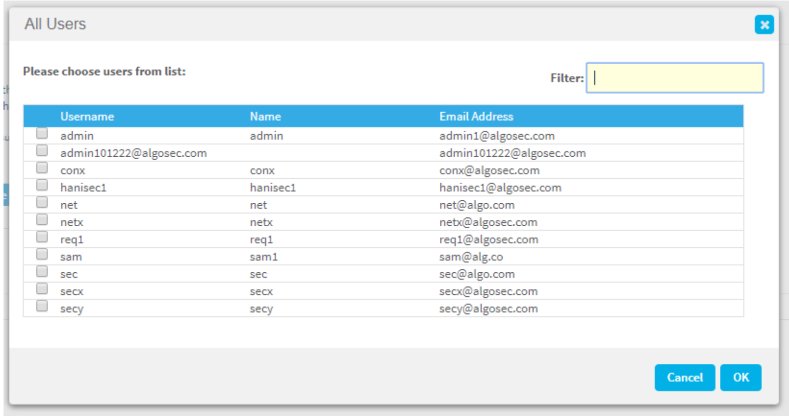
   Notify Requestors

   The following users have made change requests that depend on the traffic currently requested to be dropped.
   Please select the users you wish to notify about the planned policy change.

   | Requestor | Name | Email Address | Related Change Requests |
   |---|---|---|---|
   | ☑ admin | AlgoSec Administrator | admin@company.com | 1202, 1203, 1329, 1333, 1508, 2018, 2019, 2020, 2021, 2022, 2024, 2025, 2052, 3731, 3734, 3736, 3738, 3741, 3743, 4304, 4305 |
   | ☑ ned | Ned NetOps | ned@company.com | 1961, 1962, 1963, 1964, 1965, 1966, 1967, 1968, 2354, 2355, 4006, 4007, 4012, 4013, 4015, 4016, 4022, 4023, 4025, 4037, 4038, 4348, 4353, 4356, 4357, 882, 911 |

3. Specify which requestors to notify, by doing any of the following:
   - Select the check box next to their name to notify an individual requestor in the list.
   - Click **Check All** to notify all requestors in the list.
   - Click **Clear All** to notify none of the requestors in the list.
   - To notify additional users who are not listed, do the following:
     1. Click **Select additional users to notify**.

        The **All Users** dialog box opens with a list of all users in the FireFlow system.


All Users

Please choose users from list:

Filter:

| | Username | Name | Email Address |
|---|---|---|---|
| □ | admin | admin | admin1@algosec.com |
| □ | admin101222@algosec.com | | admin101222@algosec.com |
| □ | conx | conx | conx@algosec.com |
| □ | hanisec1 | hanisec1 | hanisec1@algosec.com |
| □ | net | net | net@algo.com |
| □ | netx | netx | netx@algosec.com |
| □ | req1 | req1 | req1@algosec.com |
| □ | sam | sam1 | sam@alg.co |
| □ | sec | sec | sec@algo.com |
| □ | secx | secx | secx@algosec.com |
| □ | secy | secy | secy@algosec.com |

b. (Optional) To filter the table, in the **Filter** field, type the string according to which the table should be filtered.

   The table is filtered, and only users whose name, username, or email address contains the specified string are displayed.

c. Select the check boxes next to the users you want to notify and click **OK**.

   The selected users appear in the list of users to notify, with an asterisk next to their name.

4. To view an individual change request, click on the change request's ID number.
5. In the **Related Change Requests** page, click **Next**.

FireFlow sends the selected users an email notifying them that the traffic is slated to be blocked.

For rule removal requests, you can optionally customize this email.

The change request is displayed.

### Re-certification Requests

Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click **Notify Traffic Requestors**.

The related change requests page appears displaying all requestors of related change requests.

3. Specify which requestors to notify, by doing any of the following:
    - Select the check box next to their name to notify an individual requestor in the list.
    - Click **Check All** to notify all requestors in the list.
    - Click **Clear All** to notify none of the requestors in the list.
    - To notify additional users who are not listed, do the following:
        a. Click **Select additional users to consult**.

           The **All Users** dialog box opens with a list of all users in the FireFlow system.
        b. (Optional) To filter the table, in the **Filter** field, type the string according to which the table should be filtered.

           The table is filtered, and only users whose name, username, or email address contains the specified string are displayed.
        c. Select the check boxes next to the users you want to notify and click **OK**.

      The selected users appear in the list of users to notify, with an asterisk next to their name.
4. To view an individual change request, click on the change request's ID number.
5. In the **Related Change Requests** page, click **Next**.

FireFlow sends the selected users an email notifying them that the Allow traffic added by the expired change request is slated for removal.

The recertification request is displayed.

## Notify requestors for related change requests again

The following procedures describe how to re-notify requestors about changes in related change requests:

### Drop traffic change requests, rule removal requests, and rule modification requests

Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click **Re-Notify Requestors**.

   The related change requests page appears displaying all requestors of related change requests.
3. Specify which requestors to notify, by doing any of the following:
   - To notify an individual requestor in the list, select the check box next to their name.
   - Click **Check All** to notify all requestors in the list.
   - Click **Clear All** to notify none of the requestors in the list.
   - To notify additional users who are not listed, do the following:
     a. Click **Select additional users to notify**.

        The **All Users** dialog box opens with a list of all users in the FireFlow system.

     b. (Optional) To filter the table, in the **Filter** field, type the string according to which the table should be filtered.

        The table is filtered, and only users whose name, username, or email address contains the specified string are displayed.

     c. Select the check boxes next to the users you want to notify.

     d. Click **OK**.

   The selected users appear in the list of users to notify, with an asterisk next to their name.
4. To view an individual change request, click on the change request's ID number.
5. In the **Related Change Requests** page, click **Next**.

FireFlow sends the selected users an email notifying them that the traffic is slated to be blocked.

For rule removal requests, you can optionally customize this email.

The change request is displayed.

### Recertification requests

Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click **Notify Traffic Requestors**.

   The related change requests page appears displaying all requestors of related change requests.
3. Specify which requestors to notify, by doing any of the following:
   - Select the check box next to their name to notify an individual requestor in the list.
   - Click **Check All** to notify all requestors in the list.
   - Click **Clear All** to notify none of the requestors in the list.
   - To notify additional users who are not listed, do the following:
     a. Click **Select additional users to consult**.

        The **All Users** dialog box opens with a list of all users in the FireFlow system.

     b. (Optional) To filter the table, in the **Filter** field, type the string according to which the table should be filtered.

        The table is filtered, and only users whose name, username, or email address contains the specified string are displayed.

   c. Select the check boxes next to the users you want to notify.

   d. Click **OK**.

   The selected users appear in the list of users to notify, with an asterisk next to their name.

4. To view an individual change request, click on the change request's ID number.
5. In the **Related Change Requests** page, click **Next**.

FireFlow sends the selected users an email notifying them that the Allow traffic added by the expired change request is slated for removal.

The recertification request is displayed.

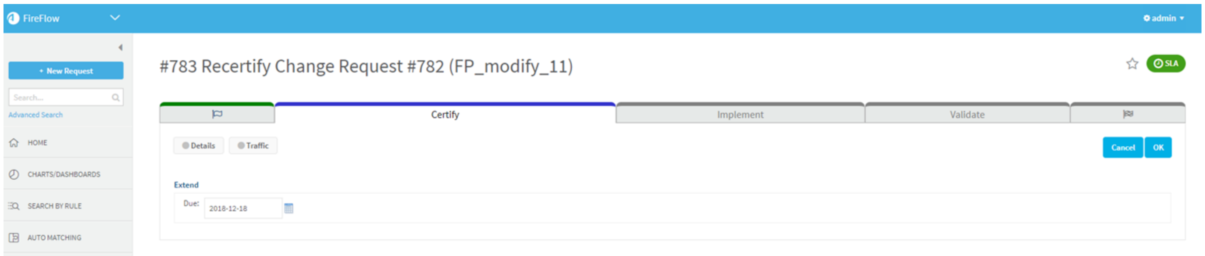
## Extend a rule removal due date

A rule removal request's due date represents the date by which requestors must respond to the notification they received regarding rule removal/disablement. Here is a description of how to extend this due date.

### Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click **Extend**.

   The **Extend** page appears.



#783 Recertify Change Request #782 (FP_modify_11)

Extend

Due: 2018-12-18

3. Do one of the following:

   - Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.

- Type the desired date in the field provided. You can use most relative and absolute formats, for example `yyyy-mm-dd`, `mm/dd/yyyy`, `Mon dd yyyy`, “next week”, and “now + 3 days”.

4. Click **OK**.

The change request is displayed.

## Extend a re-certification request due date

A recertification request's due date represents the date by which requestors must respond to the notification they received regarding traffic removal. Here is a description of how to extend this due date.

Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click ☰ , and then click **Extend**.

   > **Note:** The list of options available in the drop-down list may be changed by an administrator, by editing a workflow's available actions.

   The **Extend** page is displayed.
3. Do one of the following:
   - Click ▦, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.
   - Type the desired date in the field provided. You can use most relative and absolute formats, for example `yyyy-mm-dd`, `mm/dd/yyyy`, `Mon dd yyyy`, “next week”, and “now + 3 days”.
4. Click **OK**.

The change request is displayed.

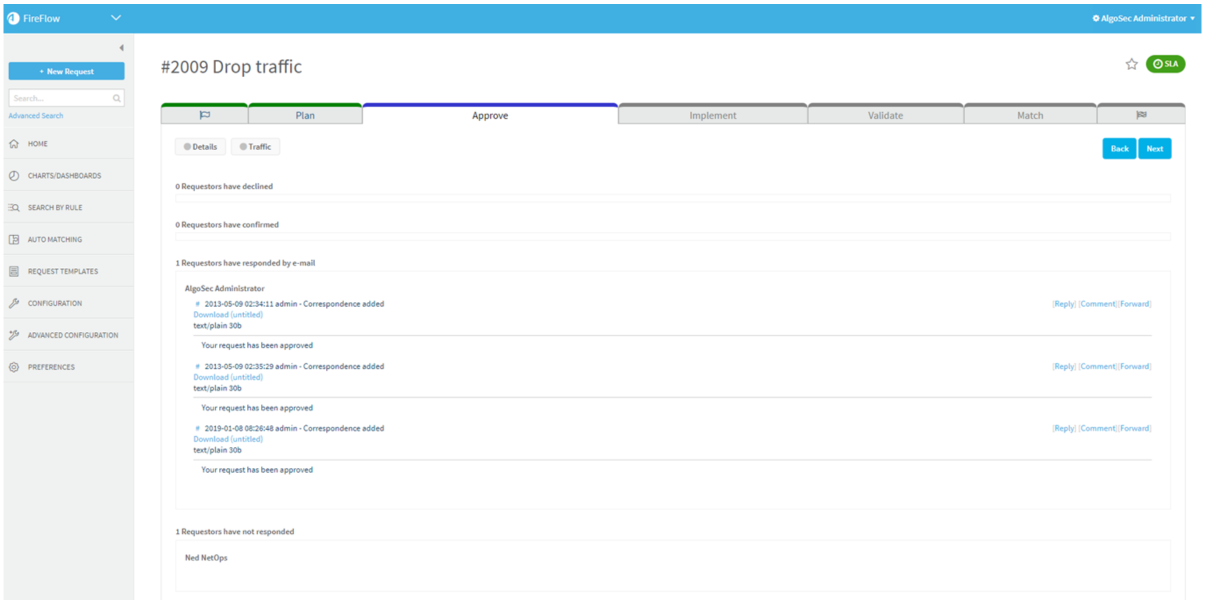
## View responses from requestors

Here is a description of how to view email responses from requestors.

Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click **Correspondence**.

   The View Correspondence page appears displaying a list of requestors who have declined to approve the change, a list of requestors who have confirmed that the change is acceptable, a list of requestors who have responded by e-mail, and a list of requestors who have not yet replied.

   #2009 Drop traffic

   0 Requestors have declined

   0 Requestors have confirmed

   1 Requestors have responded by e-mail

   AlgoSec Administrator

   2013-05-09 02:34:11 admin - Correspondence added
   Download (untitled)
   text/plain 30b

   Your request has been approved

   2013-05-09 02:35:29 admin - Correspondence added
   Download (untitled)
   text/plain 30b

   Your request has been approved

   2019-01-08 08:26:48 admin - Correspondence added
   Download (untitled)
   text/plain 30b

   Your request has been approved

   1 Requestors have not responded

   Ned NetOps

3. To view a response, click ⊞ next to the relevant requestor's name.

   The response is displayed.
4. Click **Next.**

The change request is displayed.

# Review change requests

**Relevant for: Controllers**

This topic explains how to review traffic change requests before implementation.

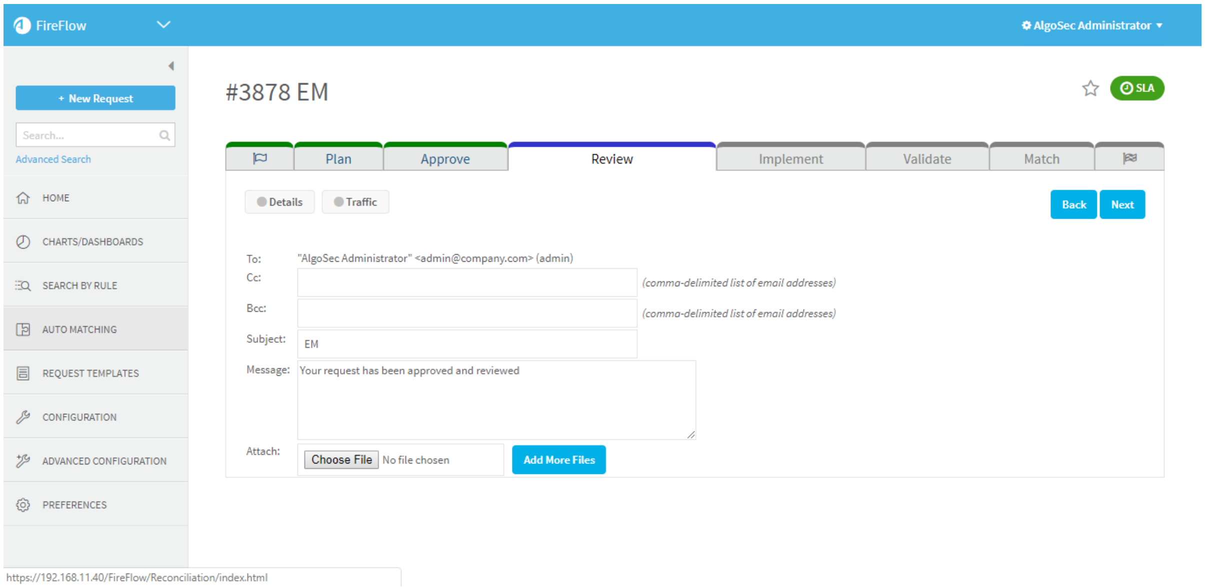
If a traffic change request uses the Multi-Approval or Parallel-Approval workflow, then after the change request has been approved by an information security user, it starts the Review stage of the FireFlow change request lifecycle. In this stage, you examine the change request, fill in any mandatory change request fields that are empty, and then notify the requestor that the change request was reviewed and approved for implementation.

> **Note:** To determine a change request's stage, view the change request. The stage is indicated by the Change Request Lifecycle Status Bar. For details, see View change requests.

## Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click **Review**.

   You are prompted to compose an email, notifying the requestor that the change request has been approved and reviewed.



To: "AlgoSec Administrator" <admin@company.com> (admin)

Cc: (comma-delimited list of email addresses)

Bcc: (comma-delimited list of email addresses)

Subject: EM

Message: Your request has been approved and reviewed

Attach:

3. Complete the fields as needed. For details, see Respond to change requests.
4. Click **Next**.

FireFlow sends your message to the requestor.

The change request proceeds to the Implement stage.

# Implement changes

**Relevant for: Network operation users**

This section explains how to implement changes specified by change requests.

> **Note:** To determine a change request's stage, view the change request. The stage is indicated by the Change Request Lifecycle Status Bar. For details, see View change requests.

## Implementation process per request type

The following table describes how to implement changes, depending on the type of request you're working with.

| Request type | Description |
|---|---|
| **Traffic change requests** | 1. In the **Implement** stage of a traffic change request or rule removal request, FireFlow creates a work order consisting of a list of recommendations for implementing the requested change, and you can then edit the work order as needed.<br>2. You then implement the suggested changes on the device according to the plan, either manually, or with ActiveChange.<br>**Note:** If the change request has multiple devices or policies, you must perform these steps separately for each device or policy. |
| **Rule removal requests** | |
| **Recertification requests** | 1. In the Implement stage of an object change request or recertification request, FireFlow creates a work order consisting of a list of recommendations for implementing the requested change, and you can then edit the work order as needed.<br>2. Next, you implement the requested changes on the security device according to plan.<br>**Note:** ActiveChange is supported on some device types for multi-device object change requests. For more details, see Implement changes with ActiveChange and the AlgoSec support matrix. |
| **Object change requests (including multi device)** | |

| Request type | Description |
|---|---|
| **Rule modification requests** | 1. When working with a rule modification request, FireFlow creates a work order consisting of a list of recommendations for implementing the requested change.<br>2. If the rule has changed while the change request was being processed, re-plan the change request.<br>3. You can then edit the work order as needed.<br>4. Next, you implement the requested changes on the security device according to plan. |
| **Web filtering change requests** | 1. When working with a Web filtering change request, you must first choose an organizational methodology to use for implementing the requested change.<br>2. FireFlow then creates a work order consisting of a list of recommendations for implementing the requested change, and you can then edit the work order as needed.<br>For details, see Select an organization method and edit work orders for web filtering change requests.<br>3. Finally, you implement the requested changes on the security device according to selected methodology and the work order. |
| **Generic change requests** | When working with a generic change request lifecycle, no work order is generated.<br>Instead, you immediately implement the requested changes on the security device according to plan. |

# Re-plan a rule modification request

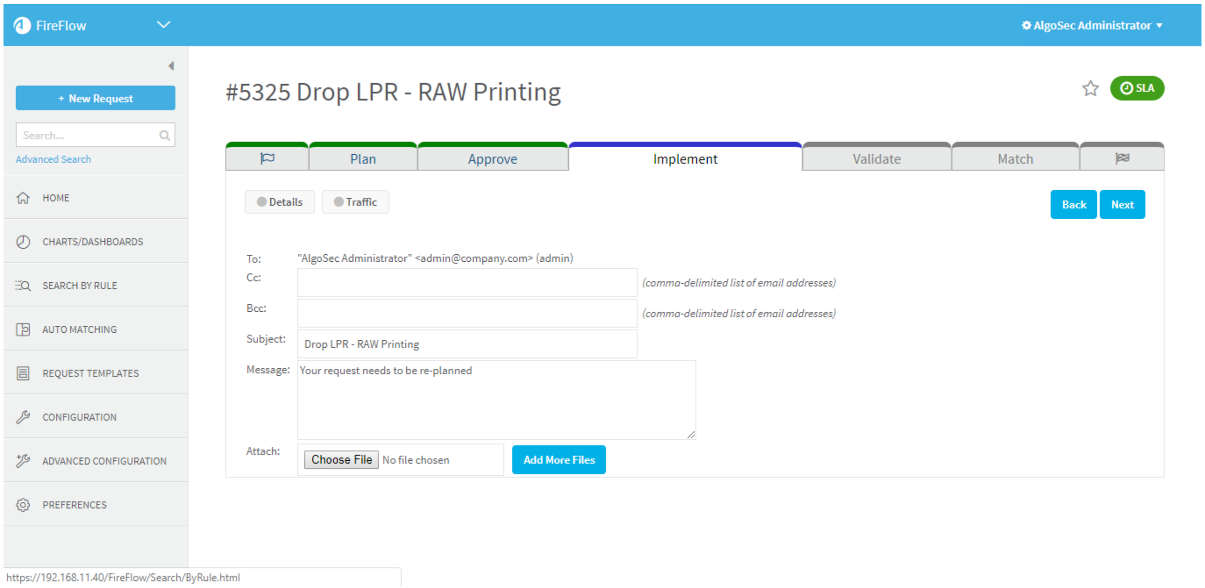
If the rule has changed while the change request was being processed, re-plan the change request. Re-planning updates the current rule values in FireFlow.

## Do the following:

1. View the change request. For details, see View change requests.

2. Click **Re-Plan**.

   You are prompted to compose an email, notifying the requestor that the change request needs to be re-planned.



#5325 Drop LPR - RAW Printing

To: "AlgoSec Administrator" <admin@company.com> (admin)

Cc: (comma-delimited list of email addresses)

Bcc: (comma-delimited list of email addresses)

Subject: Drop LPR - RAW Printing

Message: Your request needs to be re-planned

Attach: No file chosen

3. Complete the fields as needed. For details, see Respond to change requests.

4. Click **Next**.

   The change request's status goes back to "Plan".

5. Modify the change request as necessary. For details, see Manage rule modification requests.

## Edit work orders for rule removal and object change requests

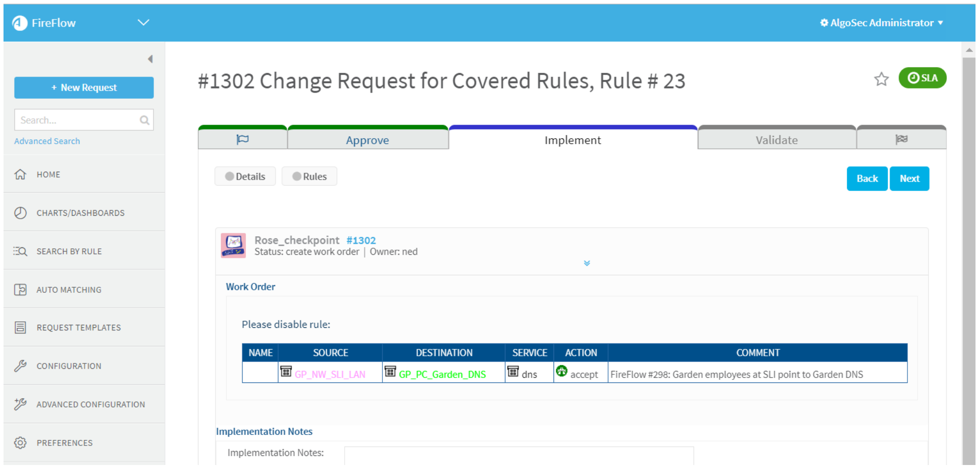
You can edit a work order by adding notes to the work order. For Amazon Web Services and Microsoft Azure, only removing rules (not disabling rules) is supported.

> **Note:** In addition, you can change a rule removal request's action (disable or remove), by editing the change request's **Device change > Rules Details** area. For details, see The Advanced Editing wizard .

## Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the workspace, click **Create Work Order**.

   The **Work Order** appears.

   #1302 Change Request for Covered Rules, Rule # 23

   Rose_checkpoint #1302
   Status: create work order | Owner: ned

   Work Order

   Please disable rule:

   | NAME | SOURCE | DESTINATION | SERVICE | ACTION | COMMENT |
   |---|---|---|---|---|---|
   | | GP_NW_SLI_LAN | GP_PC_Garden_DNS | dns | accept | FireFlow #298: Garden employees at SLI point to Garden DNS |

   Implementation Notes

   Implementation Notes:

   The **Work Order** area displays FireFlow's recommendations for implementing the change specified in the change request.

3. In the **Implementation Notes** area, type your comments for implementing the change specified in the change request.

   This field is optional.

4. Click **Next**.

The work order is saved.

The change request appears with the work order and notes.

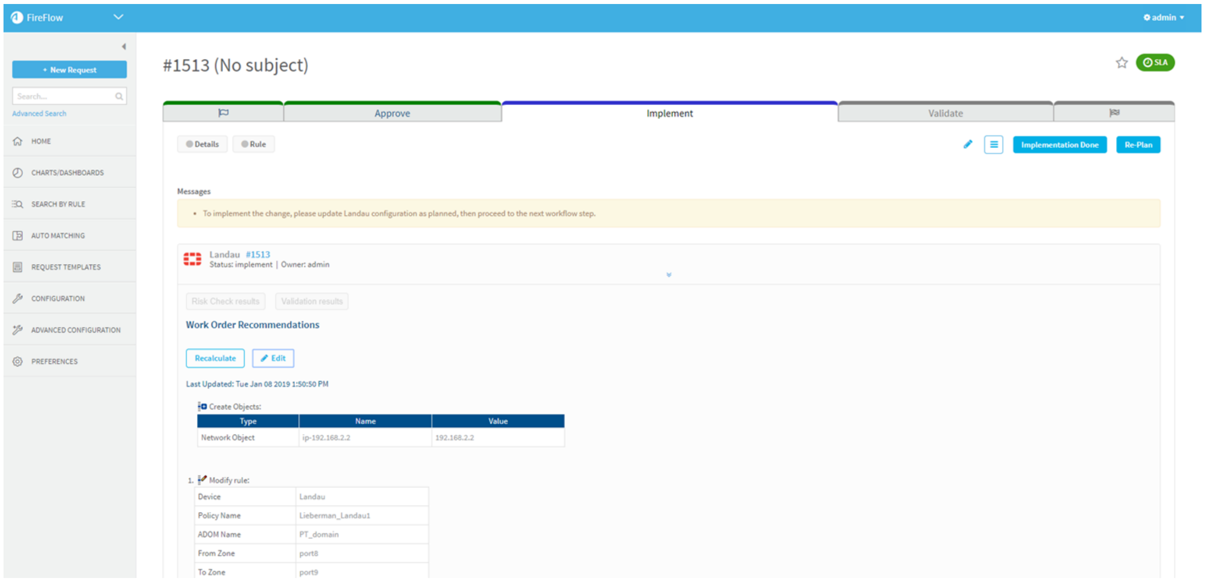
# Edit work orders for rule modification requests

You can edit a work order by adding notes to the work order.

## Do the following:

1. View the change request. For details, see View change requests.
2. If the work order is not available, or the device policies have changed since the work order was created, refresh the work order by clicking **Recalculate**.

   FireFlow examines the relevant devices' saved policies, and the work order appears in the **Work Order Recommendations** area.

   #1513 (No subject)

   Messages

   - To implement the change, please update Landau configuration as planned, then proceed to the next workflow step.

   Landau #1513
   Status: implement | Owner: admin

   Work Order Recommendations

   Last Updated: Tue Jan 08 2019 1:50:50 PM

   Create Objects:

   | Type | Name | Value |
   |---|---|---|
   | Network Object | ip-192.168.2.2 | 192.168.2.2 |

   1. Modify rule:

   | | |
   |---|---|
   | Device | Landau |
   | Policy Name | Lieberman_Landau1 |
   | ADOM Name | PT_domain |
   | From Zone | port8 |
   | To Zone | port9 |

   The **Work Order Recommendations** area displays FireFlow's recommendations for implementing the change specified in the change request. Values to add to the rule are highlighted in yellow, and values to remove are crossed out.

   > **Note:** For layer 3 protocols (non-TCP/UDP/ICMP), the work order only will recommend using services that are already defined on the device. FireFlow will not recommend adding a new service for these protocols. If the layer 3 protocol that was used in the change request is not found on the device, FireFlow issues a warning. For more details, see Change request field references.

3. To add a comment regarding implementing the change specified in the change request, do the following:

a. Click **Edit** in the **Implementation Notes** area. The **Edit Implementation Notes** window is displayed.

b. In the **Implementation Notes** field, Type a comment regarding implementing the change specified in the change request.

c. Click **OK**.

The work order is saved.

The change request appears with the work order and notes.

# Edit work orders for recertificaiton requests

You can edit a work order by adding notes to the work order.

> **Note:** In order to implement changes for a request, you must perform this procedure for all of its devices and policies.

### Change requests that include traffic with NAT

For change requests including traffic with NAT, requests will include only the relevant addresses. A request for a device that is located before NAT will only include the before translation address, a request for a device that is located after NAT will only include the after translation address, and the request for a device that performs NAT will include the before translation and after translation addresses.

## Do the following:

1. View the change request. For details, see View change requests.
2. If the change request has multiple devices or policies, click ▸ next to a device.

   The device's action buttons, and the **Work Order Recommendations** area appear below the device panel.
3. If the work order is not available, or the device policies have changed since the work

order was created, refresh the work order by clicking **Recalculate**.

FireFlow examines the relevant devices' saved policies, and the work order appears in the **Work Order Recommendations** area.

The **Work Order Recommendations** area displays FireFlow's recommendations for implementing the change specified in the change request. If the change request contains multiple requests, FireFlow provides a recommendation for each request. Note that the recommendation may be "No action required", if the requested traffic is already allowed by the device.

For a “Modify rule” recommendation, values that should be added are highlighted in yellow, and values that should be deleted are highlighted in pink.

> **Note:** If FireFlow was configured to allow the user to choose to add a new rule instead of modifying an existing one, the **New Rule** button appears next to **Recalculate**. To manually force "Add rule" recommendations, click **New Rule**. Selecting **Recalculate** will prefer a "Modify rule" recommendation. If FireFlow was configured to always recommend adding a rule, the **New Rule** button will not appear, and FireFlow will always recommend adding a new rule.

4. To view the query on which the recommendation is based, click Find out why.

   A new window opens displaying the query.

5. In the **Implementation Notes** area, type your comments for implementing the change specified in the change request.

   This field is optional.

6. Click **Next**.

The work order is saved.

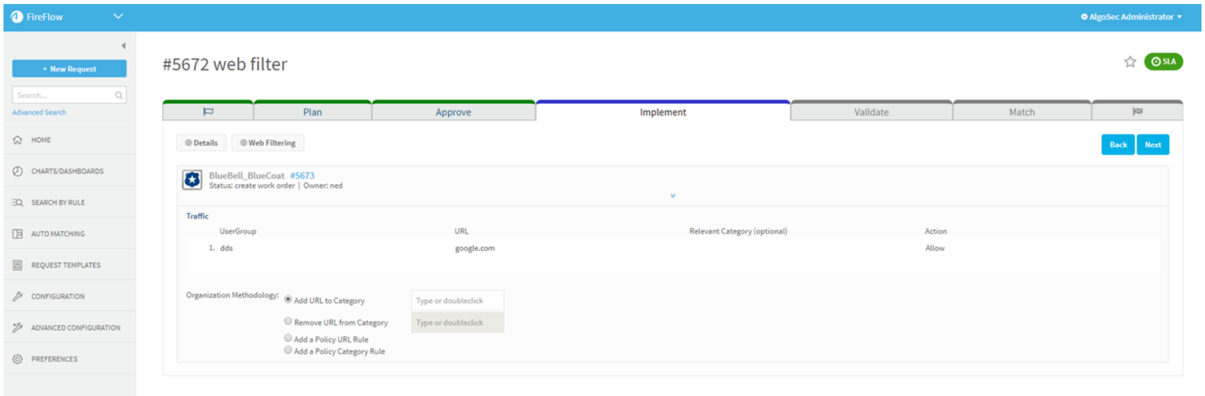
The change request is displayed with the work order and notes.

# Select an organization method and edit work orders for web filtering change requests

## Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click **Organize**.

   The Organize Change Request page appears displaying the Web filtering change request.

   #5672 web filter

   BlueBell_BlueCoat #5673
   Status: create work order | Owner: ned

   Traffic

   | | UserGroup | URL | Relevant Category (optional) | Action |
   |---|---|---|---|---|
   | 1. | dds | google.com | | Allow |

   Organization Methodology:
   ● Add URL to Category — Type or doubleclick
   ○ Remove URL from Category — Type or doubleclick
   ○ Add a Policy URL Rule
   ○ Add a Policy Category Rule

3. In the **Organization Methodology** list, specify the method to use for implementing the Web filtering change request, by doing one of the following:
   - Add a rule to the device's Web filtering policy. Select **Add a Policy URL Rule**.
   - Add a Web filtering category to the device. Select **Add a Policy Category**.
   - **Remove the specified URL from the specified Web filtering category**
     a. Choose **Remove URL from Category**.
     b. In the field provided, specify the category from which the URL should be removed, either by typing the category name, or by double-clicking in the field to open the **Choose Category** wizard.
   - **Add the specified URL to the specified Web filtering category**
     a. Choose **Add URL to Category**.

   b. In the field provided, specify the category to which the URL should be added, either by typing the category name, or by double-clicking in the field to open the **Choose Category** wizard.

   For more details, see Change request wizards.

4. Click **Next**.

   FireFlow examines the relevant devices' saved policies, and creates a work order that consists of a list of recommendations for implementing the requested change.

   The work order appears.

5. In the **Implementation Notes** area, type your comments for implementing the change specified in the change request.

   This field is optional.

6. Click **Next**.

The work order is saved.

The change request appears with the work order and notes.

# The Advanced Editing wizard

The **Advanced Editing** wizard provides the ability to edit the source, destination, or service fields of a work order. By default, the **Advanced Editing** wizard provides the ability to replace these fields' content with the following options:

- A new or existing object with the same definition as the field's current content.
- An existing object with a wider definition as the field's current content.

**Note:** Replacing a field's content with an object with a wider definition can be disabled.

### Advanced editing for specific scenarios

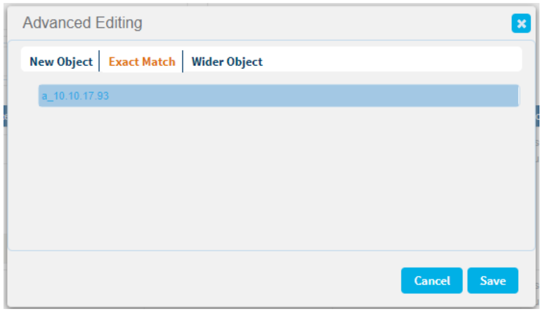
The following table shows additional notes about advanced editing for specific scenarios:

| | |
|---|---|
| **Palo Alto Networks devices** | For Palo Alto Networks devices, FireFlow does not support editing applications in a work order.<br>Editing services for Palo Alto devices is only supported when the application value is "Any". |
| **Layer 3 protocols** | Layer 3 protocols (non-TCP/UDP/ICMP) cannot be created or renamed when editing a work order. |
| **Cisco IOS/ASA devices** | For Cisco IOS/ASA devices, you can enter a single IP or a network (CIDR notation) with or without creating an object. If you enter a range, you are forced to create an object. In addition, there must be exactly one item in each field, so if you enter multiple items you are forced to create an object. |
| **Juniper SRX and Cisco IOS devices** | **Note:** For Juniper SRX and Cisco IOS devices, you can only enter objects into the source, destination, and service fields. In addition, objects cannot contain ranges (you must use CIDR notation). |

## Do the following:

1. In the source, destination or service field, click ✎.

   The **Advanced Editing** wizard appears displaying the **Exact Match** tab.

   a_10.10.17.93

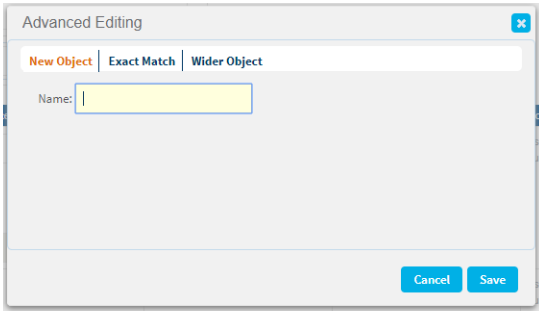
2. To select an object for the field that is an exact match for the content in the field, select an object from the list, and click **Save.**

   The selected object appears as the definition for the field in the work order.

3. To create a new object for the field whose definition matches the content in the field, do the following:

   a. Click the **New Object** tab.

      The **New Object** tab appears.

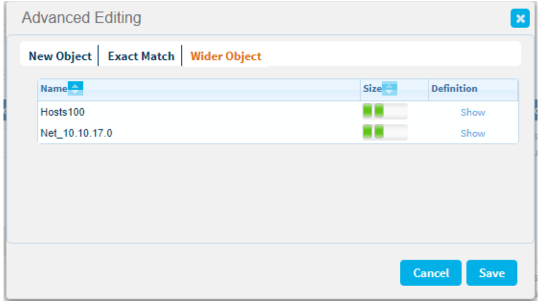
   b. In the **Name** field, enter the object's new name, and click **Save**.

   The new object is created and appears as the definition for the field in the work order.

4. To select an object for the field with a wider definition than the content currently in the field, do the following:

   a. Click the **Wider Object** tab.

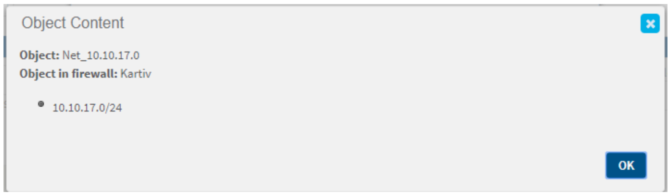
      The **Wider Object** tab appears.

      | Name | Size | Definition |
      |---|---|---|
      | Hosts100 | | Show |
      | Net_10.10.17.0 | | Show |

   b. To view an object's definition, click **Show**.

      The **Object Content** window appears, displaying the object's definition.



Object Content

**Object:** Net_10.10.17.0
**Object in firewall:** Kartiv

- 10.10.17.0/24

Click **OK** to close the dialog.

c. Select an object from the list.

All of the objects listed in the **Wider Object** tab contain the field's current content.

d. Click **Save**.

> **Note:** Choosing a wider object may introduce risks which were not assessed during the risk check.
>
> The **Wider Object** tab is only available for the source and destination fields.

The wider object appears as the definition for the field in the work order. Any objects in the work order that are wider than initially requested are indicated as such with the ↗ icon.

## Implement changes manually

> **Note:** In order to implement changes for a change request, you must perform this procedure for all of its devices and policies.

### Do the following:

1. Implement changes via the device's relevant management system (for example, Check Point Dashboard or Juniper NSM).

> **Note:** If you implement the changes even slightly different than the work order,

> Validation will fail.
>
> For example, if the work order specified one rule with multiple sources, and you added multiple rules (with one source each), Validation will fail.
>
> This is particularly relevant for Amazon Web Services because rules can only include one object per field.

2. When you have completed implementation, do *one* of the following:
   - For a change request with no devices or policies, click **Implementation Done**.
   - For *each* device or policy:
     a. Display the device's change request information by clicking ▸ next to the device.

        The device's action buttons, and the **Work Order Recommendations** area appear below the device panel.

     b. Click **Implementation Done**.
   - For a request with multiple devices or policies, click **Mark All Sub Requests As Implemented**.

     In the confirmation message, click **OK**.

The change request proceeds to the Validate stage.

➔ **See also**:

- Edit work orders
- Implement changes with ActiveChange

# Edit work orders

FireFlow enables you to edit work orders by adding notes to the work order, by editing the list of recommendations, or renaming the objects that FireFlow creates for the work order.

## Supported editing scope

You may want to edit a FireFlow work order, such as when you want to provide specific names for objects on your device. Depending on your configuration or the device you're making the change on, editing may be required before continuing on in the flow.

In other cases, editing a work flow is not supported at all, such as for work orders with a drop action, or for AWS or Symantec Blue Coat devices.

When editing a workflow, keep in mind that change requests that include traffic with NAT only include the relevant addresses in the request, as follows:

- **Requests for devices that located before NAT** only include the before-translation address.
- **Requests for devices that are located after NAT** only include the after-translation address.
- **Requests for devices that perform NAT** includes both the before- and after-translation addresses.

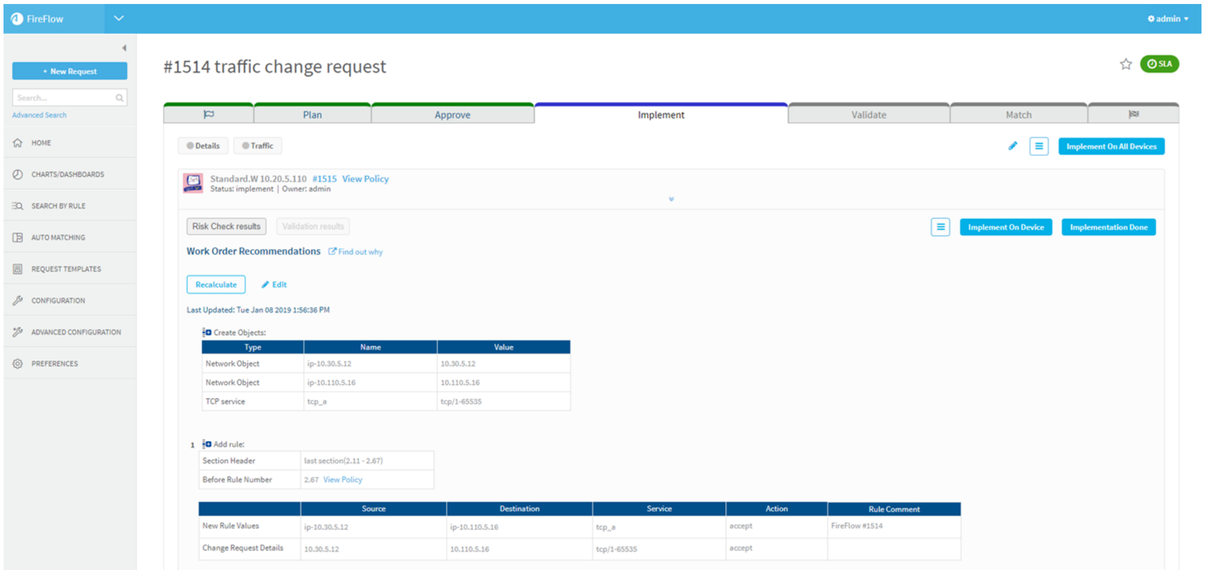
## Edit a work order

### Do the following:

1. View the change request. For details, see View change requests.
2. Do the following:
    - If the change request has multiple devices or policies, click ▶ next to a device.
    - If the work order is not available, or the device policies have changed since the work order was created, refresh the work order by clicking **Recalculate**.

   The work order and any device action buttons are shown in the **Work Order Recommendations** area.

   For example:



#1514 traffic change request

Standard.W 10.20.5.110 #1515 View Policy
Status: implement | Owner: admin

Work Order Recommendations

Last Updated: Tue Jan 08 2019 1:56:36 PM

Create Objects:

| Type | Name | Value |
|---|---|---|
| Network Object | ip-10.30.5.12 | 10.30.5.12 |
| Network Object | ip-10.110.5.16 | 10.110.5.16 |
| TCP service | tcp_a | tcp/1-65535 |

1 Add rule:

| | |
|---|---|
| Section Header | last section(2.11 - 2.67) |
| Before Rule Number | 2.67 View Policy |

| | Source | Destination | Service | Action | Rule Comment |
|---|---|---|---|---|---|
| New Rule Values | ip-10.30.5.12 | ip-10.110.5.16 | tcp_a | accept | FireFlow #1514 |
| Change Request Details | 10.30.5.12 | 10.110.5.16 | tcp/1-65535 | accept | |

This area shows FireFlow's recommendations for implementing the change specified in the change request.

> **Note:** If the traffic is already allowed by the device, your recommendation may be **No action required**.

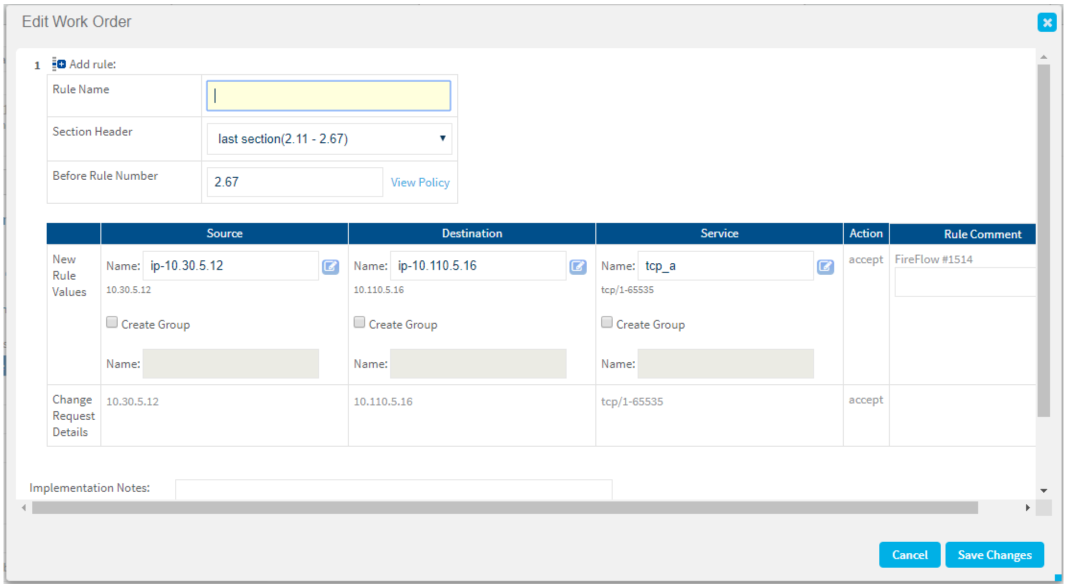
For more details, see:

- Work order recommendation details
- Implement changes with ActiveChange

4. If your change request includes only an **Allow** action, edit the values recommended by FireFlow as needed. Do the following:

   a. At the top of the **Work Order Recommendations** area, click 🖉.

      The **Edit Work Order** window appears.



Edit Work Order

1 Add rule:

| | |
|---|---|
| Rule Name | \| |
| Section Header | last section(2.11 - 2.67) ▾ |
| Before Rule Number | 2.67 View Policy |

| | Source | Destination | Service | Action | Rule Comment |
|---|---|---|---|---|---|
| New Rule Values | Name: ip-10.30.5.12<br>10.30.5.12<br>□ Create Group<br>Name: | Name: ip-10.110.5.16<br>10.110.5.16<br>□ Create Group<br>Name: | Name: tcp_a<br>tcp/1-65535<br>□ Create Group<br>Name: | accept | FireFlow #1514 |
| Change Request Details | 10.30.5.12 | 10.110.5.16 | tcp/1-65535 | accept | |

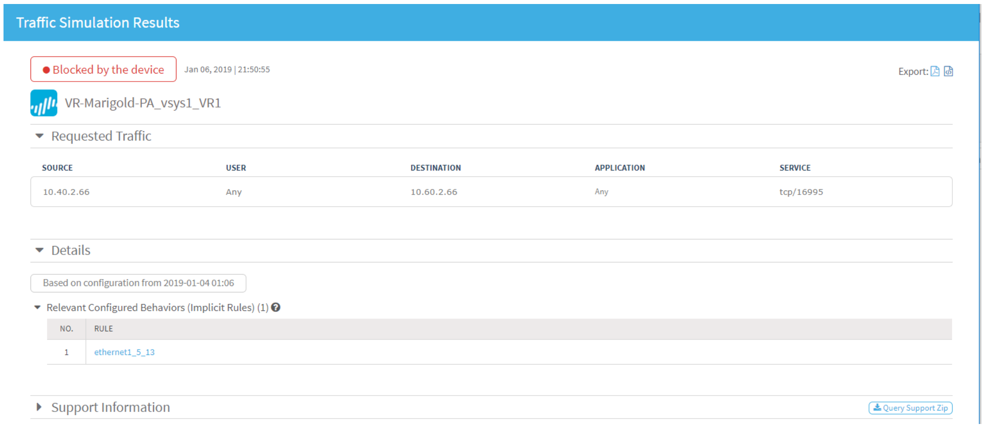
Implementation Notes:

b. Edit the fields as needed, and click **Save Changes**. For more details, see Work order recommendation details.

> **Note:** If CLI commands were generated, editing the work order will cause the CLI commands to be regenerated.

5. To view the query on which the recommendation is based, in the **Work Order Recommendations** area, click Find out why. The query details open in a new tab.

   For example:



Traffic Simulation Results

● Blocked by the device Jan 06, 2019 | 21:50:55

Export:

VR-Marigold-PA_vsys1_VR1

Requested Traffic

| SOURCE | USER | DESTINATION | APPLICATION | SERVICE |
|---|---|---|---|---|
| 10.40.2.66 | Any | 10.60.2.66 | Any | tcp/16995 |

Details

Based on configuration from 2019-01-04 01:06

Relevant Configured Behaviors (Implicit Rules) (1)

| NO. | RULE |
|---|---|
| 1 | ethernet1_5_13 |

Support Information

6. To add comments, scroll down to the **Implementation Notes** area at the bottom, and

click **Edit**.

Enter your comment in the text box, and then click **OK** back up at the top.

Your work order is updated.

## Work order recommendation details

Work order recommendations and editing scope vary greatly, depending on your scenario, configurations, and device types. For example:

- Fields where *exactly one* suitable option exists will be pre-filled with the relevant option and read-only.
- If no suitable object option exists, you may be able to enter the name of a new object to create. Your object name must be valid and unique.
- For source, destination, and service fields, use the Advanced Editing wizard to access additional options. For details, see The Advanced Editing wizard

For more details, see:

- Traffic already partially blocked or allowed
- Editing rule names
- Creating new rules instead of modifying existing ones
- Policy-Based change requests
- Zone spanning support
- Layer 3 Protocols
- Cloud device behavior
- Cisco ACI device behavior
- Junos Space Security Director behavior

### Traffic already partially blocked or allowed

IP ranges are not split for the sake of omitting irrelevant traffic from the work order recommendations. This means:

- If the action is **Drop**, and some of the traffic is already blocked, the work order will suggest blocking all the traffic, including traffic that is already blocked.
- If some of the requested traffic is already allowed, work orders may still recommend allowing that traffic.

### Editing rule names

Editing a work order enables you to manually enter a new name, or FireFlow can be configured to automatically set a rule name via a hook.

**Tip:** We recommend consulting with AlgoSec professional services when configuring a hook to set rule names.

### Creating new rules instead of modifying existing ones

FireFlow may be configured as follows:

- **Always recommend creating a new rule.** The New Rule button does not appear in this case, and FireFlow recommends creating new rules by default.
- **Allow new users to add new rules instead of modifying existing ones.** In this case, click the **New Rule** button instead of **Recalculate**. Clicking **Recalculate** will always prefer a modify rule recommendation.
- **Prevent new rules**. If FireFlow is not configured to create new rules at all, the New Rule button does not appear, and FireFlow always recommends modifying rules.

### Policy-Based change requests

FireFlow uses policy-based change requests for Palo Alto Networks Panorama, Check Point, Fortinet Fortimanager, and Junos Space Security Director.

In the work order, FireFlow will choose objects from the same domain in which the policy exists, or higher domains. FireFlow will recommend installing the change on all devices with the policy. If desired, you can set FireFlow to only install changes on the relevant devices or simply to always use device-based change requests.

### Zone spanning support

Zone spanning support differs as follows:

| | |
|---|---|
| **Juniper devices** | Zone spanning support for Juniper devices includes only Junos Space Security Directors. For all other Juniper devices, the work order will always recommend adding a single rule even though you must add 2 or more rules (one for each source zone / destination zone pair).<br>When ActiveChange is enabled for Juniper devices which do not support zone spanning, CLI generation will fail when zone spanning occurs.<br>You can edit the CLI command field and still use ActiveChange to execute the commands directly from FireFlow. See Implement changes with ActiveChange. |
| **Palo Alto and Fortinet Devices** | By default, when a rule with zone spanning is recommended for Palo Alto or Fortinet devices, FireFlow will recommend the zone "any".<br>If desired, you can configure FireFlow to recommend the specific multiple zones. |

### Layer 3 Protocols

For layer 3 protocols (non-TCP/UDP/ICMP), the work order will only recommend using services that are already defined on the device. FireFlow will not recommend adding a new service for these protocols.

If the layer 3 protocol that was used in the change request is not found on the device, FireFlow issues a warning, and in the case when CLI recommendations would have been generated, they are aborted. For more details, see Change request field references.

### Cisco ACI device behavior

Default recommendations will be to remove allowing rules.

Editing a request for Cisco ACI devices enables you to change details such as rule name, application profile, and service graph, as well as the EPG values selected for the new rule.

The work order will never recommend editing an existing contract (only adding a new one).

### FireFlow support for EPGs

- When relevant, FireFlow will first look for an EPG that matches the request exactly. If none is found, the narrowest existing EPG that satisfies the requirements will be automatically suggested.
- If no relevant EPG exists at all, FireFlow will create a new one as part of the request.

### FireFlow support for application profiles

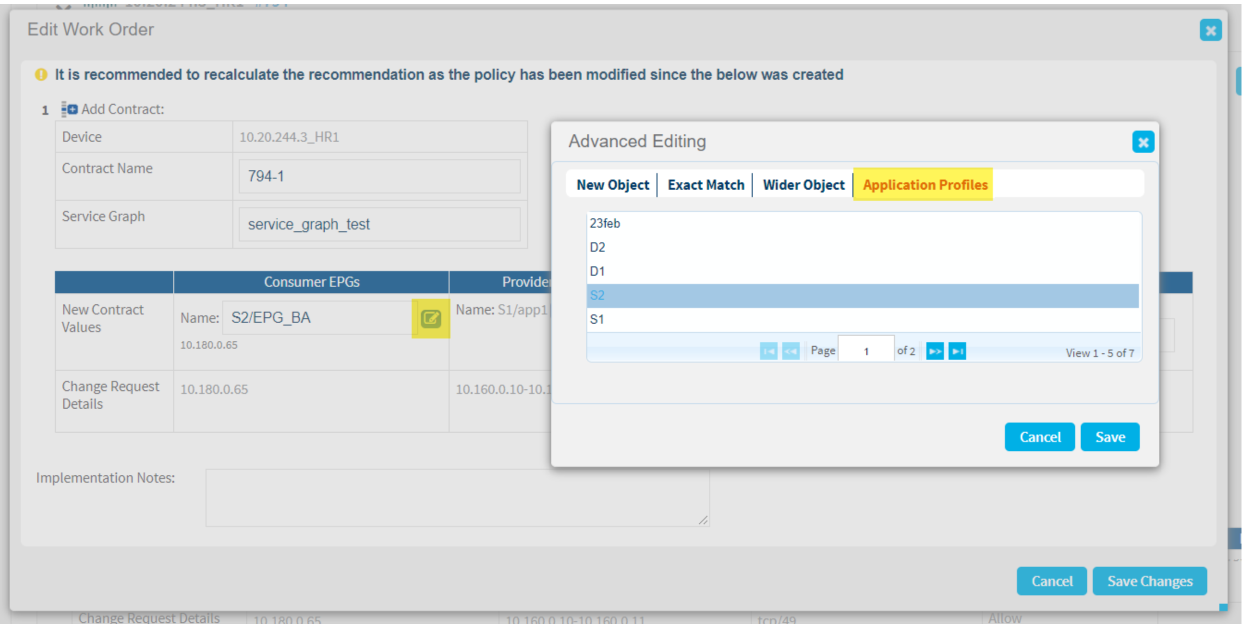
For traffic change requests for IP addresses that are not sub-sets of existing EPGs, the work order will recommend creating a new EPG. Application profiles are handled as follows:

- **If the application profile is known**, either from another EPG in the traffic line, or because the user has edited the work order, an EPG is created under the same application profile.
- **When multiple application profiles are known**, the EPG is created with one of them only.
- **If no application profile is known**, ActiveChange is disabled, and the user is prompted to specify the application profile. In such cases, add an application profile by editing the work order.

### Advanced editing for EPGs

The Edit Work order dialog enables you to make changes to your work order, including to any new EPGs being created. For example, modify the name for a new EPG in the **Name** field, or click the **Advanced Editing** button to make additional changes.

The following image shows an example of how to select an Application Profile for a new Consumer EPG:



Edit Work Order

It is recommended to recalculate the recommendation as the policy has been modified since the below was created

1 Add Contract:

| | |
|---|---|
| Device | 10.20.244.3_HR1 |
| Contract Name | 794-1 |
| Service Graph | service_graph_test |

| | Consumer EPGs | Provide |
|---|---|---|
| New Contract Values | Name: S2/EPG_BA<br>10.180.0.65 | Name: S1/app1 |
| Change Request Details | 10.180.0.65 | 10.160.0.10-10.1 |

Implementation Notes:

Advanced Editing

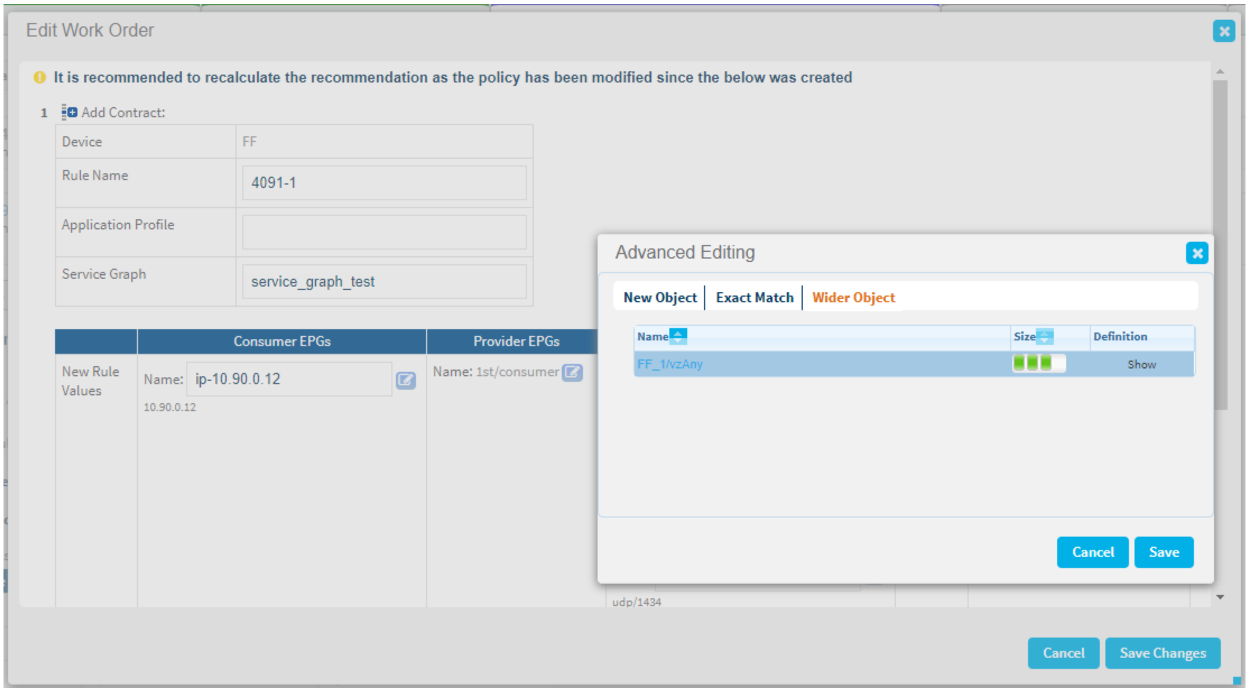
| |
|---|
| 23feb |
| D2 |
| D1 |
| S2 |
| S1 |

Page 1 of 2 View 1 - 5 of 7

### vzAny objects

By default, **vzAny** objects are not selected, but you can edit the change request to select them manually.

For example:



It is recommended to recalculate the recommendation as the policy has been modified since the below was created

1 Add Contract:

| | |
|---|---|
| Device | FF |
| Rule Name | 4091-1 |
| Application Profile | |
| Service Graph | service_graph_test |

| | Consumer EPGs | Provider EPGs |
|---|---|---|
| New Rule Values | Name: ip-10.90.0.12<br>10.90.0.12 | Name: 1st/consumer |

| Name | Size | Definition |
|---|---|---|
| FF_1/vzAny | | Show |

udp/1434

### Cloud device behavior

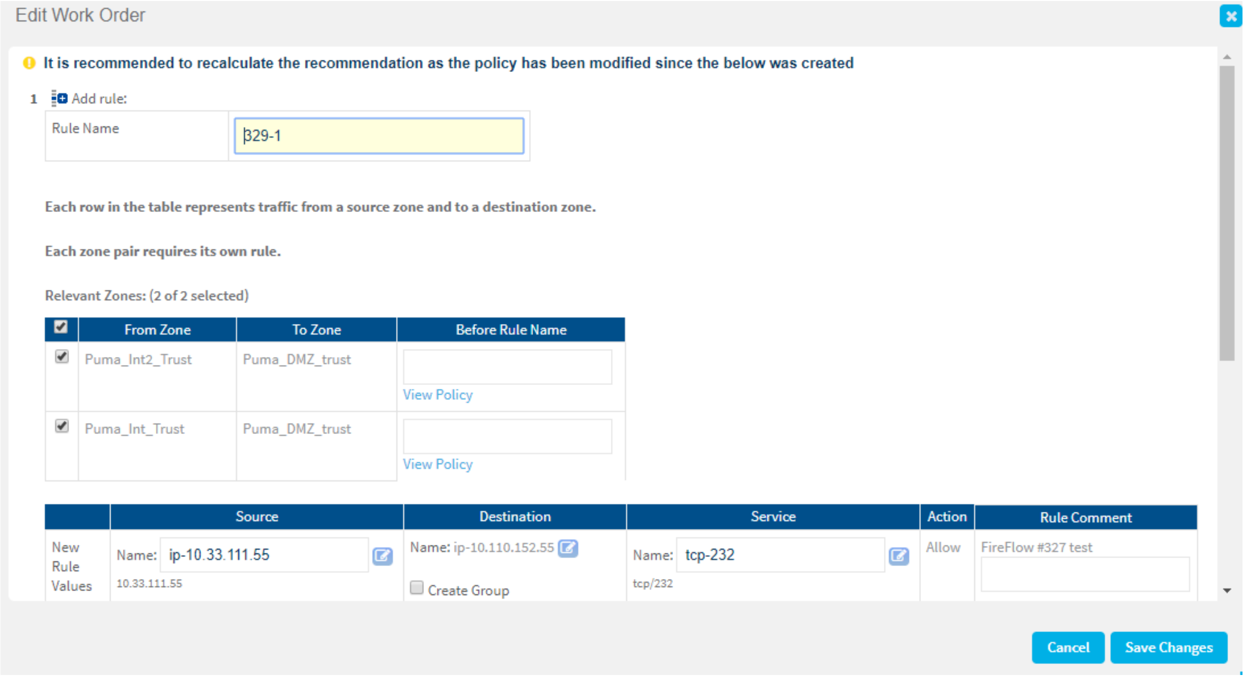
Cloud device behavior differs as follows:

| | |
|---|---|
| **Amazon Web Services (AWS)** | FireFlow will never recommend changing the rules in the NACL. If the traffic is completely blocked by the NACL, a warning appears in the work order stating this is the case. If the traffic is only partially blocked, a warning appears stating that the traffic might be blocked by the NACL.<br>If the relevant security group is full, a message appears. You must create a new security group and re-plan the change request. |
| **Microsoft Azure** | If a security set has only one network security group or subnet network security group, FireFlow will recommend changing it. If a security set has a network security group and a subnet network security group, FireFlow will not recommend changing the subnet network security group (even when it blocks the desired traffic).<br>If the relevant network security group is full, a message appears. |

### Junos Space Security Director behavior

For Junos Space Security Director recommendations with zone spanning, you can deselect source / destination zone pairs for which you do not want to create a new rule.

For example:



Edit Work Order

It is recommended to recalculate the recommendation as the policy has been modified since the below was created

1 Add rule:

| | |
|---|---|
| Rule Name | 329-1 |

Each row in the table represents traffic from a source zone and to a destination zone.

Each zone pair requires its own rule.

Relevant Zones: (2 of 2 selected)

| ☑ | From Zone | To Zone | Before Rule Name |
|---|---|---|---|
| ☑ | Puma_Int2_Trust | Puma_DMZ_trust | View Policy |
| ☑ | Puma_Int_Trust | Puma_DMZ_trust | View Policy |

| | Source | Destination | Service | Action | Rule Comment |
|---|---|---|---|---|---|
| New Rule Values | Name: ip-10.33.111.55<br>10.33.111.55 | Name: ip-10.110.152.55<br>□ Create Group | Name: tcp-232<br>tcp/232 | Allow | FireFlow #327 test |

# Implement changes with ActiveChange

Use FireFlow's ActiveChange functionality to implement changes directly from FireFlow on any relevant devices.

## Implement changes from FireFlow

Implementing changes on your devices directly from FireFlow is supported when all of the following conditions are met:

- **ActiveChange is supported for the device.**
- **ActiveChange is enabled for the device in AFA.**
- **The change request's workflow is supported for the device brand.**

  All devices that support ActiveChange are supported for traffic and rule removal requests.

  Additionally, some device types support the multi-device object change requests.

For more details, see the Support Matrix on the AlgoSec portal.

### Additional details for Cisco and Juniper devices

For Cisco and Juniper devices, ActiveChange generates CLI commands to implement the changes suggested in the work order.

FireFlow provides the opportunity to edit the CLI commands and then execute them on the device, pushing the changes directly to the device.

The following is relevant only to Cisco and Juniper devices:

- You must ensure that no changes are made to the device between the time that ASMS generates the CLI commands and implements them on the device.

  If you find that changes may have been made, click **Recalculate** to recalculate the work order before you implement the commands.

- ActiveChange CLI generation is only supported for Juniper SRX and Netscreen when the device is managed locally, not when the device is managed by NSM or Space. This is true even if the device is defined directly in AFA (without the NSM or Space).
- For work orders with IPv6 traffic, you must attach the IPv6 ACL to an interface (access group syntax) before ASMS can generate the CLI commands.

**Note:** By default, any new rules are created with logging enabled, and logging is set to the default log level.

Do one of the following:

- Implement changes across all devices and policies
- Implement changes on a single device

## Implement changes across all devices and policies

This procedure describes how to use ActiveChange to implement changes for all relevant devices and policies simultaneously.

**Tip:** Alternately, see Implement changes on a single device.

Do the following:

1. **Optional, Cisco / Juniper only: Edit the CLI commands**

   To edit your CLI commands, do the following:

   a. Click **Modify** in the **Implementation Recommendation** area.

      The **Modify Implementation Recommendation** window appears.

   b. In the **Implementation Recommendation** field, edit the CLI commands for your specific requirements.

   c. Click **OK**.

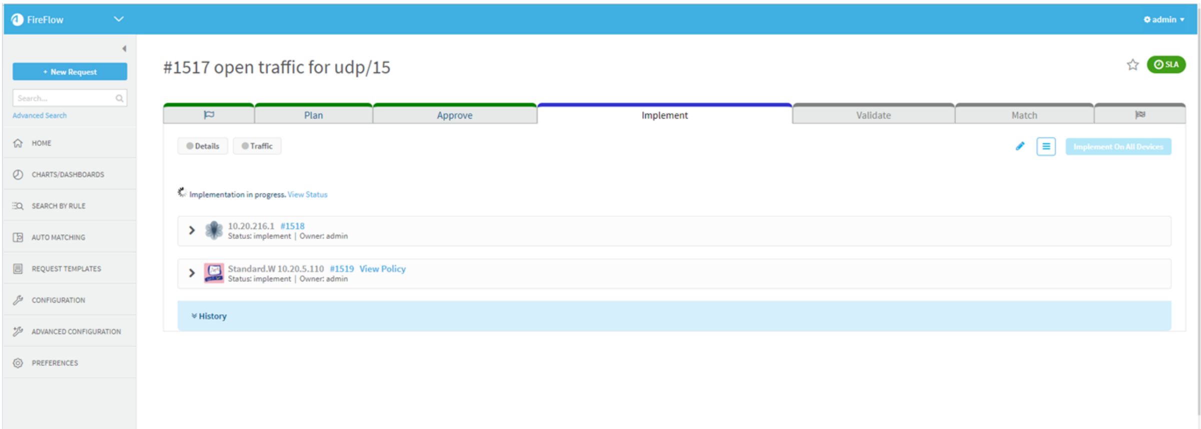
      The CLI commands are saved, and the work order is grayed out (because the work order does not reflect the CLI commands). In this case, the work order will be ignored during the Validate stage.

   d. To discard edits you have made and return to the CLI commands which reflect the work order, click **Regenerate CLI**.

   For more details, see Additional details for Cisco and Juniper devices.

2. Click **Implement On All Devices**.

   The **View Status** link appears.



#1517 open traffic for udp/15

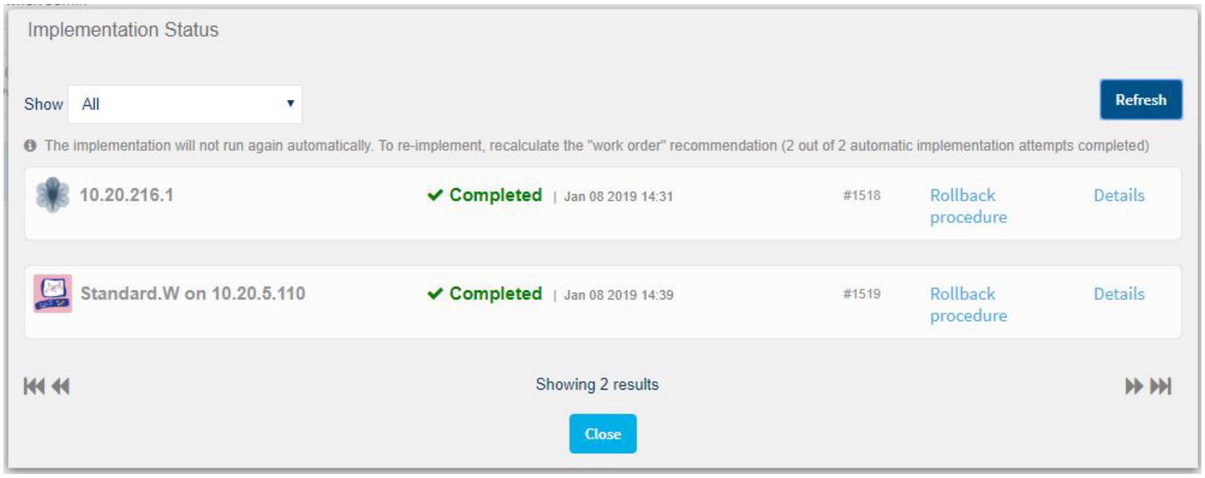
Implementation in progress. View Status

10.20.216.1 #1518
Status: implement | Owner: admin

Standard.W 10.20.5.110 #1519 View Policy
Status: implement | Owner: admin

3. To view the implementation status, click **View Status**.

   The **Implementation Status** dialog box appears.



Implementation Status

Show: All

The implementation will not run again automatically. To re-implement, recalculate the "work order" recommendation (2 out of 2 automatic implementation attempts completed)

10.20.216.1 ✓ Completed | Jan 08 2019 14:31 #1518 Rollback procedure Details

Standard.W on 10.20.5.110 ✓ Completed | Jan 08 2019 14:39 #1519 Rollback procedure Details

Showing 2 results

Each device will have one of the following statuses:

| | |
|---|---|
| **In progress** | The implementation is in progress. |
| **Completed** | The implementation successfully completed. |
| **Failed** | The implementation failed. |
| **Not supported** | The device brand is not supported in the **Implementation Status** page. |
| **Inapplicable CLI command** | There is a problem with the CLI commands that were used to implement the changes on the device.<br>Do any of the following:<br>• Click **Rollback procedure** to display instructions for how to reverse the changes done to the device.<br>• Click **Details** to display the device's response.<br>• Click **Error details** to display a description of the error.<br>• Filter the devices in the list by status by selecting a status in the **Show only** drop-down menu. |

**Note:** The **Implementation Status** dialog box only is relevant only for devices

> which Active Change supports. Other devices will appear, but their status will always be **Not supported**.

> **Note:** If implementation fails on a Juniper SRX or Netscreen, the changes are automatically rolled back, and a note in the status states the device has not been changed.

4. If devices that are not supported for automatic implementation are included in the change request, implement changes on these devices manually. For details, see Implement changes.
5. If you implemented changes manually on any devices, click **Mark All As Implemented**.
6. Click **OK**.

   The change is implemented on the device policy, and the change request proceeds to the Validate stage.

## Implement changes on a single device

This procedure describes how to use ActiveChange to implement changes on a single device at a time.

> **Tip:** Alternately, see Implement changes across all devices and policies.

Do the following:

1. If you are working with a request with multiple devices or policies, click ▶ next to a device.

   The device's or policy's action buttons appear below the device or policy panel.
2. Click **Implement On Device**.

   The **View Status** link appears. See above for more information.

3. If the change request includes multiple devices or policies, repeat the previous step for each device.

   If devices that are not supported for automatic implementation are included in the change request, implement changes on these devices manually. See Implement changes.

4. If you implemented changes manually on any devices, click **Mark All As Implemented**.

5. Click **OK**.

   The change is implemented on the device policy, and the change request proceeds to the Validate stage.

## Implement changes via CLI

FireFlow provides the recommended CLI commands for implementing work orders on Cisco or Juniper devices that meet the following conditions:

- The device is a Cisco or Juniper device that supports ActiveChange.

  For Juniper SRX and Netscreen devices, the device must be managed locally, and not by NSM or Space. This is true even if the device is defined directly in AFA, without the NSM or Space.

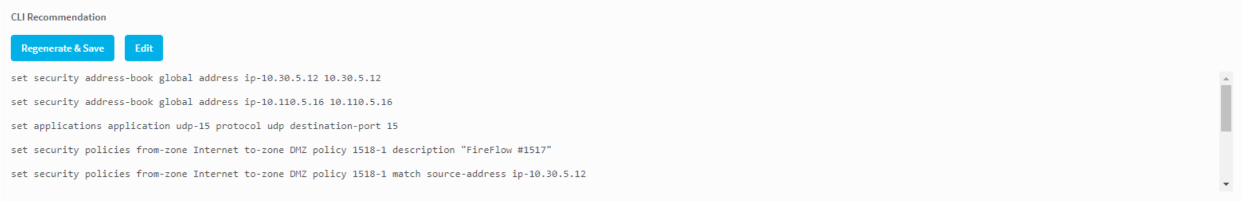
- ActiveChange is enabled for the device in AFA
- The change request is a traffic request or rule removal request.
- For work orders with IPv6 traffic, you must attach the IPv6 ACL to an interface (access group syntax) before ASMS can generate the CLI commands.

**Note:** Do not make changes on the device policy after FireFlow generates the CLI commands but before implementing the recommended changes.

If changes may have been made, click **Recalculate** to recalculate the work order before implementing the recommended commands.

The **CLI Recommendation** area shows the series of CLI commands that represent the changes to make on your device.

For example:



```
set security address-book global address ip-10.30.5.12 10.30.5.12
set security address-book global address ip-10.110.5.16 10.110.5.16
set applications application udp-15 protocol udp destination-port 15
set security policies from-zone Internet to-zone DMZ policy 1518-1 description "FireFlow #1517"
set security policies from-zone Internet to-zone DMZ policy 1518-1 match source-address ip-10.30.5.12
```

Do the following:

- (Optional) Edit the CLI commands:
- Implement the CLI commands

## (Optional) Edit the CLI commands:

1. Click **Modify** in the **Implementation Recommendation** area.

   The **Modify Implementation Recommendation** window appears.

2. In the **Implementation Recommendation** field, edit the CLI commands for your specific requirements.

3. Click **OK**.

   The CLI commands are saved, and the work order is grayed out (because the work order does not reflect the CLI commands). In this case, the work order will be ignored during the Validate stage.

4. To discard edits you have made and return to the CLI commands which reflect the work order, click **Regenerate CLI**.

## Implement the CLI commands

1. Copy the list of recommended CLI commands that appear in the **Implementation Recommendation** section of the work order, and then paste them to the device's

command line.

2. When you have completed implementation, do *one* of the following:

| | |
|---|---|
| **Requests with multiple devices or policies** | Confirm implementation has been completed for every device/policy as follows:<br>a. Click **Mark All Sub Requests As Implemented**.<br>A confirmation message appears.<br>b. Click **OK**. |
| **Requests with a single device or policy** | Confirm that implementation is completed as follows:<br>a. Display the device's change request information by clicking ▸ next to the device.<br>The device's action buttons, and the **Work Order Recommendations** area appear below the device panel.<br>b. Click **Implementation Done**. |
| **Requests with no devices or policies** | Click **Implementation Done**. |

# Validate changes

**Relevant for: Requestors and network operations users**

Once the changes specified by a change request have been implemented, the change request moves on to the Validate stage.

This section explains how to validate implemented changes.

> **Note:** To determine a change request's stage, view the change request. The stage is indicated by the Change Request Lifecycle Status Bar. For details, see View change requests.

## Validation processes per type

The following table describes the change request validation process, depending on the type of change request:

| | |
|---|---|
| **Traffic change requests** | The following process occurs:<br>1. A network operations user validates the implemented changes against the change request, to verify that the specified traffic has been allowed or blocked as required.<br>2. If validation indicates that the implemented changes did *not* achieve the desired result specified in the change request, then the network operations user re-initiates the implementation stage and repeats change validation until the change is successful.<br>3. When ready, the network operations user notifies the requestor that the changes were implemented.<br>4. The requestor then verifies that the desired result was achieved.<br>5. Depending on the results of the requestor's check, the network operations user either re-initiates the implementation stage, or resolves the change request. |

| | |
|---|---|
| **Object change requests** | The following process occurs:<br>1. A network operations user validates the implemented changes against the change request, to verify that the specified object change has been made.<br>2. If validation indicates that the implemented changes did *not* achieve the desired result specified in the change request, then the network operations user re-initiates the implementation stage and repeats change validation until the change is successful.<br>3. Next, the network operations user notifies the requestor that the changes were implemented.<br>4. The network operations user then immediately resolves the change request, without waiting for a response from the requestor. |
| **Rule removal change requests** | The following process occurs:<br>1. A network operations user validates the implemented changes against the change request, to verify that the work order recommendations have been implemented.<br>2. If validation indicates that the implemented changes did *not* achieve the desired result specified in the change request, then the network operations user re-initiates the implementation stage and repeats change validation until the change is successful.<br>3. The network operations user then resolves the change request. |
| **Rule modification change requests** | |
| **Recertification change requests** | |

| | |
|---|---|
| **Multi-device object change requests** | The following process occurs:<br>1. The network operations user does not validate changes. Instead, the network operations user immediately notifies the requestor that the changes were implemented.<br>2. The requestor then verifies that the desired result was achieved.<br>3. Depending on the results of the requestor's check, the network operations user either re-initiates the implementation stage, or resolves the change request. |
| **IPv6 traffic change requests** | |
| **Multicast traffic change requests** | |
| **Web filtering change requests** | |

For details, see:

- Verify change request results
- Notify change requestors
- Resolve or return change requests
- Report change verifications

## Verify change request results

**Relevant for: Network operations users and requestors**

This topic describes how to verify change validation results.

**Tip:** After making a change, you may want to wait a few minutes before validating the change. FireFlow can only detect changes after an AFA analysis has been run on the device.

In systems with scheduled monitoring configured, you must wait for the scheduled monitoring process to run.

### Verify change validation results (requestors)

**Relevant for: Requestors**

Once the device changes planned for your change request have been implemented, you will receive an email message from FireFlow, asking you to verify that the changes were implemented successfully.

You must check that the desired results were achieved, and respond in one of the following ways:

- Respond directly to the email message. For details, see Respond to change requests.
- Respond via the Web interface. For details, see Report change verifications.

If your response indicates that the desired results were not achieved, your change request will be re-implemented and you will be asked to check the results again.

If your response indicates that you are satisfied with the results, the change request will be resolved.

## Verify change validation results (network operations users)

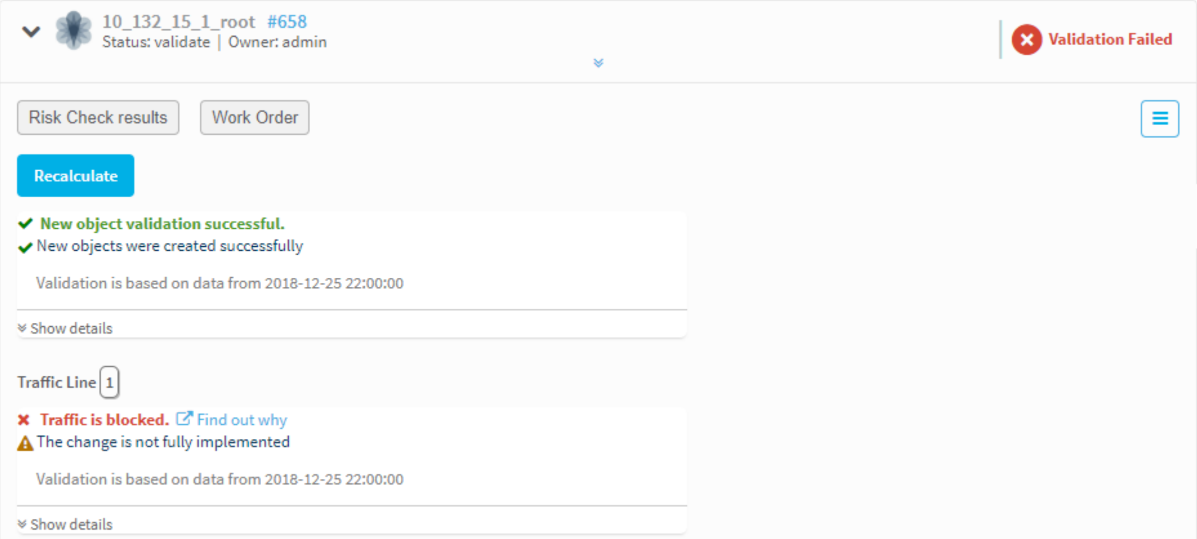
This procedure describes how network operations users can verify change validation results.

### Do the following:

1. View the change request. For details, see View change requests.
2. If the validation results are not available or old, refresh the validation calculation by clicking **Recalculate**.

   The change validation results appear, indicating whether the implemented changes achieved the result specified in the change request.

   For example:



10_132_15_1_root #658
Status: validate | Owner: admin

Validation Failed

✓ New object validation successful.
✓ New objects were created successfully

Validation is based on data from 2018-12-25 22:00:00

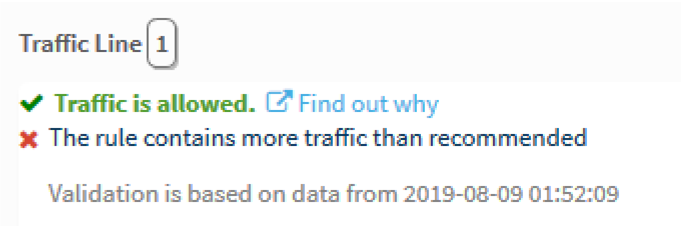
Traffic Line 1

✗ Traffic is blocked. Find out why
⚠ The change is not fully implemented

Validation is based on data from 2018-12-25 22:00:00

Details are shown as follows:

| | |
|---|---|
| **Object change, rule removal, and web filtering change requests** | The change validation verifies the changes specified in the work order were implemented by performing a traffic simulation query.<br>• Validation succeeds if the query indicates the planned changes specified in the work order have been made for every traffic line in the change request.<br>• Validation fails if the planned changes have not been made for at least one traffic line. |
| **Rule modification change requests** | The change validation displays whether the specified changes in the work order match the device policy.<br>For more details, see Advanced change validation results. |

| | |
|---|---|
| **Traffic change and recertification requests** | The change validation verifies the changes specified in the work order were implemented with a traffic simulation query and a work order/device policy comparison.<br>If the rule contains more traffic than recommended, FireFlow indicates this for you so that you can take any action, as required.<br>For example:<br><br>Traffic Line 1<br>✓ Traffic is allowed. Find out why<br>✗ The rule contains more traffic than recommended<br>Validation is based on data from 2019-08-09 01:52:09<br>For more details, see Advanced change validation results. |

**Note:** If you implemented the changes even slightly differently than the work order, Validation will fail.

For example, if the work order specified one rule with multiple sources, and you added multiple rules (with one source each), Validation will fail.

This is particularly relevant for Amazon Web Services because rules can only include one object per field.

3. To view extended information about the change validation, click **Show details**.
4. If you do not see that the result you wanted was implemented, view device reports describing the problem by clicking the **Find out why** link.

   A report opens in a new window, and you can drill down to view the relevant device rules.

   **Note:** This option is not available for rule removal or rule modification requests.

5. Click **Next**.
6. If the desired result was not achieved, do the following:

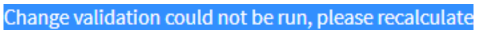
a. Re-implement the change(s). For details, see [Resolve or return change requests]().

b. Repeat change validation.

### Palo Alto Networks devices

For Palo Alto Networks Panorama devices, FireFlow will always recommend changing the lowest device group. If a higher level device group blocks the traffic the change request is attempting to allow, the traffic will still not be allowed after the work order is implemented, and validation will fail. To allow the traffic you must manually change the higher level device group.

### Validation timeouts

If validation times out before the device has been analyzed,  Change validation could not be run, please recalculate appears.

## Advanced change validation results

Traffic change, recertification, and rule modification requests support advanced change validation results.

- **Traffic change** and **recertification** requests run a traffic simulation query and work order/ device policy comparison during validation.
- **Rule modification** requests run a work order/ device policy comparison only.

Each change request receives an overall validation result, and individual validation results for each traffic line.

- **If all traffic line validations are successful**, then the overall validation is successful.
- **If at least one traffic line validation partially succeeds or fails**, the overall validation fails.

### Perfect matches / more permissive rules

When the work order/ policy comparison determines a rule is a perfect match or more permissive, the change validation in addition 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.

### Advanced change validation failures

In certain circumstances, change validation will fail even when the work order was implemented as specified.

The following are possible reasons for change validation failure:

- The traffic is partially blocked by a rule that exists above the allowing rule. The partially blocking rule is not displayed in the validation details.
- Part of the traffic was already allowed by another rule that is located lower in the policy.
- The rule was added in incorrect zones/ interfaces.
- Both a perfectly matched object and a wider rule exist, but only one of them is being matched.

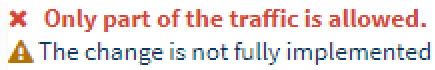
### Advanced change validation results per traffic line

Advanced change validation results are as follows, depending on the request type:

✓ Validation successful.

| | |
|---|---|
| **Traffic change/recertification requests** | • **"Allow" traffic**. Validation succeeds if the traffic simulation query indicates the planned traffic for the line is allowed, and the change on the device perfectly matches the work order recommendation.<br>• **"Drop" traffic**. Validation succeeds if the traffic simulation query indicates the planned traffic for the line is blocked, and no rule exists on the device with the relevant IUD. |

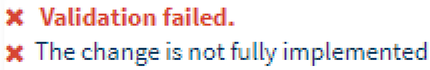
| | |
|---|---|
| **Rule modification requests** | Validation succeeds if the change on the device perfectly matches the work order recommendation. |



✖ Only part of the traffic is allowed.

⚠ The change is not fully implemented

| | |
|---|---|
| **Traffic change/recertification requests** | For "Allow" traffic, validation partially succeeds if the traffic simulation query indicates the planned traffic for the line is allowed, and the change on the device does not perfectly match the work order recommendation (but does not include traffic that is more permissive than the work order recommendation). |
| **Rule modification requests** | Validation partially succeeds if the change on the device does not perfectly match the work order recommendation, and does not include traffic that is wider than the work order recommendation. |



✖ Validation failed.

✖ The change is not fully implemented

| | |
|---|---|
| **Traffic change/recertification requests** | • **"Allow" traffic.** Validation fails if the traffic simulation indicates the planned traffic for the line is partially or fully blocked, or the change on the device is more permissive than the work order recommendation.<br>• **"Drop" traffic.** Validation fails if the traffic simulation query indicates the planned traffic for the line is partially or fully allowed, or a rule exists on the device with the relevant IUD. |
| **Rule modification requests** | Validation fails if the change on the device is more permissive than the work order recommendation. |

## Notify change requestors

**Relevant for: Network operations users**

This topic describes how network operations users can notify requestors that a change request was implemented.

For rule removal or drop traffic requests, the request may affect another change request submitted by you. In such cases, you may want to approve or decline this request.

> **Note:** To determine a change request's stage, view the change request. The stage is indicated by the **Change Request Lifecycle Status Bar**.

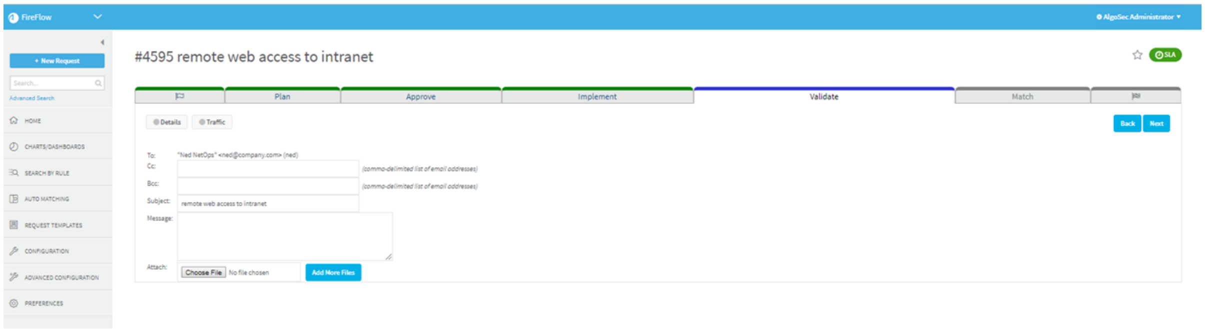
## Generic notification procedure

This procedure provide the steps to use when notifying requestors that a change request was implemented.

### Do the following:

1. View the change request. For details, see View change requests.
2. In the ☰ menu at the top right of the page, select **Notify Requestor**.

   The Notify Requestor page is displayed.

   #4595 remote web access to intranet

   To: "Ned NetOps" <ned@company.com> (ned)

   Cc: (comma-delimited list of email addresses)

   Bcc: (comma-delimited list of email addresses)

   Subject: remote web access to intranet

   Message:

   Attach: No file chosen

3. Complete the fields as needed. For details, see Respond to change requests.
4. Click **Next**.

FireFlow sends your message to the requestor.

The **Home** page appears.

## Respond to rule removal and drop traffic requests

Requestors with rules that are slated for removal or disablement must notify requestors of any change requests whose traffic intersects that of the selected rule. Likewise, requestors of traffic change requests with a **Drop** action must notify the requestors of any change requests whose traffic will be blocked by the **Drop** action.

Requestors of the affected change requests have until the request's due date to respond.

If you have received a rule removal or traffic change request notice, respond to either confirm or decline the change. If you do not respond by the due date, the request is considered to be confirmed.

Do one of the following:

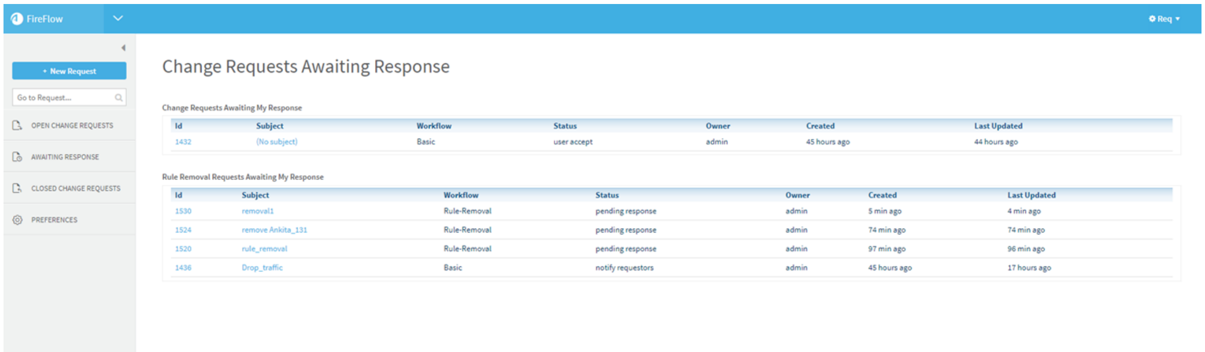
### Respond to rule removal requests

This procedure describes how to respond to a rule removal request.

Do the following:

1. In the main menu, click **Awaiting Response**.

   The **Change Requests Awaiting Response** page is displayed.



Change Requests Awaiting Response

Change Requests Awaiting My Response

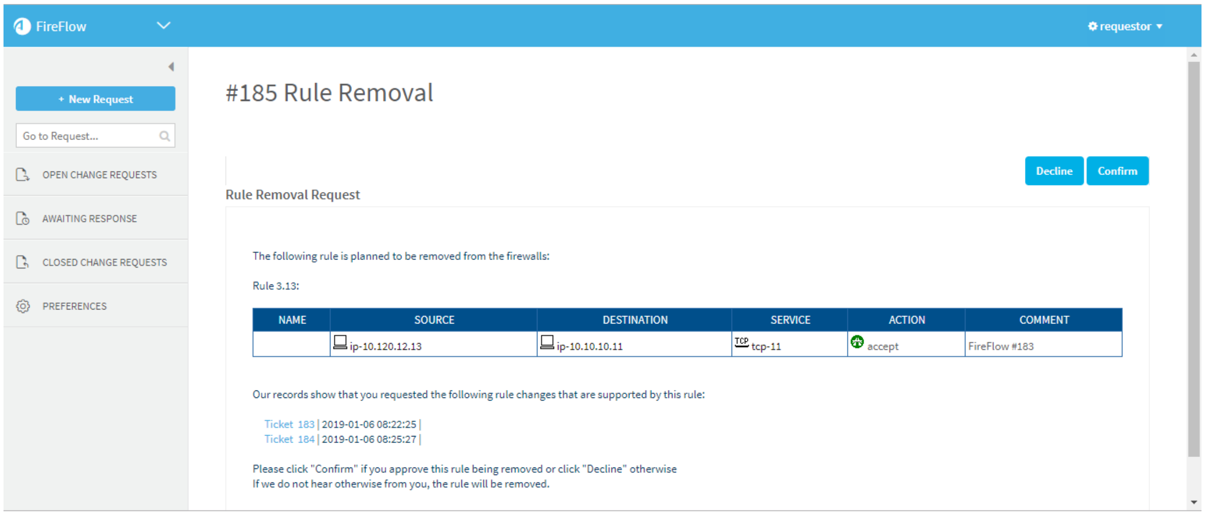
| Id | Subject | Workflow | Status | Owner | Created | Last Updated |
|---|---|---|---|---|---|---|
| 1432 | (No subject) | Basic | user accept | admin | 45 hours ago | 44 hours ago |

Rule Removal Requests Awaiting My Response

| Id | Subject | Workflow | Status | Owner | Created | Last Updated |
|---|---|---|---|---|---|---|
| 1530 | removal1 | Rule-Removal | pending response | admin | 5 min ago | 4 min ago |
| 1524 | remove Ankita_131 | Rule-Removal | pending response | admin | 74 min ago | 74 min ago |
| 1520 | rule_removal | Rule-Removal | pending response | admin | 97 min ago | 96 min ago |
| 1436 | Drop_traffic | Basic | notify requestors | admin | 45 hours ago | 17 hours ago |

2. In the **Rule Removal Requests Awaiting My Response** list, click the change request.

   The **Rule Removal Request** page is displayed.



#185 Rule Removal

Rule Removal Request

The following rule is planned to be removed from the firewalls:

Rule 3.13:

| NAME | SOURCE | DESTINATION | SERVICE | ACTION | COMMENT |
|---|---|---|---|---|---|
|  | ip-10.120.12.13 | ip-10.10.10.11 | tcp-11 | accept | FireFlow #183 |

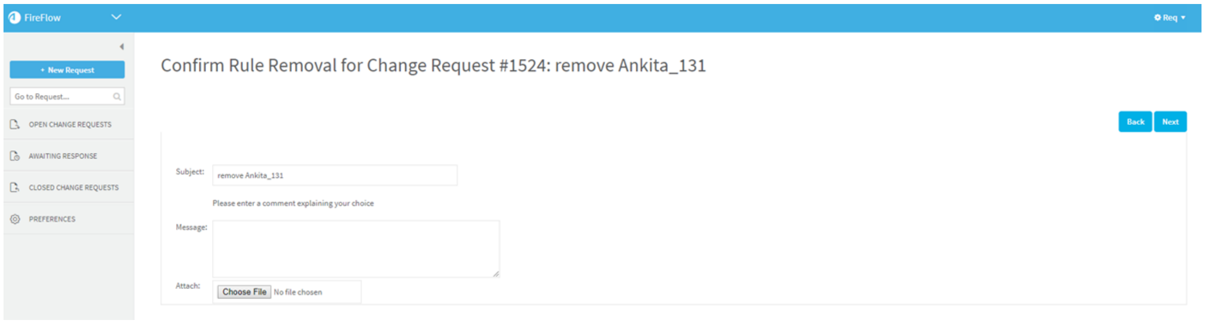
Our records show that you requested the following rule changes that are supported by this rule:

Ticket 183 | 2019-01-06 08:22:25 |
Ticket 184 | 2019-01-06 08:25:27 |

Please click "Confirm" if you approve this rule being removed or click "Decline" otherwise
If we do not hear otherwise from you, the rule will be removed.

3. At the top of the page, click **Confirm** to approve the rule deletion or **Decline** to decline the rule deletion.

   The **Confirm Rule Removal** or **Decline Rule Removal** page is displayed.



Confirm Rule Removal for Change Request #1524: remove Ankita_131

Subject: remove Ankita_131

Please enter a comment explaining your choice

Message:

Attach: No file chosen

4. Modify the **Subject** field to describe the subject of your comment.
5. To attach a file to your comment, do one of the following:
   - In the **Attach** field, type the path to the file.
   - Click **Browse**, browse to the desired file, and click **Open**.
6. In the **Message** text box, type your comment.
7. Click **Next**.

The Requestors Web Interface displays the change request, and your comment appears in the **History** area.

Your comment is sent as an email message to the change request's current owner.

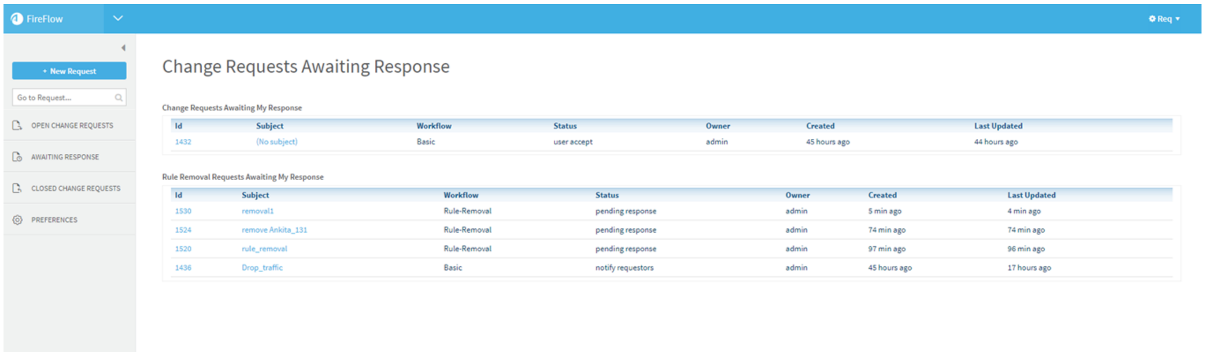
### Respond to drop traffic requests

This procedure describes how to respond to drop traffic requests.

Do the following:

1. In the main menu, click **Awaiting Response**.

   The **Change Requests Awaiting Response** page is displayed.



Change Requests Awaiting Response

Change Requests Awaiting My Response

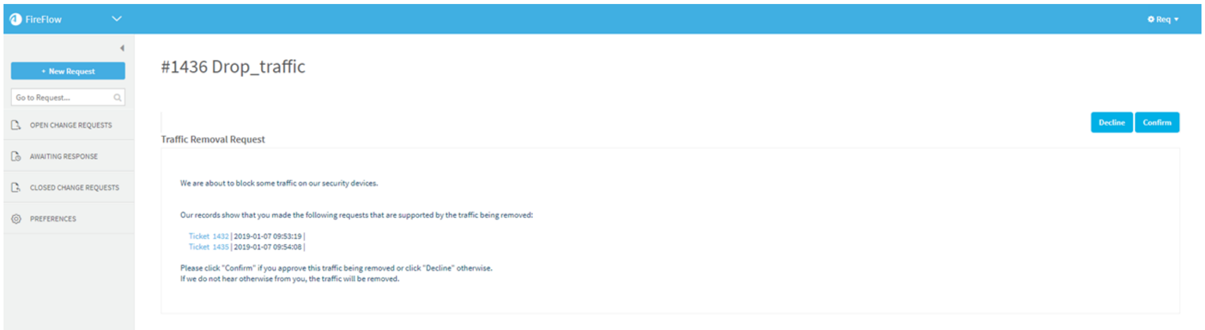
| Id | Subject | Workflow | Status | Owner | Created | Last Updated |
|---|---|---|---|---|---|---|
| 1432 | (No subject) | Basic | user accept | admin | 45 hours ago | 44 hours ago |

Rule Removal Requests Awaiting My Response

| Id | Subject | Workflow | Status | Owner | Created | Last Updated |
|---|---|---|---|---|---|---|
| 1530 | removal1 | Rule-Removal | pending response | admin | 5 min ago | 4 min ago |
| 1524 | remove Ankita_131 | Rule-Removal | pending response | admin | 74 min ago | 74 min ago |
| 1520 | rule_removal | Rule-Removal | pending response | admin | 97 min ago | 96 min ago |
| 1436 | Drop_traffic | Basic | notify requestors | admin | 45 hours ago | 17 hours ago |

2. In the **Change Requests Awaiting My Response** list, click the change request.

   The **Traffic Removal Request** page is displayed.



#1436 Drop_traffic

Traffic Removal Request

We are about to block some traffic on our security devices.

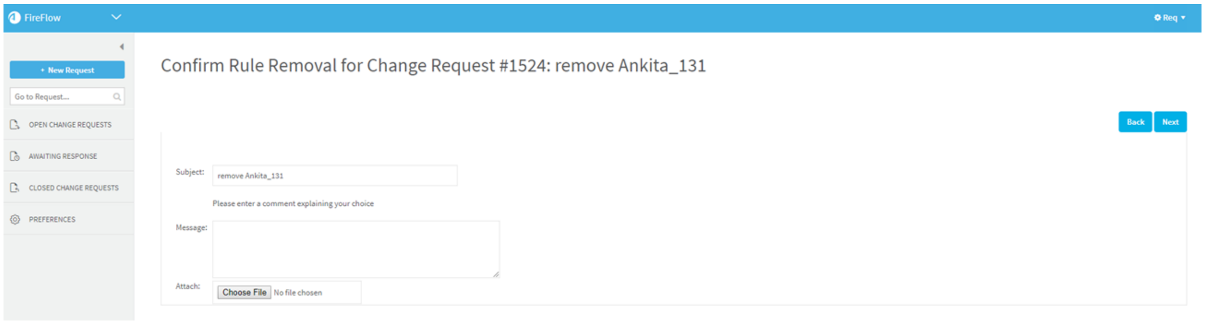
Our records show that you made the following requests that are supported by the traffic being removed:

Ticket 1432 | 2019-01-07 09:53:19 |
Ticket 1435 | 2019-01-07 09:54:08 |

Please click "Confirm" if you approve this traffic being removed or click "Decline" otherwise.
If we do not hear otherwise from you, the traffic will be removed.

3. At the top of the page, click **Confirm** to approve the rule deletion or **Decline** to decline the rule deletion.

The **Confirm Rule Removal** or **Decline Rule Removal** page is displayed.



Confirm Rule Removal for Change Request #1524: remove Ankita_131

Subject: remove Ankita_131

Please enter a comment explaining your choice

Message:

Attach: Choose File No file chosen

4. Modify the **Subject** field to describe the subject of your comment.
5. To attach a file to your comment, do one of the following:
   - In the **Attach** field, type the path to the file.
   - Click **Browse**, browse to the desired file, and click **Open**.
6. In the **Message** text box, type your comment.
7. Click **Next**.

The Requestors Web Interface displays the change request, and your comment appears in the **History** area.

Your comment is sent as an email message to the change request's current owner.

# Resolve or return change requests

**Relevant for: Network operations users**

This topic describes how network operations users can resolve a change request that has been implemented and validated correctly, or return the change request to an earlier stage in the workflow for more changes.

## Resolve a change request

If the requestor responded via email that the requested change was implemented successfully, you can resolve the change request.

> **Note:** If the requestor marked the change request as **Change Works** in the Requestor

Web Interface, then the change request has already been resolved, and you can skip this step.

### Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click **Resolve**.

If you are resolving a Web Filtering change request, a confirmation message appears. Click **OK**.

The change request is resolved, and FireFlow displays the change request.

The change request moves on to the **Match** stage. For more details, see Match changes to requests.

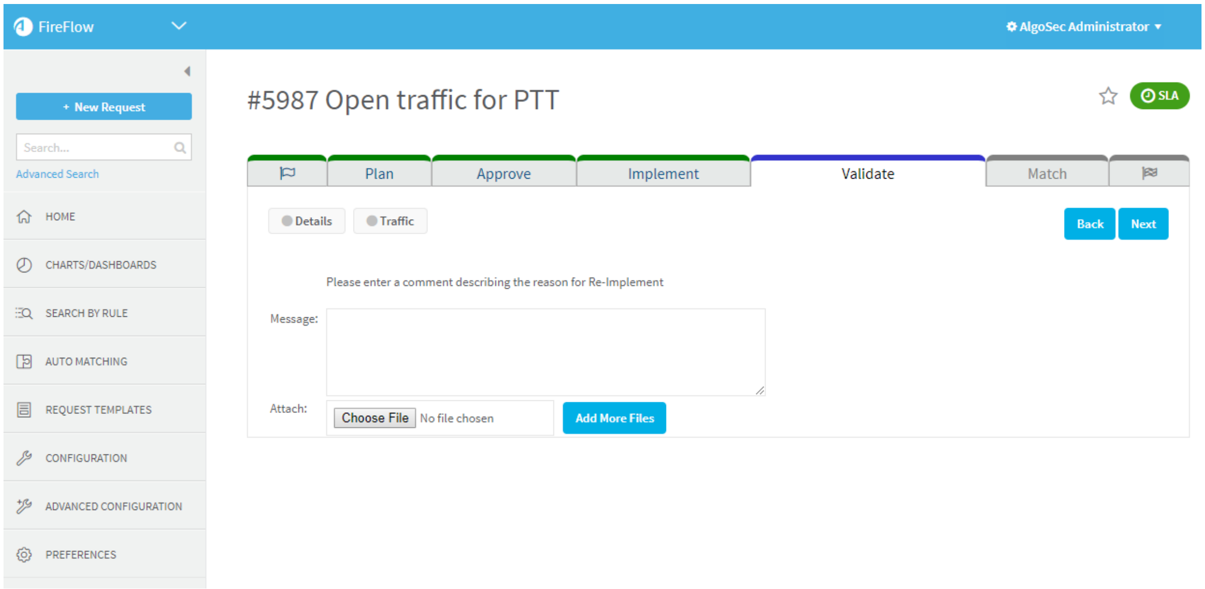
## Return a change request to the Implement stage

If the requester determined that the requested change was not implemented successfully, return the change request to the Implement stage for re-implementation.

### Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click **Re-Implement**.

   The Re-Implement Change Request page is displayed.



3. In the **Message** text box, type an explanation of why you are returning the change request to the Implement stage.
4. To attach files to your message:
   a. In the **Attach** field, do one of the following:
      - Type the path to the file in the field provided.
      - Click **Browse**, browse to the desired file, and click **Open**.

   b. To add more attachments, click **Add More Files** and repeat the previous step.
5. Click **Next**.

The change request is returned to the **Implement** stage for re-implementation.

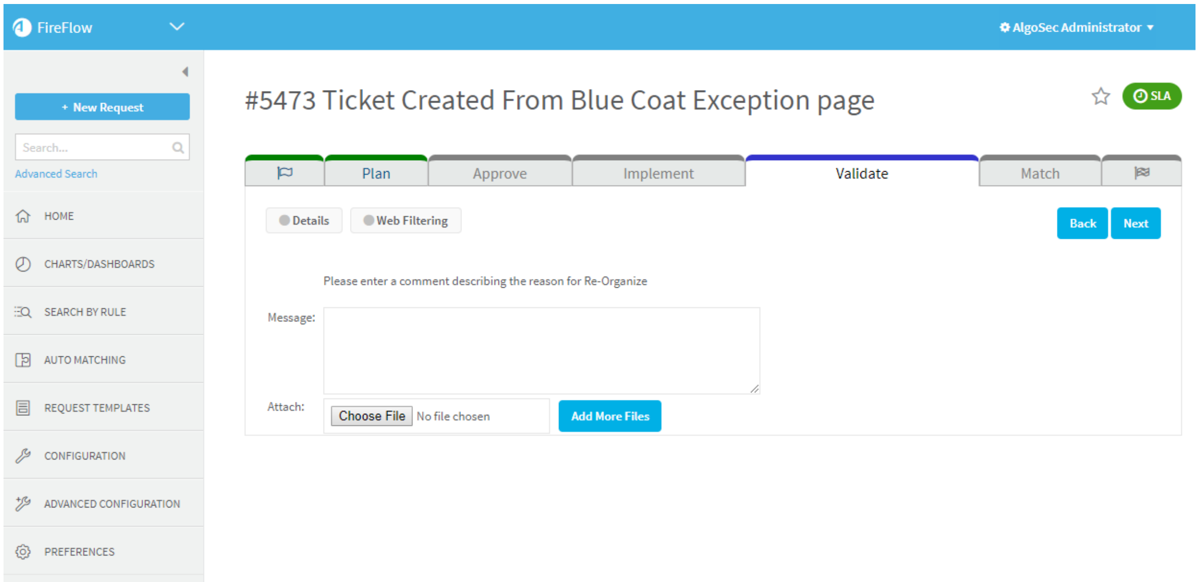
For more details, see Implement changes.

## Return a web filter change request for reorganization

### Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click **Re-Organize**.

   The **Message** field appears.



#5473 Ticket Created From Blue Coat Exception page

Please enter a comment describing the reason for Re-Organize

Message:

Attach: No file chosen

3. In the **Message** text box, type an explanation of why you are returning the change request for re-organization.
4. To attach files to your message:
   a. In the **Attach** field, do one of the following:
      - Type the path to the file in the field provided.
      - Click **Browse**, browse to the desired file, and click **Open**.

   b. To add more attachments, click **Add More Files** and repeat the previous step.
5. Click **Next**.

The change request is returned to the **Approve** stage for re-organization.

For more details, see Approve planned changes.

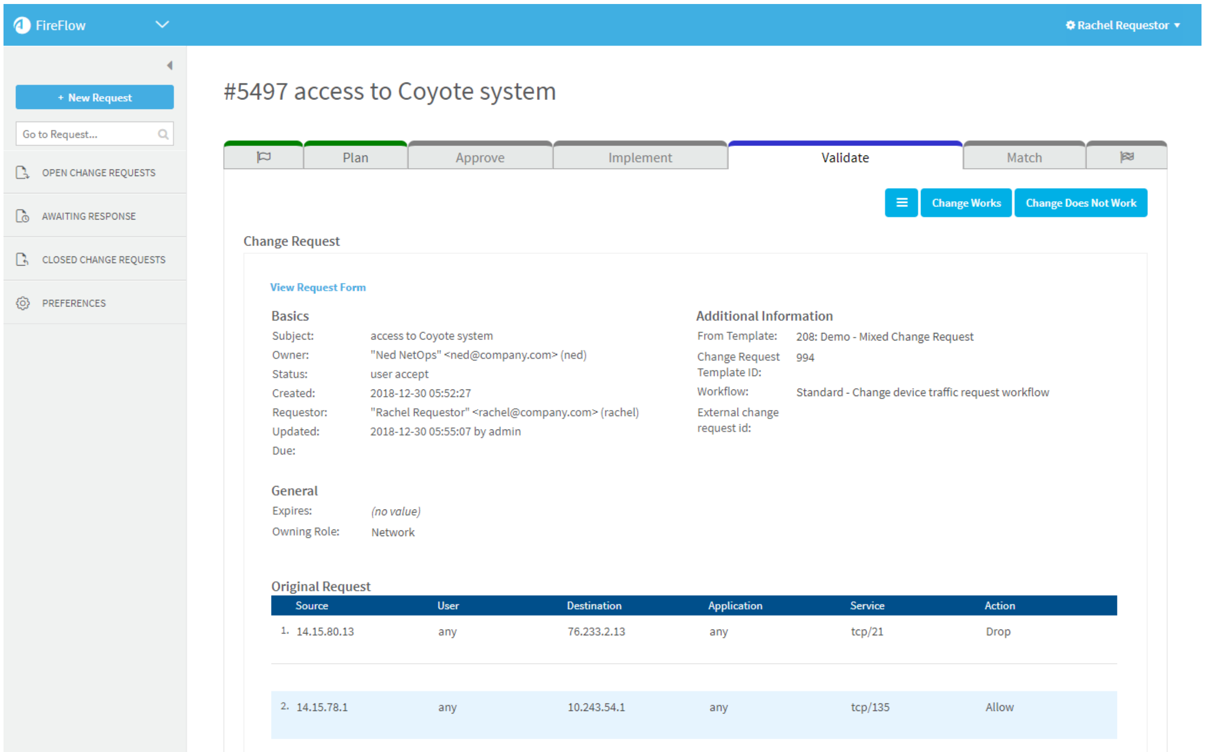
## Report change verifications

### Relevant for: All requestors

When asked to verify that the changes were implemented successfully, you can report your findings directly in FireFlow.

## Do the following:

1. View the change request. For details, see View change requests.



#5497 access to Coyote system

Change Request

Basics

Subject: access to Coyote system
Owner: "Ned NetOps" <ned@company.com> (ned)
Status: user accept
Created: 2018-12-30 05:52:27
Requestor: "Rachel Requestor" <rachel@company.com> (rachel)
Updated: 2018-12-30 05:55:07 by admin
Due:

Additional Information

From Template: 208: Demo - Mixed Change Request
Change Request Template ID: 994
Workflow: Standard - Change device traffic request workflow
External change request id:

General

Expires: *(no value)*
Owning Role: Network

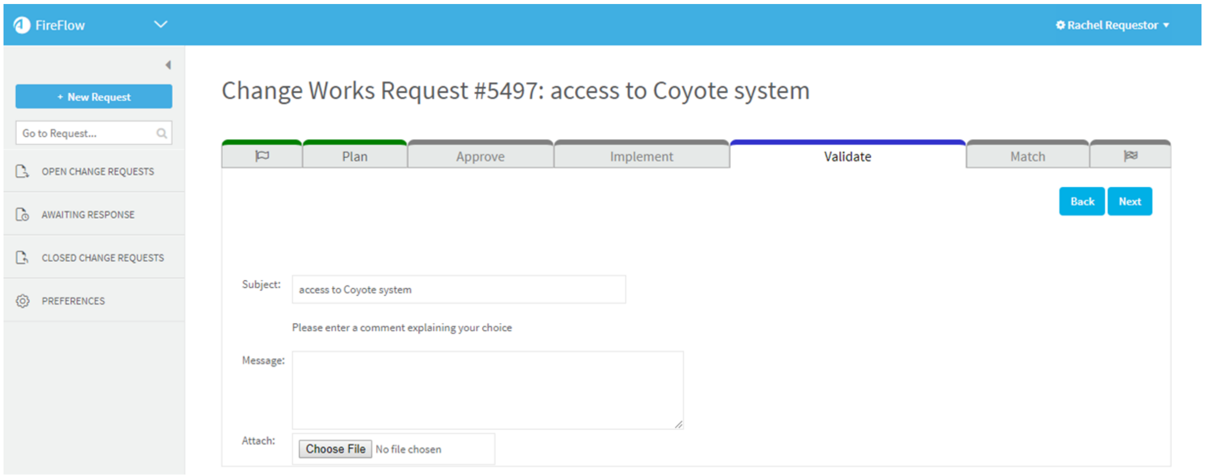
Original Request

| | Source | User | Destination | Application | Service | Action |
|---|---|---|---|---|---|---|
| 1. | 14.15.80.13 | any | 76.233.2.13 | any | tcp/21 | Drop |
| 2. | 14.15.78.1 | any | 10.243.54.1 | any | tcp/135 | Allow |

2. Do one of the following:

3. If the change works, at the top of the page, click **Change Works**. If the change does not work, click **Change Does Not Work**.

   The **Change Works** or **Change Does Not Work** page is displayed.



Change Works Request #5497: access to Coyote system

Subject: access to Coyote system

Please enter a comment explaining your choice

Message:

Attach: No file chosen

The **Subject** field displays the change request name.

4. If desired, modify the **Subject** field to describe the subject of your comment.
5. To attach a file to your comment, do one of the following:
    - In the **Attach** field, type the path to the file.
    - Click **Browse**, browse to the desired file, and click **Open**.
6. In the **Message** text box, type your comment.
7. Click **Next**.

The change request is displayed, and your comment appears in the **History** area.

Your comment is sent as an email message to the change request's current owner.

If you clicked **Change Works**, the change request is resolved.

# Match changes to requests

**Relevant for: Information security users**

This section describes how to manually match change requests to the actual changes made.

In most cases, once a change request has been resolved, the change is automatically matched to the relevant request, and no further action is required.

However, some workflows do not support auto-matching, and FireFlow may not be successful in finding a match for all changes.

We recommend checking weekly or monthly to verify that FireFlow matches the changes and change requests correctly.

**Note:** Auto Matching is not supported for the IPv6 traffic workflow. You must resolve change requests and changes for this workflow manually.

For more details, see:

- Auto-matching flow
- View matching results
- Resolve unmatched changes
- View and edit match records
- View and edit change records

**Note:** To determine a change request's stage, view the change request. The stage is indicated by the Change Request Lifecycle Status Bar. For details, see View change requests.

## Auto-matching flow

FireFlow periodically checks for changes in device policy rules and tries to match them to FireFlow change requests.

If FireFlow detects that a device rule was added or modified, it checks the rule's comment to look for a change request ID, and then handles it as follows:

| | |
|---|---|
| **Change request ID found** | If the comment contains a change request ID, FireFlow does the following:<br>1. Associates the change with the relevant change request. This is called an **ID match**.<br>2. Verifies that the added or modified rule allows the traffic that is approved in the change request, and nothing more or less.<br>3. Defines the change and change requests matching state as either a **Perfect Match**, or an item with **Action Required**.<br>Both types are listed in their relevant list on the **Auto Matching** page in FireFlow.<br>other perfectly.<br>**Note:** For change requests with multiple traffic requests, FireFlow performs ID matches only. |
| **No change request ID found** | If the comment does not contain a change request ID, the change appears in the **Auto Matching** page's **Action Required > Changes Without Request** sub-list.<br>This list also includes changes where FireFlow detects that a device rule was deleted. |

## Rule comment requirements

Change request IDs in the rule's comment must match the Change Request ID format configured in the workflow options.

The default format is as follows:

```
Before:                  FireFlow #Change Request Id:      \d+After:                   (nc
```

This format requires that the rule comment for change request #375 include the following text:

```
"FireFlow #357"
```

**Note:** If the system is configured to use a 3rd party change management system, the change request ID must match the 3rd party system requirements.

# View matching results

### Relevant for: Privileged users

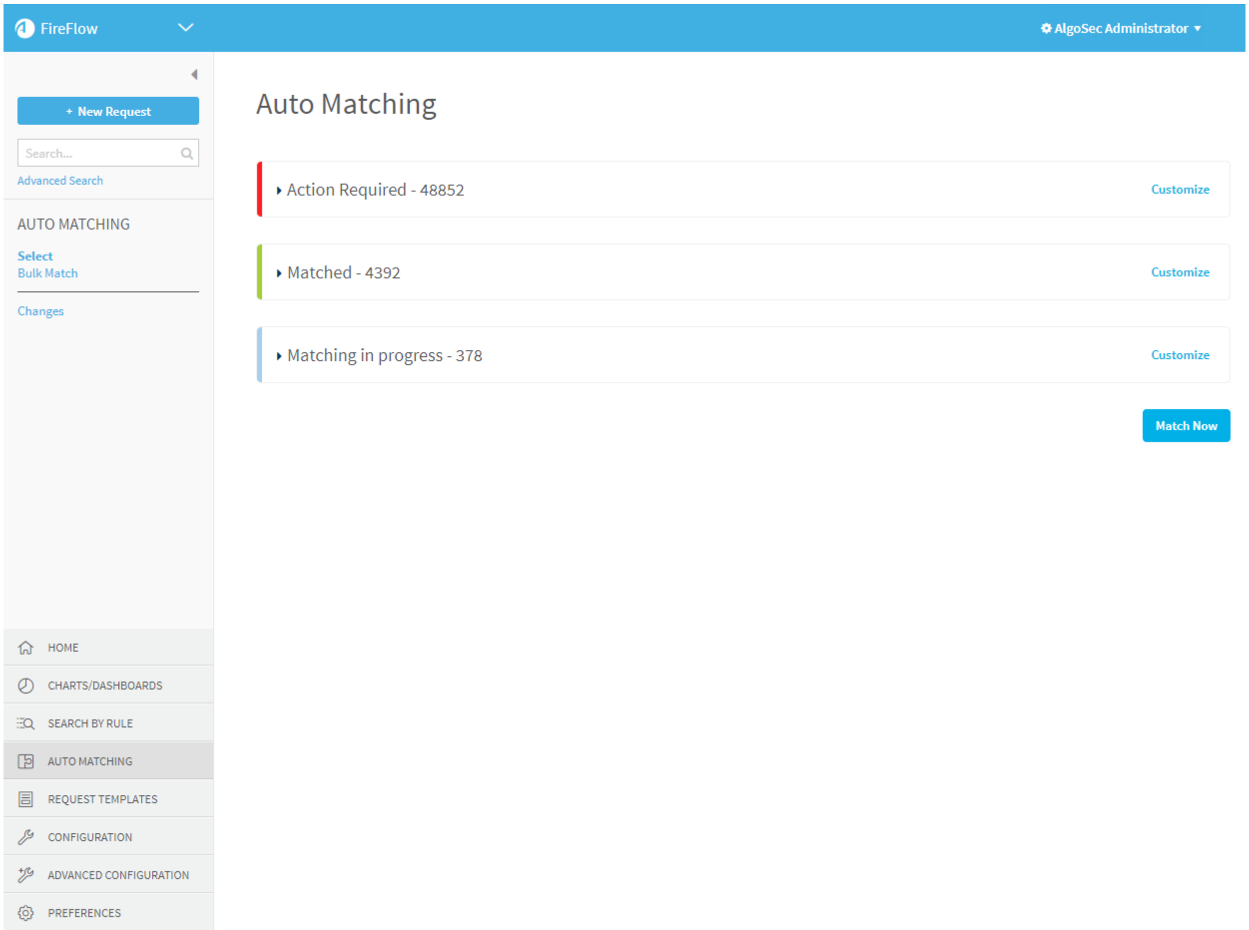
This topic describes how to view the results of FireFlow's auto matching process, as well as any manual matching performed.

## Access the Auto Matching page

In FireFlow's main menu on the left, click **Auto Matching**.

The **Auto Matching** page appears displaying lists of change requests and changes.

For example:



Items are organized into the following categories:

- **Action Required**. FireFlow could not find a perfect match automatically. You may need to manually match these items or otherwise understand the change that was made. For details, see Action required device changes.
- **Matched**. Items where FireFlow automatically found a perfect match, or a user has manually matched a change and change request. For details, see Matched device changes.
- **Matching In Progress**. Change requests that still require attention, either by FireFlow or manual changes by a user. For details, see Matching in progress device changes.

**Tip:** The number of rows displayed in each sub-list depends on your configured preferences.

## Action required device changes

FireFlow defines the following sorts of device changes as **Action Required**:

- Changes Without Request
- Mismatches

For more details, see Resolve unmatched changes.

### Changes Without Request

The **Changes Without Request** list includes all detected device changes where a matching change request was not found automatically.

Do any of the following:

- Click the rule to view the full rule change.
- Click the **Summary** or **Content** to modify the description.

For details, see View and edit change records.

### Mismatches

The following lists include all devices where the changes detected do not match the changes approved.

| | |
|---|---|
| **Change <-> Change Request Mismatch** | Includes all non-matching changes. |
| **Changes Wider than Request** | Includes all device changes that are more extensive than the changes approved in the linked change request.<br>For example, when more services appear in the device change than appear in the approved change request. |
| **Change Requests Partially Implemented** | Includes instances where the change request calls for more extensive changes than were actually made.<br>For example, when not all of the source IP addresses that appear in the change request appear in the updated device rule. |

Click a rule to view the full rule change. For details, see View and edit change records.

**Note:** Traffic change requests with requested traffic that is partially blocked may appear in the **Change Requests Partially Implemented** sub-list. Resolve these change requests manually.

For details, see Resolve unmatched changes.

## Matched device changes

FireFlow marks all device changes that match approved change requests as **Matched**.

These do not require any additional action, and include the following types:

- Last X days matches
- Approved changes

**Note:** Web filtering change requests and object change requests are automatically marked as **Matched**.

## Last X days matches

Change requests from a configurable number of days include the following types:

| | |
|---|---|
| **Perfect Auto Match, Last X Days** | All change requests that were auto matched over a certain numbers of days. |
| **ID Match, Last X Days** | All change requests that were auto matched by means of an ID match over a certain numbers of days.<br>**Note:** This sub-list includes only change requests with multiple traffic requests and Palo Alto traffic change requests. |
| **Manual Match, Last X Days** | All change requests that were manually matched over a certain numbers of days. |

Click a rule to view the full rule change. For details, see View and edit change records.

## Approved changes

Approved changes are categorized as follows:

| | |
|---|---|
| **Changes Without Request - Approved** | All device changes for which a matching change request was not found, but which were manually approved regardless. |
| **Requests Without Change - Approved** | All change requests for which a matching device change was not found, but which were manually approved regardless. |
| **Change Requests that Already Work** | All change requests for which the requested traffic is already allowed/blocked, and therefore no action is needed. |
| **Requests with Object Change** | All object change requests. These change requests are automatically marked as matched. |
| **Recertification Requests** | All recertification requests. These change requests are automatically marked as matched. |

Do any of the following, as relevant:

- Click a rule to view the full rule change. For details, see View and edit change records.
- Click a change request ID number or subject to view the change request.

## Matching in progress device changes

FireFlow marks the following types of changes as **Matching in Progress**:

| | |
|---|---|
| **Change Requests Pending Auto Matching** | All change requests that are currently pending auto matching. |
| **Requests Pending Auto Matching** | All requests that are currently pending auto matching. |
| **Requests with Rule Removal Request Pending Auto Matching** | All rule removal requests that are currently pending auto matching. |
| **Changes Pending Auto Matching** | All changes that are currently pending auto matching. |

These items still require attention, either by FireFlow or manual changes by users. For details, see Resolve unmatched changes.

Depending on the matching type, click a change request ID number, subject, or device or policy specific request ID to view the change request.

# Resolve unmatched changes

**Relevant for: Privileged users**

This topic describes how to manually match a change request to device changes, when FireFlow was unable to do so automatically.

**Note:** The options available to you may differ, depending on your role and permissions configured. For more details, contact a FireFlow administrator.

## Resolve individual change requests and changes

To resolve an individual change and change request, follow one of the following procedures, depending on the item's matching status:

- Changes Without Request
- Mismatched changes
- Requests Pending Auto Matching

### Changes Without Request

Resolve a change where no matching request was found by doing one of the following:

**Confirm that the change is acceptable**

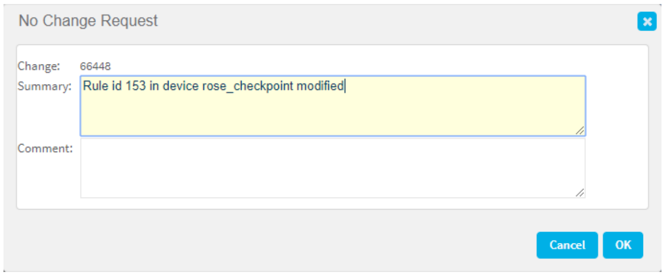
Do the following:

1. In the main menu, click **Auto Matching**.

   The **Auto Matching** page appears displaying lists of change requests and changes.

2. In the change's row, click **No Request**.

   The **No Change Request** dialog box opens.

   No Change Request

   Change: 66448
   Summary: Rule id 153 in device rose_checkpoint modified
   Comment:

3. To change the rule's description, edit the text in the **Summary** field as desired.
4. In the **Comment** field, type an explanation of why you are resolving the change in this manner.
5. Click **OK**.

In the **Auto Matching** page, the change will now appear in the **Matched** list's **Changes Without Request- Approved** sub-list.

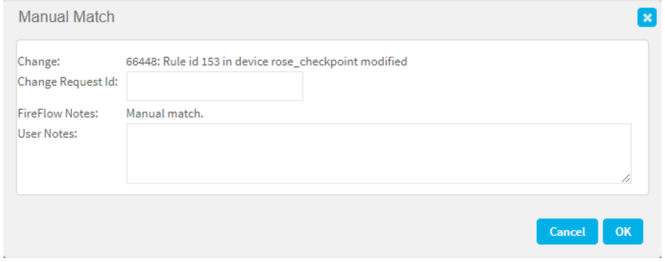
### Manually associate the change with a change request

1. In the main menu, click **Auto Matching**.

   The **Auto Matching** page appears displaying lists of change requests and changes.

2. In the change's row, click **Match**.

   The **Manual Match** dialog box opens.

   Change: 66448: Rule id 153 in device rose_checkpoint modified
   Change Request Id:
   FireFlow Notes: Manual match.
   User Notes:

3. In the **Change Id** field, type the ID number of the change request that should be associated with this change.

4. In the **User Notes** field, type an explanation of why you are resolving the change request in this manner.

5. Click **OK**.

The change is matched with the change request. In the **Auto Matching** page, the change request will now appear in the **Matched** list's **Manual Match, Last X Days** sub-list.

## Mismatched changes

Mismatched changes are items with differences between the change made and the change request approved, including:

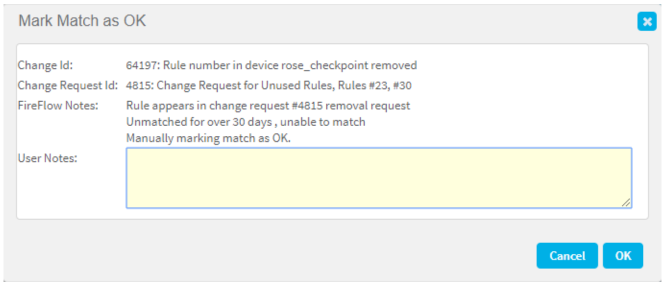
- **Change <-> Change Request Mismatch**
- **Changes Wider than Request**
- **Change Requests Partially Implemented**

Handle these items by doing one of the following:

### Confirm that a change matches a change request

1. View the relevant match record. For details, see [View and edit match records](#).
2. Click ≡ , and then click **Match OK**.

   The **Mark Match as OK** dialog box opens.



Mark Match as OK

Change Id: 64197: Rule number in device rose_checkpoint removed

Change Request Id: 4815: Change Request for Unused Rules, Rules #23, #30

FireFlow Notes: Rule appears in change request #4815 removal request
Unmatched for over 30 days , unable to match
Manually marking match as OK.

User Notes:

3. In the **User Notes** field, type an explanation of why you are resolving the discrepancy in this manner.
4. Click **OK**.

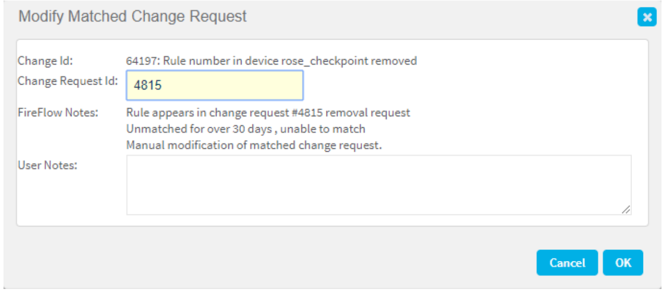
The change request is matched, and its status changes to "resolved".

In the **Auto Matching** page, the change request will now appear in the **Matched** list's **Manual Match, Last X Days** sub-list.

### Manually associate the change with a different change request

1. View the relevant match record. For details, see [View and edit match records](#).
2. Click ≡ , and then click **Wrong Change Request**.

   The **Modify Matched Change Request** dialog box opens.



Modify Matched Change Request

Change Id: 64197: Rule number in device rose_checkpoint removed

Change Request Id: 4815

FireFlow Notes: Rule appears in change request #4815 removal request
Unmatched for over 30 days , unable to match
Manual modification of matched change request.

User Notes:

3. In the **Change Request Id** field, type the ID number of the change request with which the change should be associated.
4. In the **User Notes** field, type an explanation of why you are resolving the discrepancy in this manner.
5. Click **OK**.

The change request is matched, and its status changes to "resolved".

In the **Auto Matching** page, the change request will now appear in the **Matched** list's **Manual Match, Last X Days** sub-list.

### Disassociate the change from the change request

1. View the relevant match record. For details, see View and edit match records.
2. Click ☰ , and then click **Remove Match**.

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

The match record is deleted, and the change and change request are no longer associated.

In the **Auto Matching** page, the change will now appear in the **Action Required** list's **Changes Without Request** sub-list, and the change request will appear in the **Matching in Progress** list's **Change Requests Pending Auto Matching** sub-list.

> **Note:** The change and change request are not deleted from the system.

## Requests Pending Auto Matching

The **Matching in Progress** list's **Requests Pending Auto Matching** sub-list displays requests that are currently pending auto matching.

If scheduled FireFlow auto matching passes, and the change requests still appear in this list, handle them by doing one of the following:

### Confirm that a change request is acceptable

1. View the relevant match record. For details, see View and edit match records.
2. Click ≡ , and then click **No Change Record**.

   The **No Change Record** dialog box opens.
3. In the **Comment** field, type an explanation of why you are resolving the change request in this manner.
4. Click **Next**.

The change request is matched, and its status changes to "resolved".

In the **Auto Matching** page, the change request will now appear in the **Matched** list's **Manual Match, Last X Days** sub-list.

### Manually associate a change request with a change

1. View the relevant match record. For details, see View and edit match records.
2. Click ≡ , and then click **Manually Match**.

   The **Manual Match** dialog box opens.
3. In the **Change Id** field, type the ID number of the change that should be associated with this change request.
4. In the **User Notes** field, type an explanation of why you are resolving the change request in this manner.

5. Click **Next**.

The change request is matched, and its status changes to "resolved".

In the **Auto Matching** page, the change request will now appear in the **Matched** list's **Manual Match, Last X Days** sub-list.

## Resolve multiple change requests and changes

Resolve multiple change requests and changes simultaneously, such as when you want to perform a cleanup across all devices.

Resolve multiple changes as follows, depending on the matching status:

- Changes Without Request
- Mismatched changes
- Change Requests Pending Auto Matching

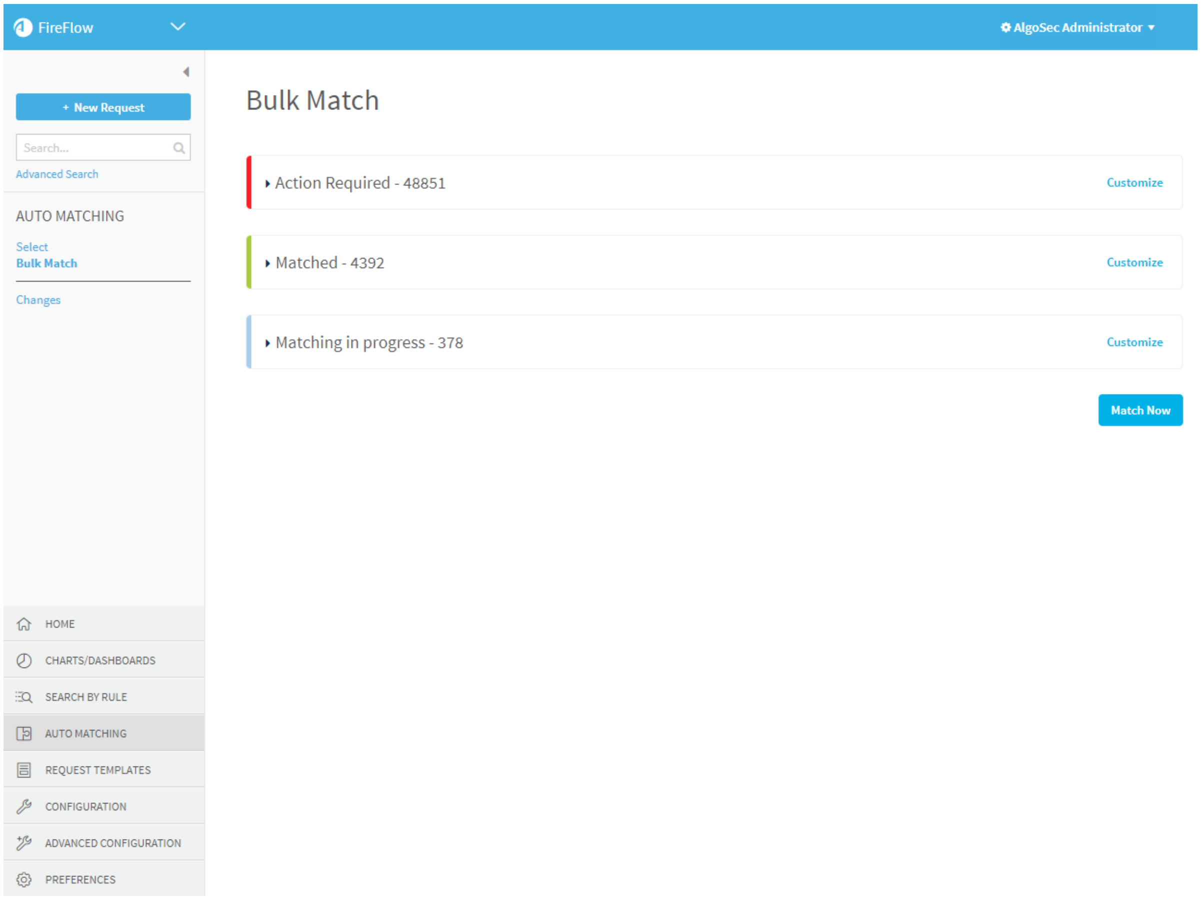
### Changes Without Request

Resolve all changes where no matching requests were found by doing one of the following:

**Confirm that changes are acceptable**

1. In the main menu, click **Auto Matching**, and then click **Bulk Match**.

   The **Bulk Match** page appears displaying lists of change requests and changes.



Bulk Match

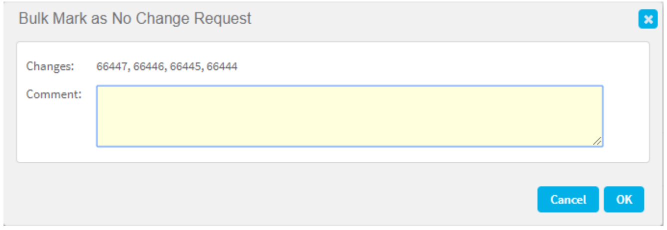
- Action Required - 48851
- Matched - 4392
- Matching in progress - 378

2. Do one of the following:

   - Select the check boxes next to the desired changes.
   - Click **Check All** to select all changes, at the bottom of the sub-list.
   - Click **Clear All** to deselect all changes, at the bottom of the sub-list.

3. At the bottom of the sub-list, click **No Change Request**.

   The **Bulk Mark as No Change Request** dialog box opens.



Bulk Mark as No Change Request

Changes: 66447, 66446, 66445, 66444

Comment:

4. In the **Comment** field, type an explanation of why you are resolving the selected changes in this manner.
5. Click **OK**.

In the **Bulk Match** page, the changes will now appear in the **Matched** list's **Changes Without Request - Approved** sub-list.

### Manually associate changes with a change request

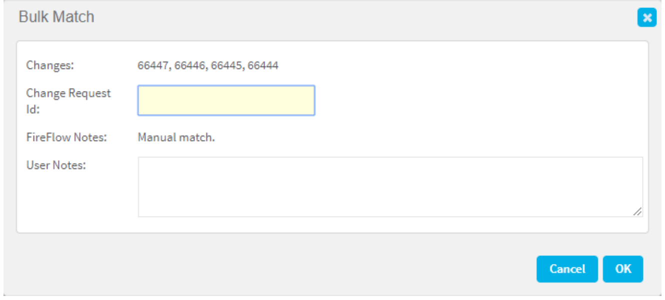
1. In the main menu, click **Auto Matching**, and then click **Bulk Match**.

   The **Bulk Match** page appears displaying lists of change requests and changes.

2. Do one of the following:
   - Select the check boxes next to the desired changes.
   - Click **Check All** to select all changes, at the bottom of the sub-list.
   - Click **Clear All** to deselect all changes, at the bottom of the sub-list.

3. At the bottom of the sub-list, click **Match**.

   The **Bulk Match** dialog box opens.



Bulk Match

Changes: 66447, 66446, 66445, 66444

Change Request Id:

FireFlow Notes: Manual match.

User Notes:

4. In the **Change Request Id** field, type the ID number of the change request that should be associated with the selected changes.
5. In the **User Notes** field, type an explanation of why you are resolving the selected changes in this manner.
6. Click **OK**.

The changes are matched with the change request. In the **Bulk Match** page, the change request will now appear in the **Matched** list's **Manual Match, Last X Days** sub-list.

## Mismatched changes

Mismatched changes are items with differences between the change made and the change request approved, including:

- **Change <-> Change Request Mismatch**
- **Changes Wider than Request**
- **Change Requests Partially Implemented**

Do the following to handle all of these items at once:

### Confirm that changes match change requests

1. In the main menu, click **Auto Matching**, and then click **Bulk Match**.

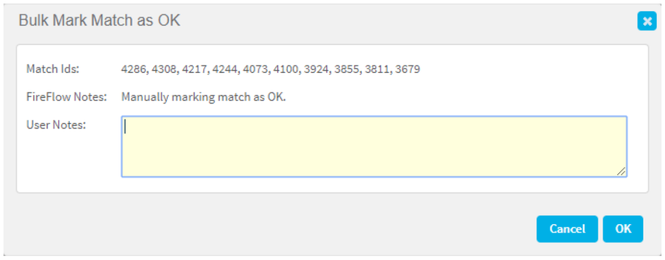
   The **Bulk Match** page appears displaying lists of change requests and changes.

2. Do one of the following:

   - Select the check boxes next to the desired change requests.
   - Click **Check All** to select all change requests, at the bottom of the sub-list.
   - Click **Clear All** to deselect all change requests, at the bottom of the sub-list.

3. At the bottom of the sub-list, click **Match OK**.

   The **Bulk Mark Match as OK** dialog box opens.



Bulk Mark Match as OK

Match Ids: 4286, 4308, 4217, 4244, 4073, 4100, 3924, 3855, 3811, 3679

FireFlow Notes: Manually marking match as OK.

User Notes:

4. In the **User Notes** field, type an explanation of why you are resolving the discrepancy in this manner.
5. Click **OK**.

The change requests are matched, and their statuses change to "resolved".

In the **Bulk Match** page, the change requests will now appear in the **Matched** list's **Manual Match, Last X Days** sub-list.

## Change Requests Pending Auto Matching

The **Matching in Progress** list's **Change Requests Pending Auto Matching** sub-list displays change requests that are currently pending auto matching.

Handle these items by doing one of the following:

### Confirm that change requests are acceptable

1. In the main menu, click **Auto Matching**, and then click **Bulk Match**.

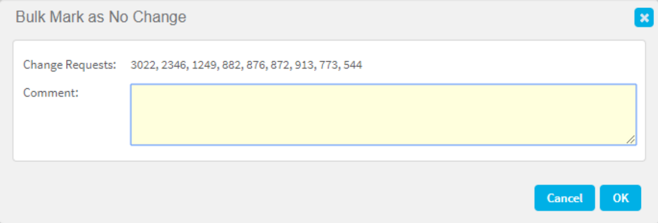
   The **Bulk Match** page appears displaying lists of change requests and changes.

2. Do one of the following:

   - Select the check boxes next to the desired change requests.
   - Click **Check All** to select all change requests, at the bottom of the sub-list.
   - Click **Clear All** to deselect all change requests, at the bottom of the sub-list.

3. At the bottom of the sub-list, click **No Change**.

   The **Bulk Mark as No Change** dialog box opens.



Bulk Mark as No Change

Change Requests: 3022, 2346, 1249, 882, 876, 872, 913, 773, 544

Comment:

4. In the **Comment** field, type an explanation of why you are resolving the change requests in this manner.

5. Click **OK**.

The change requests are matched, and their statuses change to "resolved".

In the **Bulk Match** page, the change requests will now appear in the **Matched** list's **Manual Match, Last X Days** sub-list.

### Manually associate a change request with a change

1. In the main menu, click **Auto Matching**, and then click **Bulk Match**.

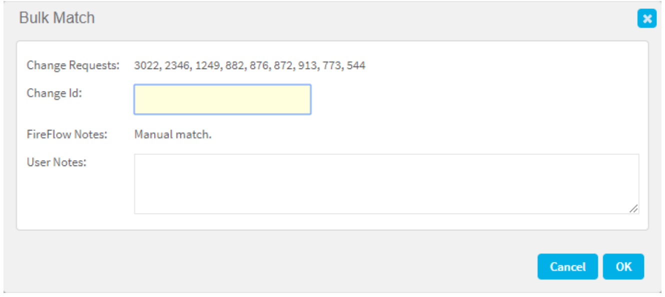
   The **Bulk Match** page appears displaying lists of change requests and changes.

2. Do one of the following:

   - Select the check boxes next to the desired change requests.
   - Click **Check All** to select all change requests, at the bottom of the sub-list.
   - Click **Clear All** to deselect all change requests, at the bottom of the sub-list.

3. At the bottom of the sub-list, click **Match**.

   The **Bulk Match** dialog box opens.



Bulk Match

Change Requests: 3022, 2346, 1249, 882, 876, 872, 913, 773, 544

Change Id:

FireFlow Notes: Manual match.

User Notes:

4. In the **Change Id** field, type the ID number of the change that should be associated with these change requests.

5. In the **User Notes** field, type an explanation of why you are resolving the change requests in this manner.

6. Click **OK**.

The change requests are matched, and their statuses change to "resolved".

In the **Bulk Match** page, the change requests will now appear in the **Matched** list's **Manual Match, Last X Days** sub-list.

# View and edit match records

This topic describes how to view a FireFlow match record, which contains all details about a change request, the relevant device change, the current matching status, and history.

## View a match record

Viewing match records for unmatched change requests or changes can help you determine how to manually match them.

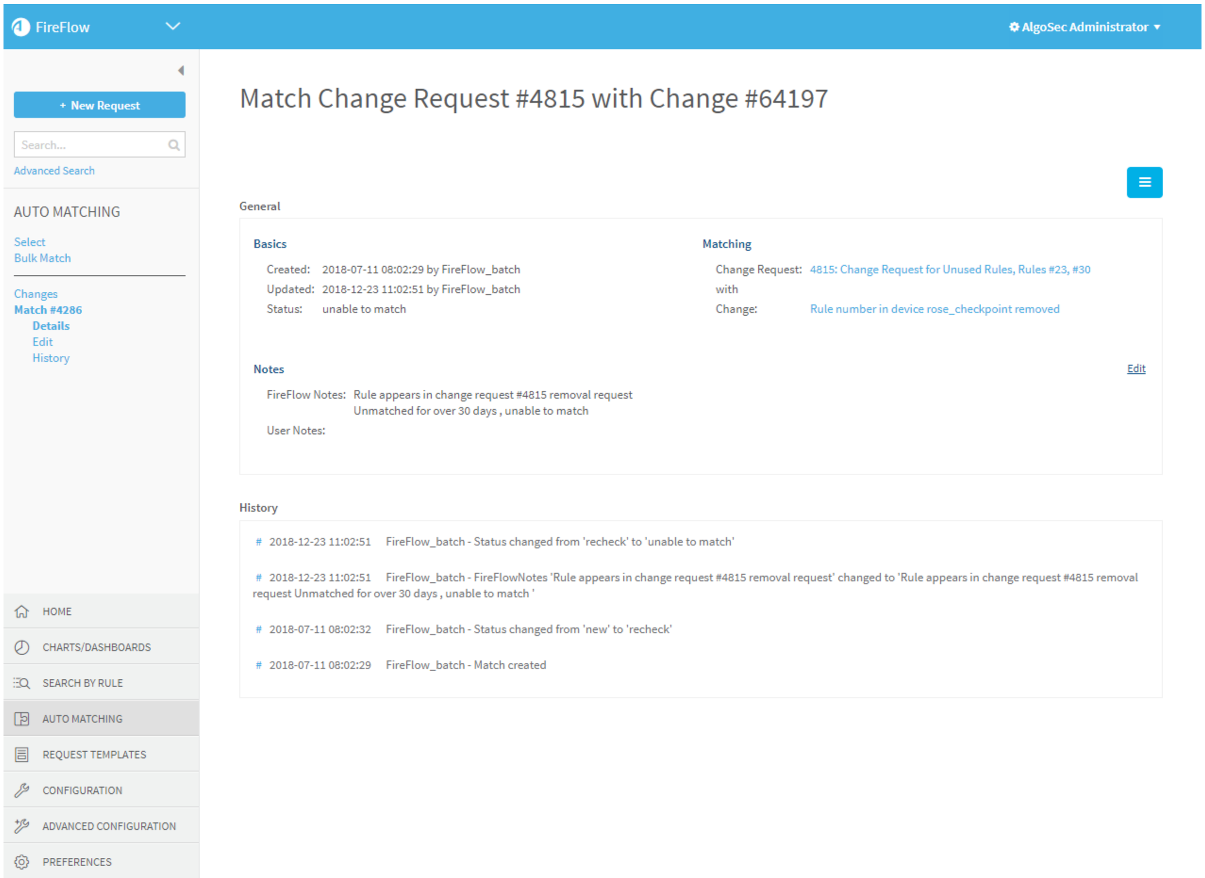
### Do the following:

1. In the main menu, click **Auto Matching**.

   The **Auto Matching** page appears displaying lists of change requests and changes.

2. In the change request's row, click **Details**.

The match record is displayed. For example:



Match Change Request #4815 with Change #64197

General

Basics

Created: 2018-07-11 08:02:29 by FireFlow_batch
Updated: 2018-12-23 11:02:51 by FireFlow_batch
Status: unable to match

Matching

Change Request: 4815: Change Request for Unused Rules, Rules #23, #30
with
Change: Rule number in device rose_checkpoint removed

Notes

Edit

FireFlow Notes: Rule appears in change request #4815 removal request
Unmatched for over 30 days , unable to match
User Notes:

History

```
# 2018-12-23 11:02:51    FireFlow_batch - Status changed from 'recheck' to 'unable to match'

# 2018-12-23 11:02:51    FireFlow_batch - FireFlowNotes 'Rule appears in change request #4815 removal request' changed to 'Rule appears in change request #4815 removal request Unmatched for over 30 days , unable to match '

# 2018-07-11 08:02:32    FireFlow_batch - Status changed from 'new' to 'recheck'

# 2018-07-11 08:02:29    FireFlow_batch - Match created
```

## Match record fields

Each match record includes the following fields:

### Basics

| | |
|---|---|
| **Created** | The date and time when the match record was created, followed by the FireFlow process that created it. |
| **Updated** | The date and time when the match record was last updated, followed by the user or FireFlow process that updated it. |
| **Status** | The matching status. |

### Matching

| | |
|---|---|
| **Change Request** | The change request's ID number and name.<br>Click to view the change request. |
| **Change** | The rule change's description.<br>Click to view the change. |

### Notes

| | |
|---|---|
| **FireFlow Notes** | FireFlow's comments on the match record. |
| **User Notes** | User notes on the match record.<br>For details, see Add notes to match records. |
| **History** | A list of all actions in the match record's history. |

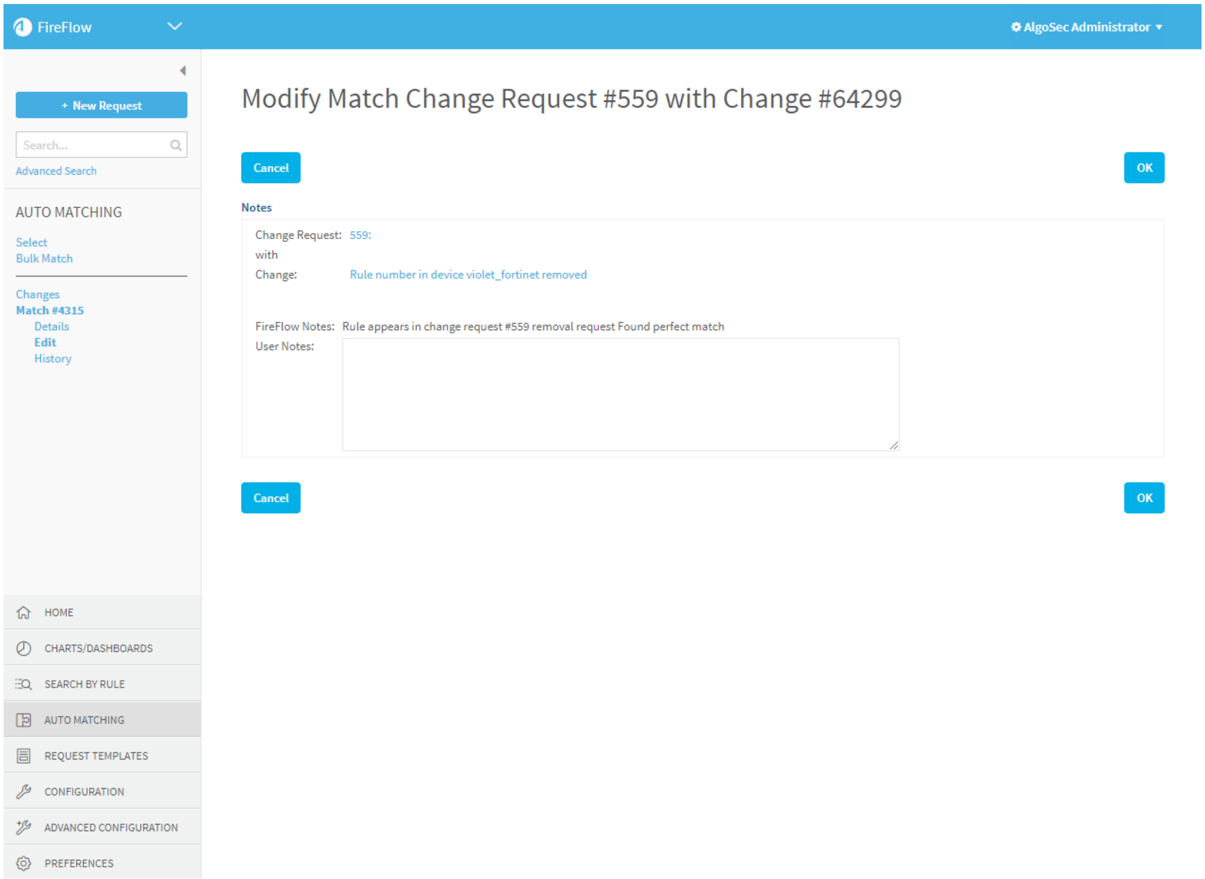
## Add notes to match records

Edit a match record to add notes as needed.

### Do the following:

1. View the match record. For details, see View a match record.
2. Under the change request number in the main menu, click **Edit**.

   The **Modify Match Change Request** page is displayed.



Modify Match Change Request #559 with Change #64299

Notes

Change Request: 559:
with
Change: Rule number in device violet_fortinet removed

FireFlow Notes: Rule appears in change request #559 removal request Found perfect match
User Notes:

3. In the **User Notes** field, type your notes on the match record.
4. Click **OK**.

## View and edit change records

This topic describes how to view and edit change records.

You may need to do this when resolving unmatched change requests to determine which change to associate with the change request.

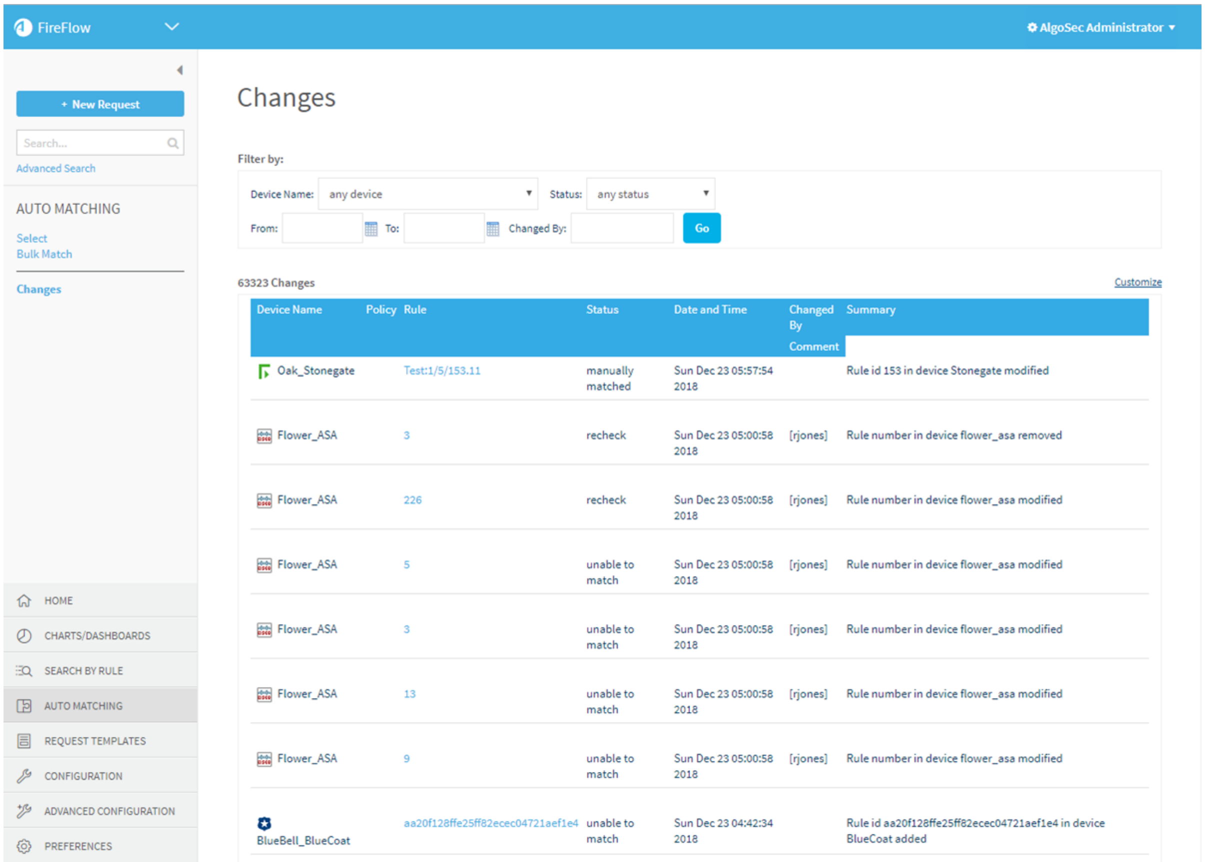
### View the changes list

View a full list of detected rule changes.

## Do the following:

1. In the main menu, click **Auto Matching** and then **Changes**.

   The **Changes** page appears displaying detected rule changes.



Changes

Filter by:

Device Name: any device ▾ Status: any status ▾

From: To: Changed By:

63323 Changes

| Device Name | Policy | Rule | Status | Date and Time | Changed By<br>Comment | Summary |
|---|---|---|---|---|---|---|
| Oak_Stonegate | | Test:1/5/153.11 | manually matched | Sun Dec 23 05:57:54 2018 | | Rule id 153 in device Stonegate modified |
| Flower_ASA | | 3 | recheck | Sun Dec 23 05:00:58 2018 | [rjones] | Rule number in device flower_asa removed |
| Flower_ASA | | 226 | recheck | Sun Dec 23 05:00:58 2018 | [rjones] | Rule number in device flower_asa modified |
| Flower_ASA | | 5 | unable to match | Sun Dec 23 05:00:58 2018 | [rjones] | Rule number in device flower_asa modified |
| Flower_ASA | | 3 | unable to match | Sun Dec 23 05:00:58 2018 | [rjones] | Rule number in device flower_asa modified |
| Flower_ASA | | 13 | unable to match | Sun Dec 23 05:00:58 2018 | [rjones] | Rule number in device flower_asa modified |
| Flower_ASA | | 9 | unable to match | Sun Dec 23 05:00:58 2018 | [rjones] | Rule number in device flower_asa modified |
| BlueBell_BlueCoat | | aa20f128ffe25ff82ecec04721aef1e4 | unable to match | Sun Dec 23 04:42:34 2018 | | Rule id aa20f128ffe25ff82ecec04721aef1e4 in device BlueCoat added |

   - Click a rule to view the rule change.
   - For more details, see Modify change records.

   > **Note:** The number of changes displayed depends on your configured preferences.
   >
   > =

2. To filter the displayed rule changes, specify filter criteria in the Filter by area as

follows:

| | |
|---|---|
| **Device Name** | Type the name of a device whose rule changes you want to display.<br>This field is optional. |
| **Status** | Select the status of changes you want to display.<br>This field is optional. |
| **From** | Specify the earliest date for which changes should be displayed, by doing one of the following:<br>• Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>• Type the desired date in the field provided. You can use most relative and absolute formats, for example `yyyy-mm-dd`, `mm/dd/yyyy`, `Mon dd yyyy`, "next week", and "now + 3 days".<br>This field is optional. |
| **To** | Specify the latest date for which changes should be displayed, by doing one of the following:<br>• Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>• Type the desired date in the field provided. You can use most relative and absolute formats, for example `yyyy-mm-dd`, `mm/dd/yyyy`, `Mon dd yyyy`, "next week", and "now + 3 days".<br>This field is optional. |
| **Changed By** | Type the user that made the changes.<br>This field is optional. |

Then click **Go**.

The rule changes are filtered according to the criteria you specified.

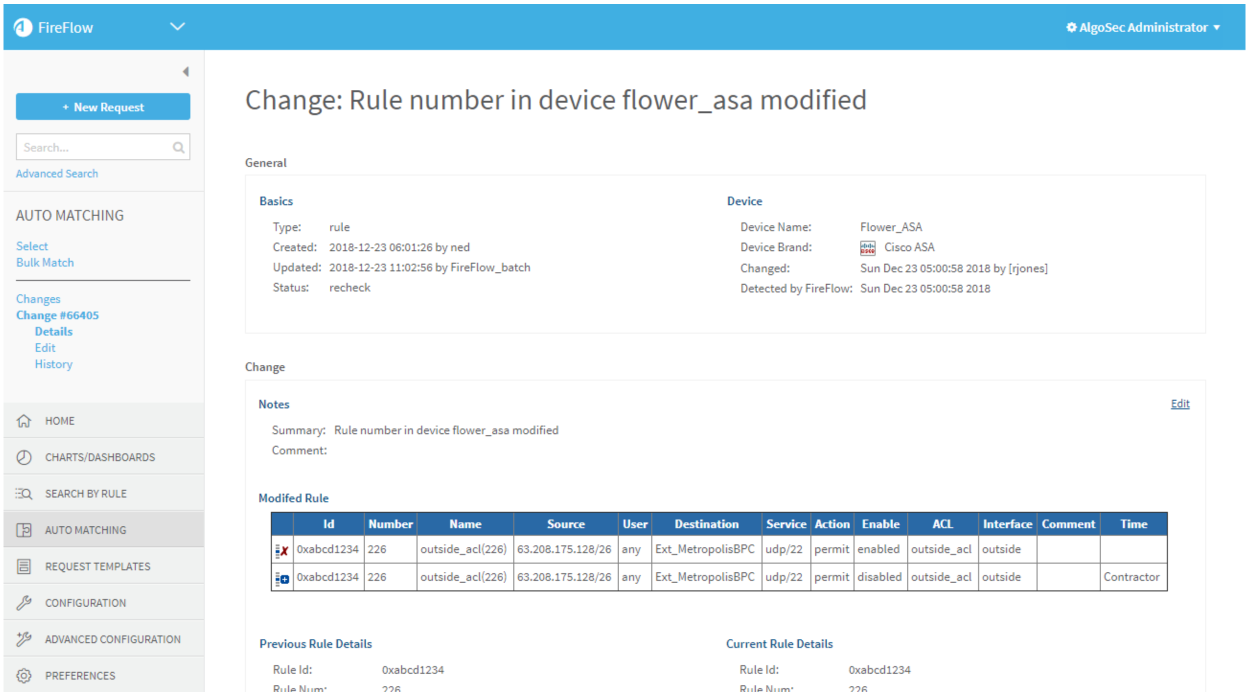
## View individual rule changes

You can view individual rule changes from matching results or the changes list.

For details, see View matching results and View the changes list.

From there, click on a rule name to view the rule change.

The change is displayed. For example:



Change: Rule number in device flower_asa modified

General

Basics

Type: rule
Created: 2018-12-23 06:01:26 by ned
Updated: 2018-12-23 11:02:56 by FireFlow_batch
Status: recheck

Device

Device Name: Flower_ASA
Device Brand: Cisco ASA
Changed: Sun Dec 23 05:00:58 2018 by [rjones]
Detected by FireFlow: Sun Dec 23 05:00:58 2018

Change

Notes | Edit

Summary: Rule number in device flower_asa modified
Comment:

Modifed Rule

| | Id | Number | Name | Source | User | Destination | Service | Action | Enable | ACL | Interface | Comment | Time |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ✗ | 0xabcd1234 | 226 | outside_acl(226) | 63.208.175.128/26 | any | Ext_MetropolisBPC | udp/22 | permit | enabled | outside_acl | outside | | |
| ⊞ | 0xabcd1234 | 226 | outside_acl(226) | 63.208.175.128/26 | any | Ext_MetropolisBPC | udp/22 | permit | disabled | outside_acl | outside | | Contractor |

Previous Rule Details

Rule Id: 0xabcd1234
Rule Num: 226

Current Rule Details

Rule Id: 0xabcd1234
Rule Num: 226

Change fields include the following:

| | |
|---|---|
| **General** | Includes basic details about the change and relevant device. |
| **Change** | Includes extended details about the change, including:<br>• Descriptions or user comments. For more details, see Modify change records.<br>• Details about the rule before and after the change was made. |
| **Matched to change request** | Details about the change request and match record associated with this change.<br>Click the ID to open the change request. |
| **History** | about the change request associated with this change. |

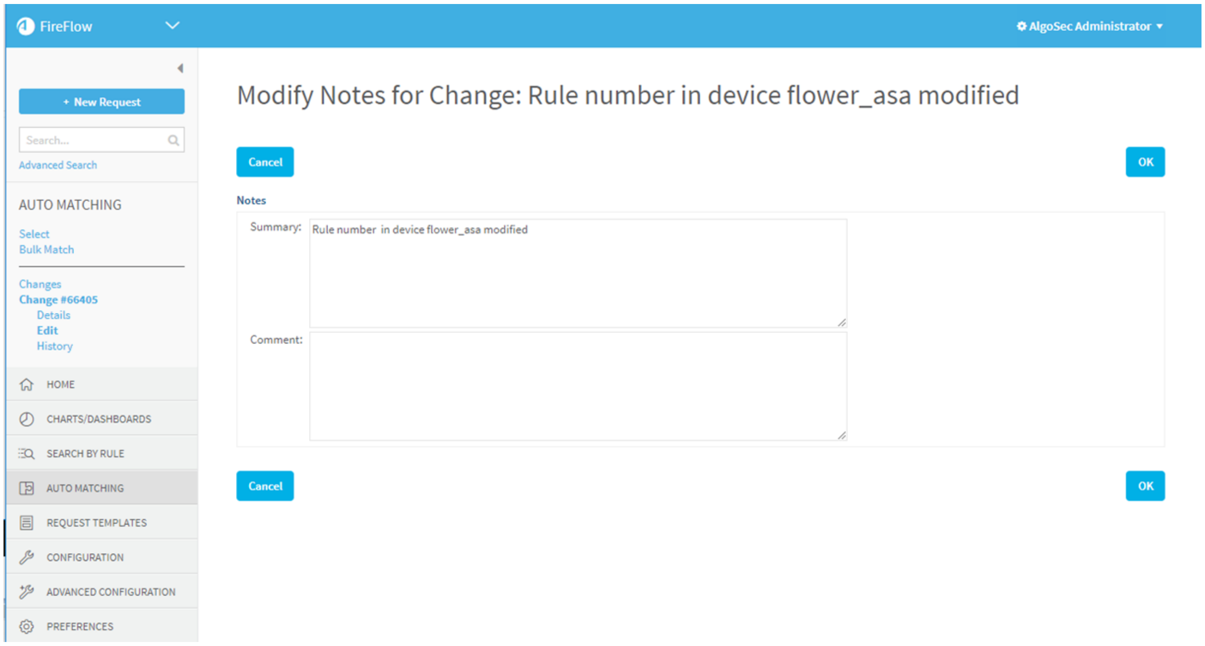
## Modify change records

Modify a rule change's description by adding comments.

Do the following:

1. View the change. For details, see View individual rule changes.
2. Under the change request number in the main menu, click **Edit**.

   The **Modify Notes for Change** page is displayed.



Modify Notes for Change: Rule number in device flower_asa modified

Notes

Summary: Rule number  in device flower_asa modified

Comment:

3. In the **Summary** field, modify the change's description as desired.
4. In the **Comment** field, type your comments on the change.
5. Click **OK**.

# Re-certify traffic

**Relevant for: Network operations users**

This topic describes how to re-certify traffic changes that were added by change requests that are now expired.

For example, if you have a traffic change request that has since expired but did require the addition of Allow traffic to a specific device policy, re-certify the change request to verify whether that change is still required.

**Note:** To determine a change request's stage, view the change request. The stage is indicated by the Change Request Lifecycle Status Bar. For details, see View change requests.

## Create a single re-certification request

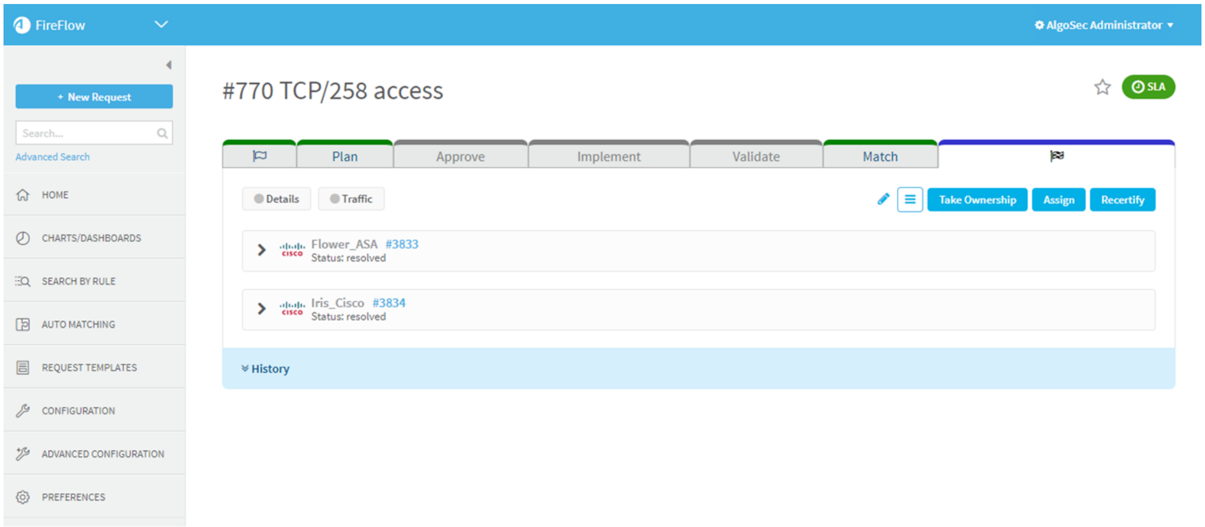
This procedure describes how to create a re-certification request for a single change request.

**Tip:** See also Create a multiple re-certification request.

### Do the following:

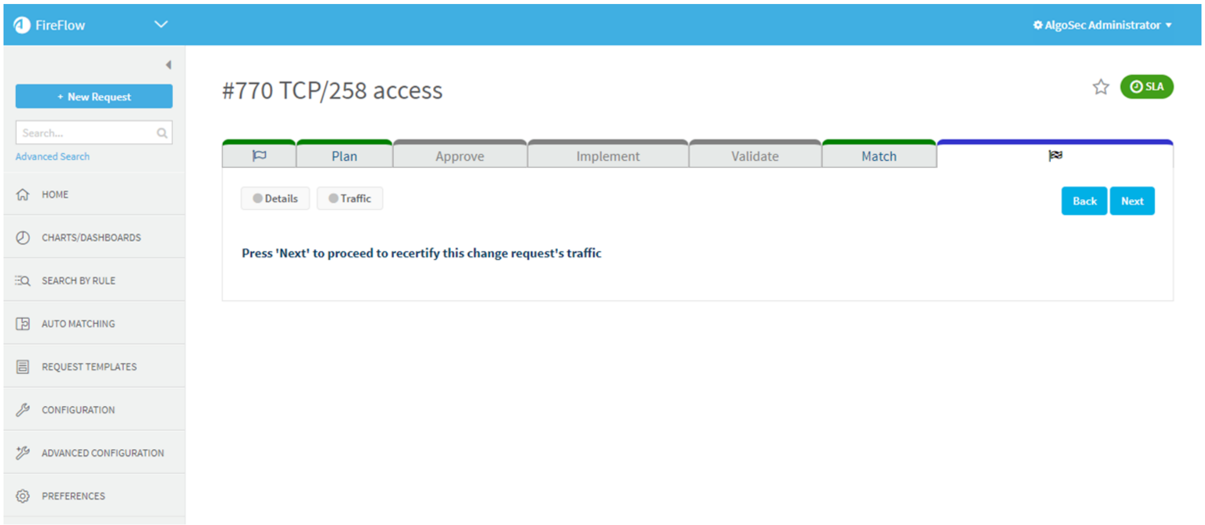
1. View a change request whose status is "resolved". For details, see View change requests.

   The change request appears.



2. Click **Recertify**.

   The Recertify Change Request page is displayed.



Press 'Next' to proceed to recertify this change request's traffic

3. Click **Next**.

A re-certification request is automatically created for the change request. The due date for the re-certification request is 14 days from the present date.

A success message appears with the ID number of the re-certification request. To view the request, click the ID number.

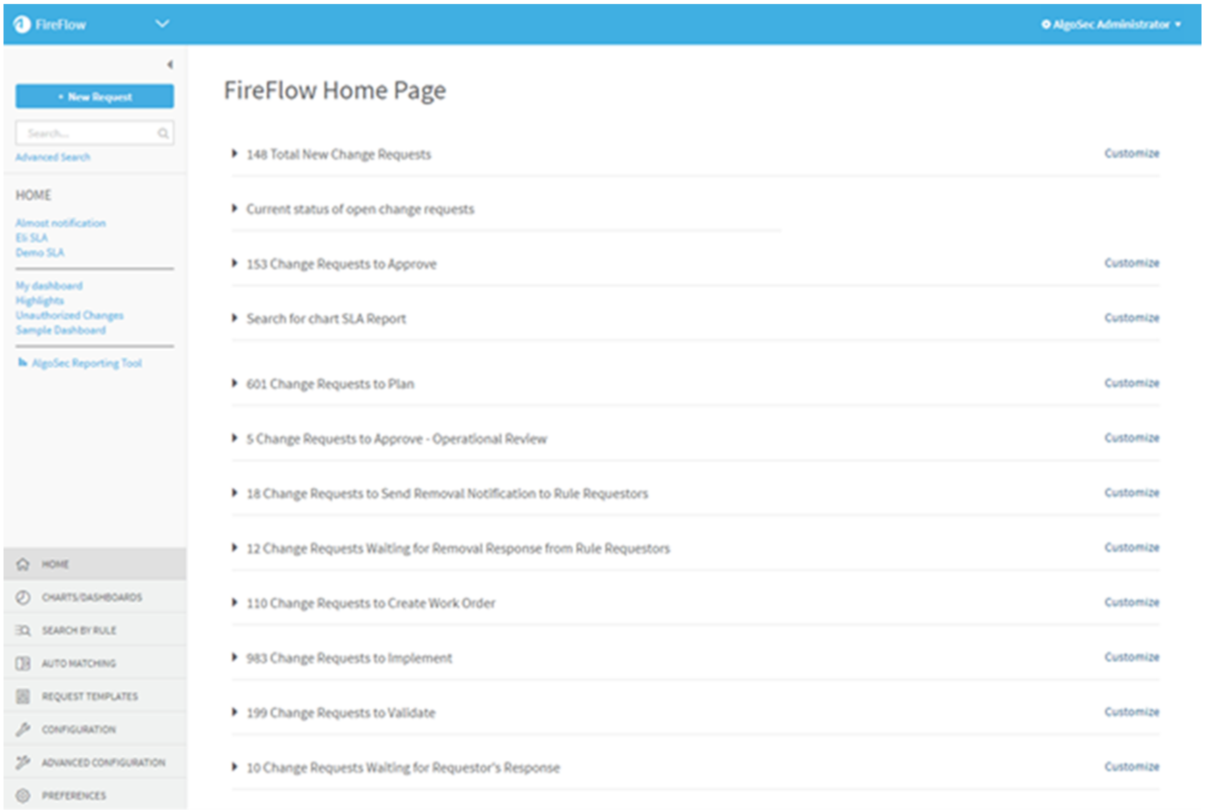
# Create a multiple re-certification request

This procedure describes how to create a recertification request for multiple expired change requests.

## Do the following:

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

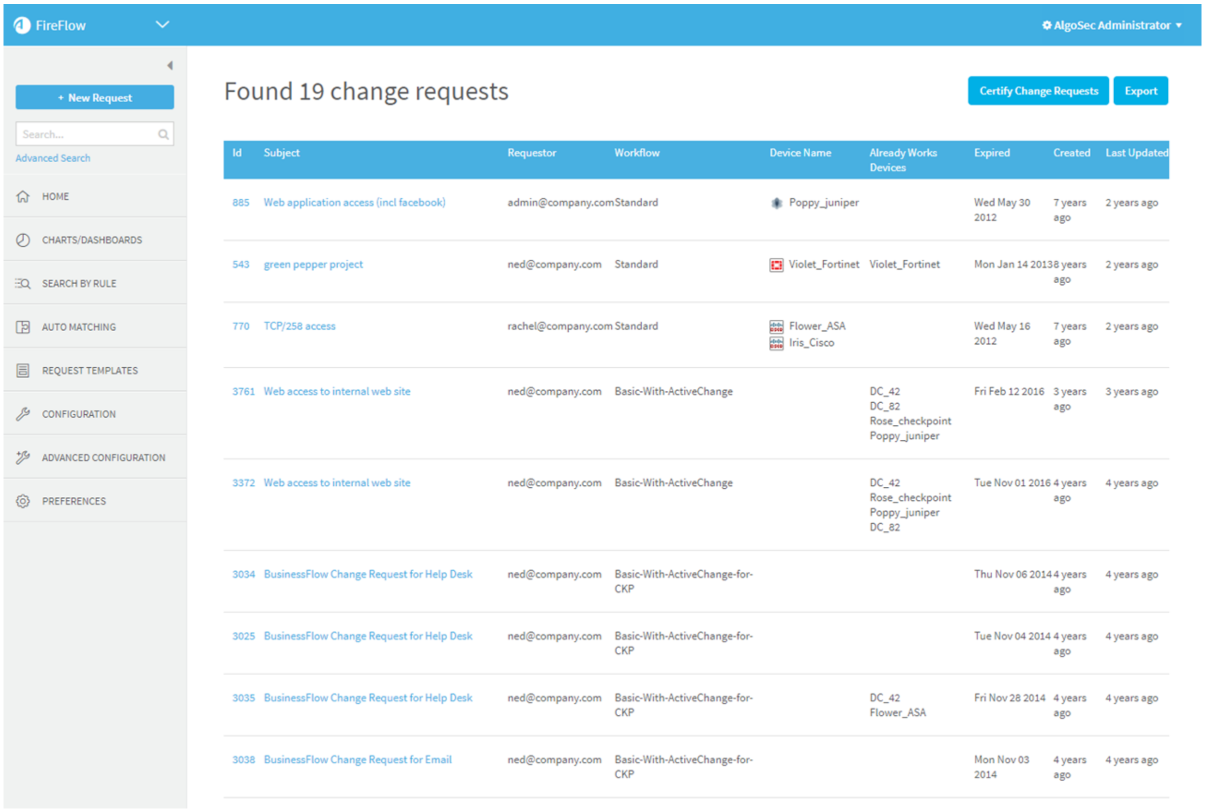
   The **FireFlow Home Page** is displayed.

   
   FireFlow
AlgoSec Administrator
• New Request
Search...
Advanced Search
HOME
Almost notification
Eli SLA
Demo SLA
My dashboard
Highlights
Unauthorized Changes
Sample Dashboard
AlgoSec Reporting Tool
HOME
CHARTS/DASHBOARDS
SEARCH BY RULE
AUTO MATCHING
REQUEST TEMPLATES
CONFIGURATION
ADVANCED CONFIGURATION
PREFERENCES
FireFlow Home Page
148 Total New Change Requests
Customize
Current status of open change requests
153 Change Requests to Approve
Customize
Search for chart SLA Report
Customize
601 Change Requests to Plan
Customize
5 Change Requests to Approve - Operational Review
Customize
18 Change Requests to Send Removal Notification to Rule Requestors
Customize
12 Change Requests Waiting for Removal Response from Rule Requestors
Customize
110 Change Requests to Create Work Order
Customize
983 Change Requests to Implement
Customize
199 Change Requests to Validate
Customize
10 Change Requests Waiting for Requestor's Response
Customize

2. Click on the **Change Requests that are due to be recertified** list heading.

   **Note:** Alternatively, you can load the saved search **Change Requests that are due to be recertified**, located under the **FireFlow's saved searches** category. For details, see Search for change requests.

The **Found** page appears displaying the all expired traffic change requests for which Allow traffic was added to the device policy.

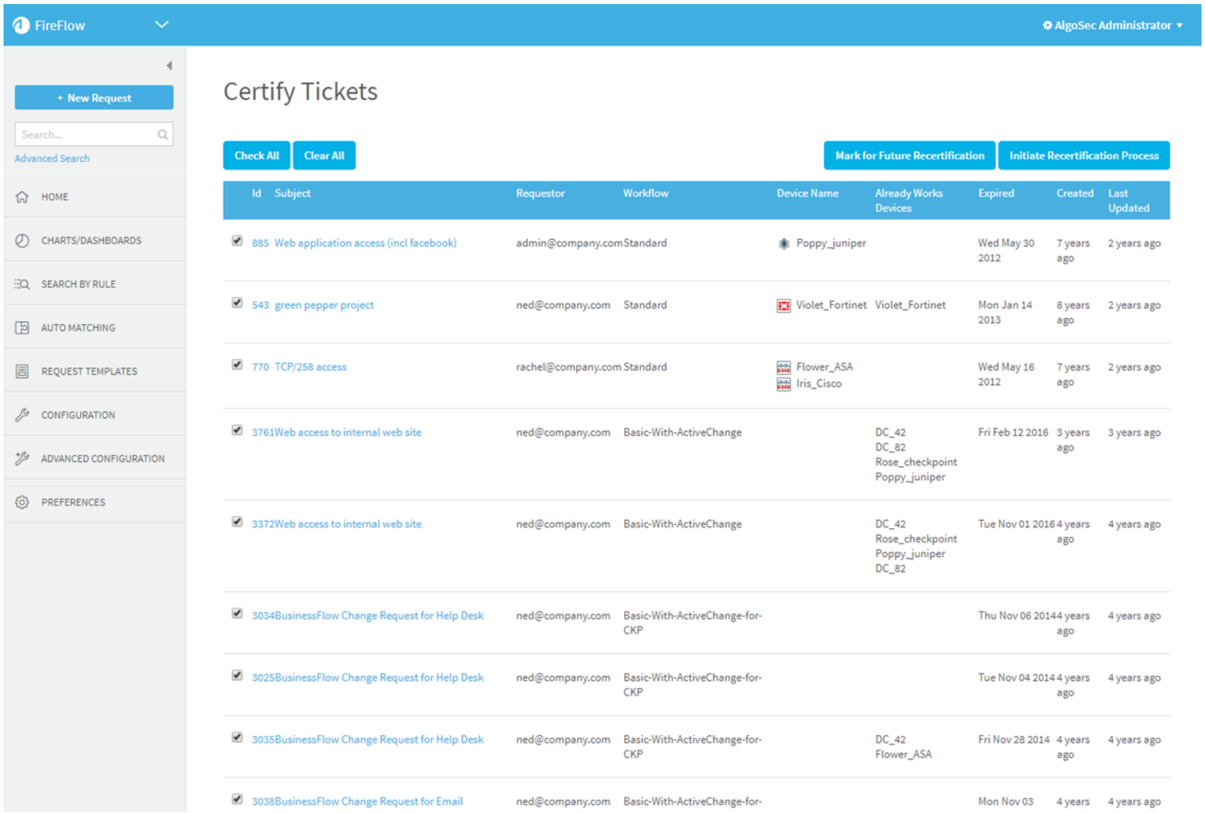


Found 19 change requests

| Id | Subject | Requestor | Workflow | Device Name | Already Works Devices | Expired | Created | Last Updated |
|---|---|---|---|---|---|---|---|---|
| 885 | Web application access (incl facebook) | admin@company.com | Standard | Poppy_juniper | | Wed May 30 2012 | 7 years ago | 2 years ago |
| 543 | green pepper project | ned@company.com | Standard | Violet_Fortinet | Violet_Fortinet | Mon Jan 14 2013 | 8 years ago | 2 years ago |
| 770 | TCP/258 access | rachel@company.com | Standard | Flower_ASA<br>Iris_Cisco | | Wed May 16 2012 | 7 years ago | 2 years ago |
| 3761 | Web access to internal web site | ned@company.com | Basic-With-ActiveChange | | DC_42<br>DC_82<br>Rose_checkpoint<br>Poppy_juniper | Fri Feb 12 2016 | 3 years ago | 3 years ago |
| 3372 | Web access to internal web site | ned@company.com | Basic-With-ActiveChange | | DC_42<br>Rose_checkpoint<br>Poppy_juniper<br>DC_82 | Tue Nov 01 2016 | 4 years ago | 4 years ago |
| 3034 | BusinessFlow Change Request for Help Desk | ned@company.com | Basic-With-ActiveChange-for-CKP | | | Thu Nov 06 2014 | 4 years ago | 4 years ago |
| 3025 | BusinessFlow Change Request for Help Desk | ned@company.com | Basic-With-ActiveChange-for-CKP | | | Tue Nov 04 2014 | 4 years ago | 4 years ago |
| 3035 | BusinessFlow Change Request for Help Desk | ned@company.com | Basic-With-ActiveChange-for-CKP | | DC_42<br>Flower_ASA | Fri Nov 28 2014 | 4 years ago | 4 years ago |
| 3038 | BusinessFlow Change Request for Email | ned@company.com | Basic-With-ActiveChange-for-CKP | | | Mon Nov 03 2014 | 4 years ago | 4 years ago |

3. Click **Certify Change Requests**.

   The **Certify Tickets** page is displayed.



Certify Tickets

| | Id | Subject | Requestor | Workflow | Device Name | Already Works Devices | Expired | Created | Last Updated |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | 885 | Web application access (incl facebook) | admin@company.com | Standard | Poppy_juniper | | Wed May 30 2012 | 7 years ago | 2 years ago |
| ☑ | 543 | green pepper project | ned@company.com | Standard | Violet_Fortinet | Violet_Fortinet | Mon Jan 14 2013 | 8 years ago | 2 years ago |
| ☑ | 770 | TCP/258 access | rachel@company.com | Standard | Flower_ASA<br>Iris_Cisco | | Wed May 16 2012 | 7 years ago | 2 years ago |
| ☑ | 3761 | Web access to internal web site | ned@company.com | Basic-With-ActiveChange | | DC_42<br>DC_82<br>Rose_checkpoint<br>Poppy_juniper | Fri Feb 12 2016 | 3 years ago | 3 years ago |
| ☑ | 3372 | Web access to internal web site | ned@company.com | Basic-With-ActiveChange | | DC_42<br>Rose_checkpoint<br>Poppy_juniper<br>DC_82 | Tue Nov 01 2016 | 4 years ago | 4 years ago |
| ☑ | 3034 | BusinessFlow Change Request for Help Desk | ned@company.com | Basic-With-ActiveChange-for-CKP | | | Thu Nov 06 2014 | 4 years ago | 4 years ago |
| ☑ | 3025 | BusinessFlow Change Request for Help Desk | ned@company.com | Basic-With-ActiveChange-for-CKP | | | Tue Nov 04 2014 | 4 years ago | 4 years ago |
| ☑ | 3035 | BusinessFlow Change Request for Help Desk | ned@company.com | Basic-With-ActiveChange-for-CKP | | DC_42<br>Flower_ASA | Fri Nov 28 2014 | 4 years ago | 4 years ago |
| ☑ | 3038 | BusinessFlow Change Request for Email | ned@company.com | Basic-With-ActiveChange-for- | | | Mon Nov 03 | 4 years | 4 years ago |

4. Specify the desired change requests, by doing any of the following:

   - Select the check box next to the change requests' names to re-certify individual change requests in the list.
   - Click **Check All** to re-certify all change requests in the list.
   - Click **Clear All** to not re-certify any of the change requests in the list.

5. Do one of the following:

| | |
|---|---|
| **Postpone expiration** | To postpone the expiration date of the selected change request(s) without recertifying them, click **Mark for Future Recertification**.<br>The due date for the change request(s) is deferred to 365 days from the original due date.<br>In this case, no re-certification request is created. |

| | |
|---|---|
| **Re-certify** | To re-certify the selected change request(s), click **Initiate Recertification Process**.<br>A re-certification request is automatically created for each of the selected change requests. The due date for the re-certification requests is 14 days from the present date.<br>A success message appears with the ID number of the re-certification request(s). To view the request(s), click the ID number(s). |

# Certify or plan traffic removal

**Relevant for network operation users**

Once you have received responses from the related change requestors, you must decide whether to certify the Allow traffic or plan its removal.

This topic describes how to certify or plan traffic removal for recertification requests in the Approve stage.

> **Note:** To determine a change request's stage, view the change request. The stage is indicated by the Change Request Lifecycle Status Bar. For details, see View change requests.

## Certify traffic

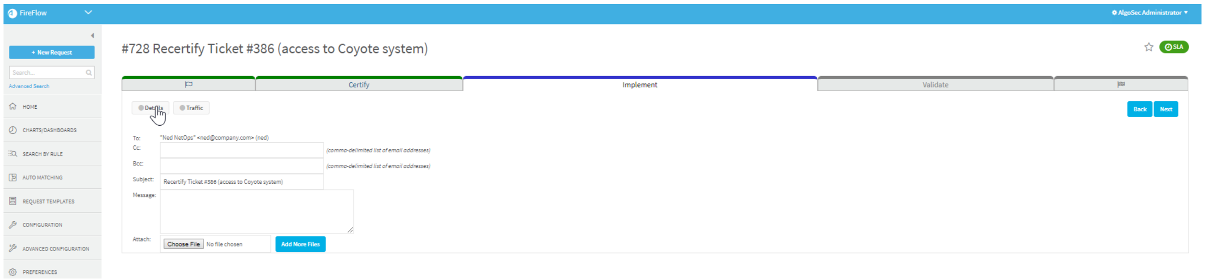
Certify the Allow traffic if the related change requestors' responses indicate that the Allow traffic should not be removed.

### Do the following:

1. View the change request. For details, see View change requests.
2. Click ≡ , and then click **Traffic is Needed**.

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

   The Certify Change Request page is displayed.



#728 Recertify Ticket #386 (access to Coyote system)

To: "Ned NetOps" <ned@company.com> (ned)

Cc: (comma-delimited list of email addresses)

Bcc: (comma-delimited list of email addresses)

Subject: Recertify Ticket #386 (access to Coyote system)

Message:

Attach:

4. Complete the fields as needed. For details, see Respond to change requests.
5. Click **Next**.

The email message is sent to the requestor, the change request is resolved, and the HOME page appears.

## Plan traffic removal

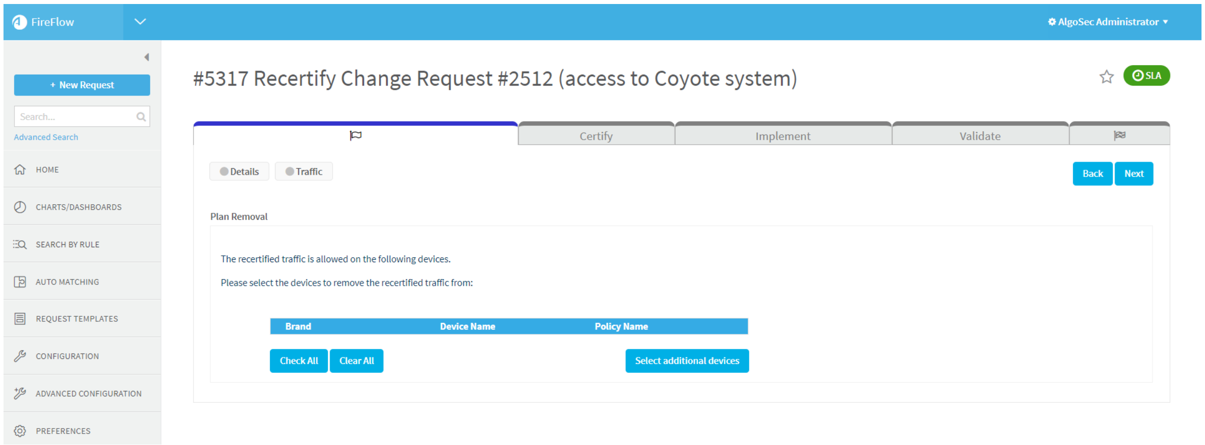
Plan traffic removal when the related change requestors' responses indicate that the Allow traffic should be removed.

**Do the following:**

**To plan traffic removal**

1. View the change request. For details, see View change requests.
2. Click , and then click **Plan Removal**.

   The Plan Removal page appears displaying a list of devices on which the traffic is allowed.



#5317 Recertify Change Request #2512 (access to Coyote system)

Plan Removal

The recertified traffic is allowed on the following devices.

Please select the devices to remove the recertified traffic from:

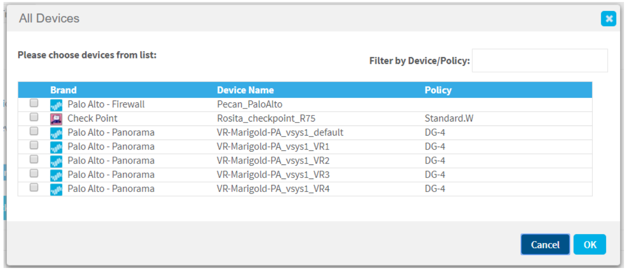
| Brand | Device Name | Policy Name |
|---|---|---|

3. Specify the devices from which the Allow traffic should be removed, by doing any of the following:

   - To select an individual device in the list, select the check box next to its name.
   - Click **Check All** to select all devices in the list.
   - Click **Clear All** to select none of the devices in the list.
   - To specify additional devices that are not listed, do the following:

     a. Click **Select additional devices**.

        The **All Devices** dialog box opens with a list of all devices in the FireFlow system.



All Devices

Please choose devices from list:

Filter by Device/Policy:

| | Brand | Device Name | Policy |
|---|---|---|---|
| □ | Palo Alto - Firewall | Pecan_PaloAlto | |
| □ | Check Point | Rosita_checkpoint_R75 | Standard.W |
| □ | Palo Alto - Panorama | VR-Marigold-PA_vsys1_default | DG-4 |
| □ | Palo Alto - Panorama | VR-Marigold-PA_vsys1_VR1 | DG-4 |
| □ | Palo Alto - Panorama | VR-Marigold-PA_vsys1_VR2 | DG-4 |
| □ | Palo Alto - Panorama | VR-Marigold-PA_vsys1_VR3 | DG-4 |
| □ | Palo Alto - Panorama | VR-Marigold-PA_vsys1_VR4 | DG-4 |

     b. Select the check boxes next to the desired device(s).

     c. Click **OK**.

        The selected devices appear in the list of devices from which to remove the Allow traffic, with an asterisk next to their name.

d. Click **Next**.

The recertification request proceeds to the Implement stage.

A request is opened for each of the selected devices.

# FireFlow for requestors

FireFlow requestors only have permissions to send requests for FireFlow requesting a device change to be made, and view and reply to their own change requests.

This topic provides an index of topics that are relevant for FireFlow requestors.

## General FireFlow information

Requestors should understand the basics of working in FireFlow and the types of change requests and workflows supported.

For details, see:

- Logins and other basics
- Welcome to FireFlow
- Configure user preferences
- Request templates and workflows

## Request and view changes

FireFlow requestors can use a variety of methods to request changes, depending on system and user configuration.

For details, see:

- Request changes
- Change request field references
- Change request wizards

Once a change request is submitted, view and track it's status as needed. For details, see:

- Manage change requests
- View change requests
- Search for change requests
- Verify change request results

- Resolve or return change requests
- Respond to change requests

# Manage change requests

**Relevant for: Privileged users**

This section includes a collection of procedures for managing different types of change requests, for various workflows, and at various stages.

For details, see:

| | |
|---|---|
| **Generic procedures** | • View change requests<br>• Advanced change request edits<br>• Respond to change requests<br>• Report change verifications |
| **Procedures per request type** | • Manage generic change requests<br>• Manage traffic change requests<br>• Manage object change requests<br>• Manage rule removal requests<br>• Manage rule modification requests<br>• Manage web filtering change requests<br>• Manage re-certification requests<br>• Manage verbatim requests |

➔ **See also**:

- Manage traffic change requests training video
- Process an object change request training video
- Removing and re-certifying rules training video

## View change requests

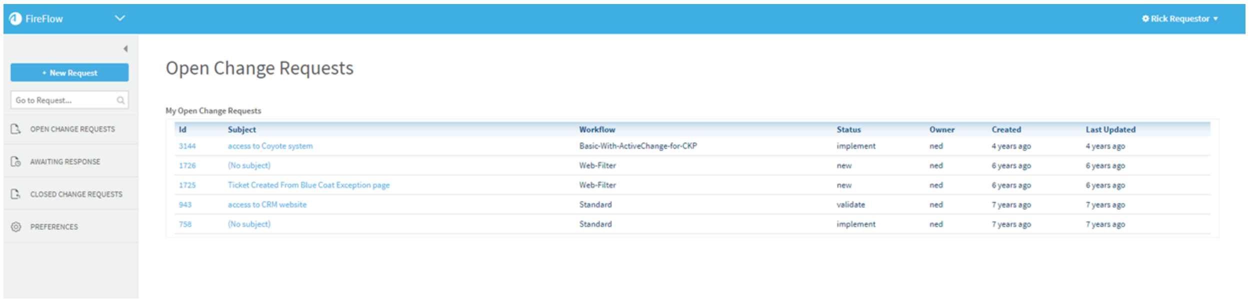
This topic describes the various procedures available to view change requests in FireFlow.

### View open change requests

The **Open Change Requests** list displays all of your change requests that have not yet been resolved, and allows you to track these change requests' statuses.

To view the **Open Change Requests** list, click **Open Change Requests** from the main menu on the left.

The **Open Change Requests** page appears with a list of your open change requests.



Open Change Requests

My Open Change Requests

| Id | Subject | Workflow | Status | Owner | Created | Last Updated |
|---|---|---|---|---|---|---|
| 3144 | access to Coyote system | Basic-With-ActiveChange-for-CKP | implement | ned | 4 years ago | 4 years ago |
| 1726 | (No subject) | Web-Filter | new | ned | 6 years ago | 6 years ago |
| 1725 | Ticket Created From Blue Coat Exception page | Web-Filter | new | ned | 6 years ago | 6 years ago |
| 943 | access to CRM website | Standard | validate | ned | 7 years ago | 7 years ago |
| 758 | (No subject) | Standard | implement | ned | 7 years ago | 7 years ago |

**Note:** Click a change request **ID** or **subject** to open the change request.

By default, statuses include the following:

| | |
|---|---|
| **plan** | The change request has been assigned an owner and is in the **Plan** stage. |
| **approve** | The change request is in the **Approve** stage and being checked for security risks.<br>An information security user will decide whether to approve the change request, based on the check results. |
| **create work order** | The change request is now in the **Implement** stage, and the work order is being planned. |
| **implement** | The change request is now in the **Implement** stage, and the required change is being implemented. |
| **validate** | The change request is now in the **Validate** stage. |
| **user accept** | The change request is now in the **Validate** stage, and the requestor has been asked to verify implementation success. |
| **user disapproved** | The change request is now in the **Validate** stage, and the requestor has marked the change as not working, using the **Change Doesn't Work** button. |

These statuses can be changed / customized by FireFlow administrators.

## View change requests awaiting response

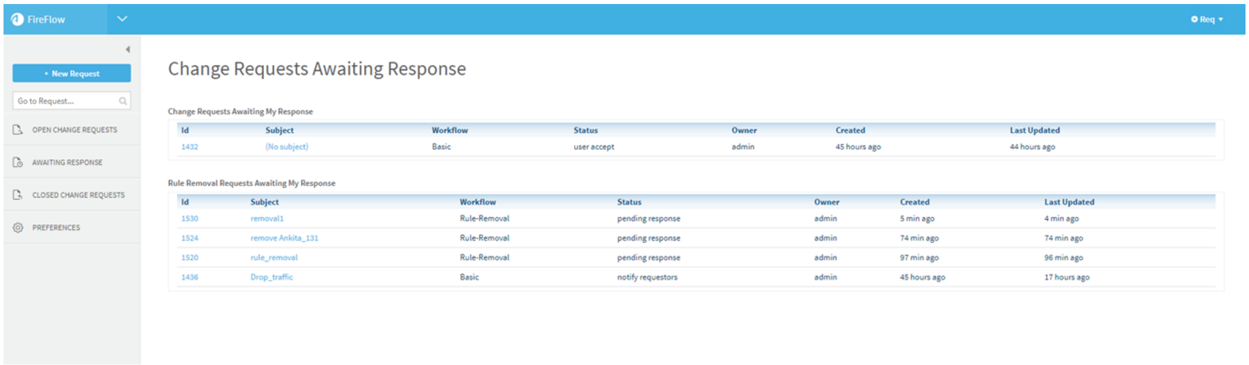
The **Awaiting Response** list displays all the change requests that are waiting to be handled by you, and allows you to view the status of these change requests.

To view the **Awaiting Response** list, click **Awaiting Response** from the main menu on the left.

The **Change Requests Awaiting Response** page is displayed with the following lists of change requests that are awaiting your response:

- **Change Requests Awaiting My Response** - Change requests you submitted.
- **Rule Removal Requests Awaiting My Response** - Rule removal requests that affect traffic that you requested.

For example:



Change Requests Awaiting Response

Change Requests Awaiting My Response

| Id | Subject | Workflow | Status | Owner | Created | Last Updated |
|---|---|---|---|---|---|---|
| 1432 | (No subject) | Basic | user accept | admin | 45 hours ago | 44 hours ago |

Rule Removal Requests Awaiting My Response

| Id | Subject | Workflow | Status | Owner | Created | Last Updated |
|---|---|---|---|---|---|---|
| 1530 | removal1 | Rule-Removal | pending response | admin | 5 min ago | 4 min ago |
| 1524 | remove Ankita_131 | Rule-Removal | pending response | admin | 74 min ago | 74 min ago |
| 1520 | rule_removal | Rule-Removal | pending response | admin | 97 min ago | 96 min ago |
| 1436 | Drop_traffic | Basic | notify requestors | admin | 45 hours ago | 17 hours ago |

**Note:** Click a change request **ID** or **subject** to open the change request.

By default, statuses include the following:

| | |
|---|---|
| **plan** | The change request has been assigned an owner and is in the **Plan** stage. |
| **approve** | The change request is in the **Approve** stage and being checked for security risks.<br>An information security user will decide whether to approve the change request, based on the check results. |

| | |
|---|---|
| **create work order** | The change request is now in the **Implement** stage, and the work order is being planned. |
| **implement** | The change request is now in the **Implement** stage, and the required change is being implemented. |
| **validate** | The change request is now in the **Validate** stage. |
| **user accept** | The change request is now in the **Validate** stage, and the requestor has been asked to verify implementation success. |
| **user disapproved** | The change request is now in the **Validate** stage, and the requestor has marked the change as not working, using the **Change Doesn't Work** button. |

For more details, see:

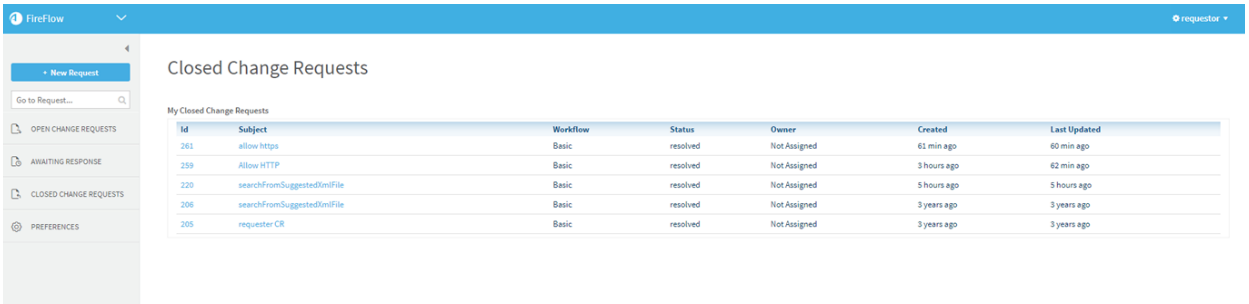
- Verify change request results
- Respond to change requests

## View closed change requests

The **Closed Change Requests** list displays all of your change requests that have been resolved, and allows you to track these change requests' statuses.

To view the **Closed Change Requests** list, click **Closed Change Requests** from the main menu on the left.

The **Closed Change Requests** page is displayed with a list of your closed change requests.



Closed Change Requests

My Closed Change Requests

| Id | Subject | Workflow | Status | Owner | Created | Last Updated |
|---|---|---|---|---|---|---|
| 261 | allow https | Basic | resolved | Not Assigned | 61 min ago | 60 min ago |
| 259 | Allow HTTP | Basic | resolved | Not Assigned | 3 hours ago | 62 min ago |
| 220 | searchFromSuggestedXmlFile | Basic | resolved | Not Assigned | 5 hours ago | 5 hours ago |
| 206 | searchFromSuggestedXmlFile | Basic | resolved | Not Assigned | 3 years ago | 3 years ago |
| 205 | requester CR | Basic | resolved | Not Assigned | 3 years ago | 3 years ago |

**Note:** Click a change request **ID** or **subject** to open the change request.

Statuses include the following:

| | |
|---|---|
| **pending match** | The change request has been resolved and is now in the **Match** stage. |
| **matched** | During auto matching, a device change was matched to the change request; however, matching is not yet complete. |
| **resolved** | Auto matching is complete. |
| **rejected** | The change request was rejected. |

## View change requests on your home page

Your **Home** page displays all of the recently updated change requests in the system, divided into lists according to their current lifecycle stage.

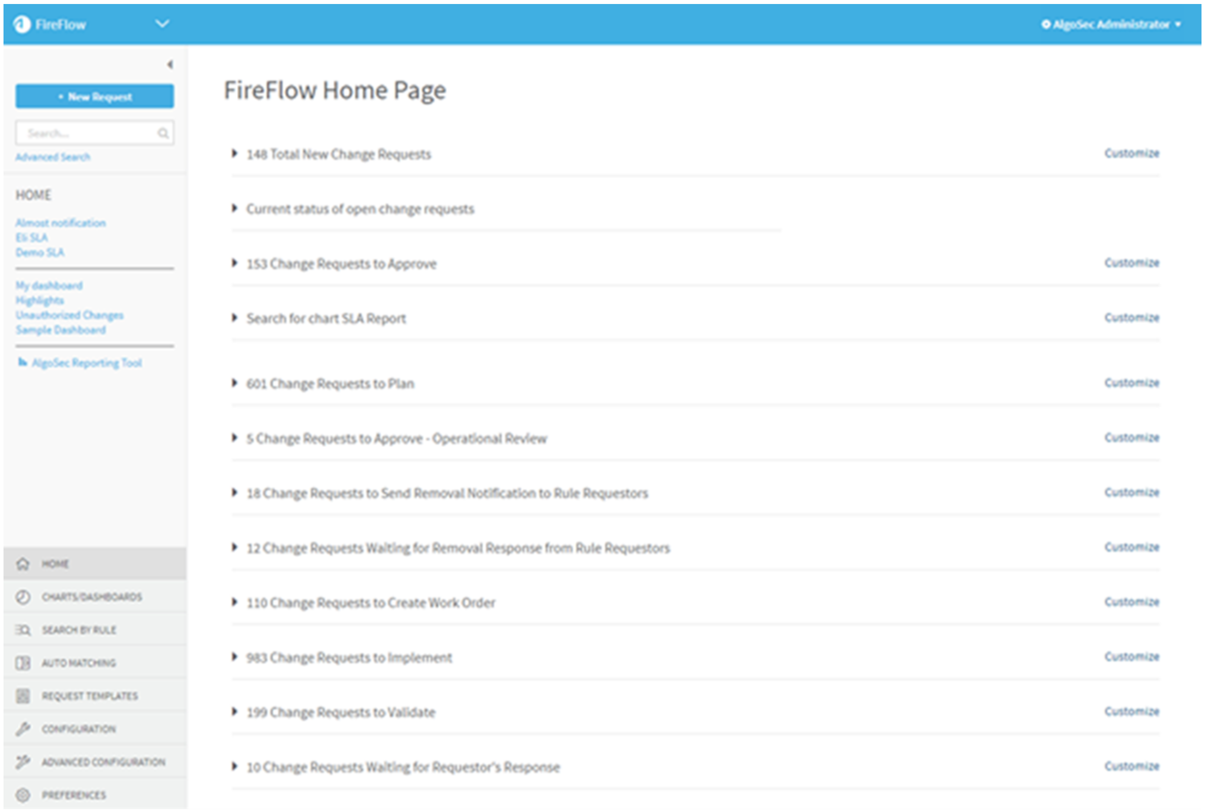
**Note:** By default, only lists that are relevant to your user role will appear in your **Home** page.

**Tip:** Customize this page by adding additional change request lists or changing the number of change requests displayed in each list.

### Do the following:

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

   The **FireFlow Home Page** is displayed.



FireFlow Home Page

- 148 Total New Change Requests — Customize
- Current status of open change requests
- 153 Change Requests to Approve — Customize
- Search for chart SLA Report — Customize
- 601 Change Requests to Plan — Customize
- 5 Change Requests to Approve - Operational Review — Customize
- 18 Change Requests to Send Removal Notification to Rule Requestors — Customize
- 12 Change Requests Waiting for Removal Response from Rule Requestors — Customize
- 110 Change Requests to Create Work Order — Customize
- 983 Change Requests to Implement — Customize
- 199 Change Requests to Validate — Customize
- 10 Change Requests Waiting for Requestor's Response — Customize

2. Click a change list to expand it and display the list of items.

> **Note:** If the number of items in the list exceeds the configured maximum number of change requests to display per list, not all change requests in the change request list will be displayed.
>
> In such cases, click the heading to view all items. The **Found** page appears displaying the relevant change requests.

3. To sort the list according to a column, click the column heading.

   To reverse the sort order, click the column heading again.

### Home page change request lists

By default, the following change requests lists are displayed on your home page:

| | |
|---|---|
| **New Change Requests** | A list of change requests in the system that are new and still in the Request stage, and for which initial change planning has been completed.<br>**Note:** Upon change request creation, FireFlow checks the traffic specified in the change request against devices. New change requests will not appear in this list until FireFlow has completed this task. This may take a few minutes.<br>This list only appears for users with network operations or administrator role. |
| **Change Requests to Plan** | A list of change requests in the system that are currently in the Plan stage.<br>This list only appears for users with network operations or administrator role. |
| **Change Requests to Approve** | A list of change requests in the system that are currently in the Check stage.<br>This list only appears for users with information security or administrator role. |
| **Change Requests to Send Removal Notification to Rule Requestors** | 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.<br>This list only appears for users with network operations user or administrator role. |
| **Change Requests Waiting for Removal Response from Rule Requestors** | 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 removals are approved.<br>This list only appears for users with network operations user or administrator role. |
| **Change Requests to Create Work Order** | A list of change requests in the system that are currently in the Implement stage and awaiting a work order to be created.<br>This list only appears for users with network operations or administrator role. |

| | |
|---|---|
| **Change Requests to Implement** | A list of change requests in the system that are currently in the Implement stage and awaiting implementation.<br>This list only appears for users with network operations or administrator role. |
| **Change Requests to Validate** | A list of change requests in the system that are currently in the Validate stage.<br>This list only appears for users with network operations or administrator role. |
| **Change Requests Waiting for Requestor's Response** | 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.<br>This list only appears for users with network operations or administrator role. |
| **Change Requests that Received Requestor's Response** | A list of change requests in the system that are currently in the Validate stage, for which the requestor has confirmed that the requested change was implemented successfully.<br>This list only appears for users with network operations or administrator role. |
| **Change Requests that Flagged by Requestor as "Change Does Not Work"** | A list of change requests in the system that have been flagged by the requestor as "Change Does Not Work".<br>This list only appears for users with network operations or administrator role. |
| **Requests Pending Implementation** | A list of requests in the system that are currently in the Implement stage and awaiting implementation of their devices and policies.<br>This list only appears for users with network operations or administrator role. |
| **Change Requests that are due to be recertified** | A list of traffic change requests in the system that expired, and which should be recertified. |

| | |
|---|---|
| **Change Requests to Expire in the Next 30 days** | A list of change requests in the system that will expire between today and 30 days from today.<br>This list only appears for users with network operations or administrator role. |
| **Total New Change Requests** | 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. |
| **Change Requests to Review** | A list of change requests in the system that use the Multi-Approval or Parallel-Approval workflow, and which are currently waiting for your review.<br>This list only appears for users with controller role. |
| **Change Requests I own** | A list of change requests in the system that are owned by you. |
| **Change Requests Relevant to My Roles** | A list of change requests in the system that are relevant to the user roles you are assigned. |
| **Bookmarked Change Requests** | A list of change requests you bookmarked. |

## View individual change requests

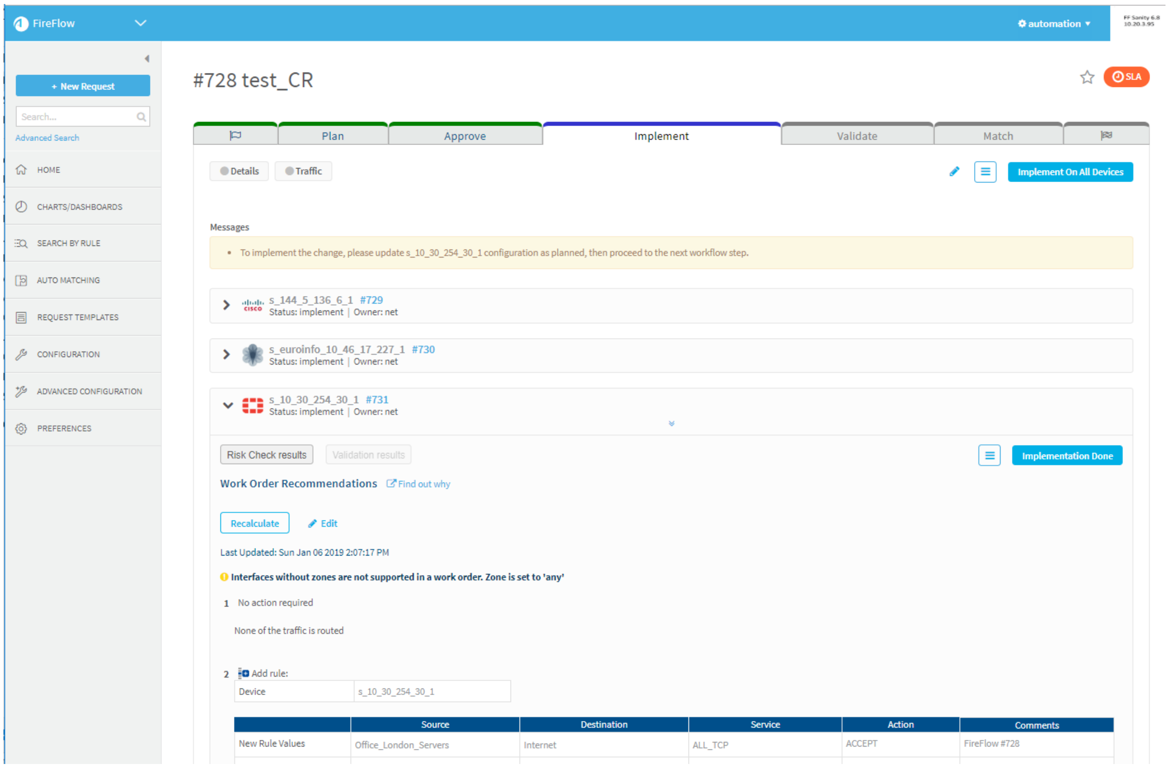
View a change request's details, including the change request's current lifecycle stage and basic information about the change request, such as the requestor, owner, original request details, and internal and external links. Additional information is provided depending on the change request's current lifecycle stage.

### Do the following:

1. Browse to or search for a change request, and click the ID or subject to open it.

   For details, see View change requests on your home page and Search for change requests.

   The change request appears.



#728 test_CR

Messages

- To implement the change, please update s_10_30_254_30_1 configuration as planned, then proceed to the next workflow step.

s_144_5_136_6_1 #729
Status: implement | Owner: net

s_euroinfo_10_46_17_227_1 #730
Status: implement | Owner: net

s_10_30_254_30_1 #731
Status: implement | Owner: net

Work Order Recommendations

Last Updated: Sun Jan 06 2019 2:07:17 PM

Interfaces without zones are not supported in a work order. Zone is set to 'any'

1 No action required

None of the traffic is routed

2 Add rule:

| | |
|---|---|
| Device | s_10_30_254_30_1 |

| | Source | Destination | Service | Action | Comments |
|---|---|---|---|---|---|
| New Rule Values | Office_London_Servers | Internet | ALL_TCP | ACCEPT | FireFlow #728 |

This page displays the following details:

| | |
|---|---|
| **Change request title and ID** | View these at the top of the page. |
| **Change request lifecycle status bar** | View this status bar just under the title and ID.<br>The status bar maps the stages in the lifecylce from left to right.<br>• The current stage appears in **blue**, completed stages appear in **green**, and future stages appear in **grey**.<br>• **An empty flag** indicates that the request is new; **a checkered flag** indicates that the request is resolved.<br>• Click a previous stage to display a read-only view of the request data for that stage.<br>For more details, see Change request statuses. |

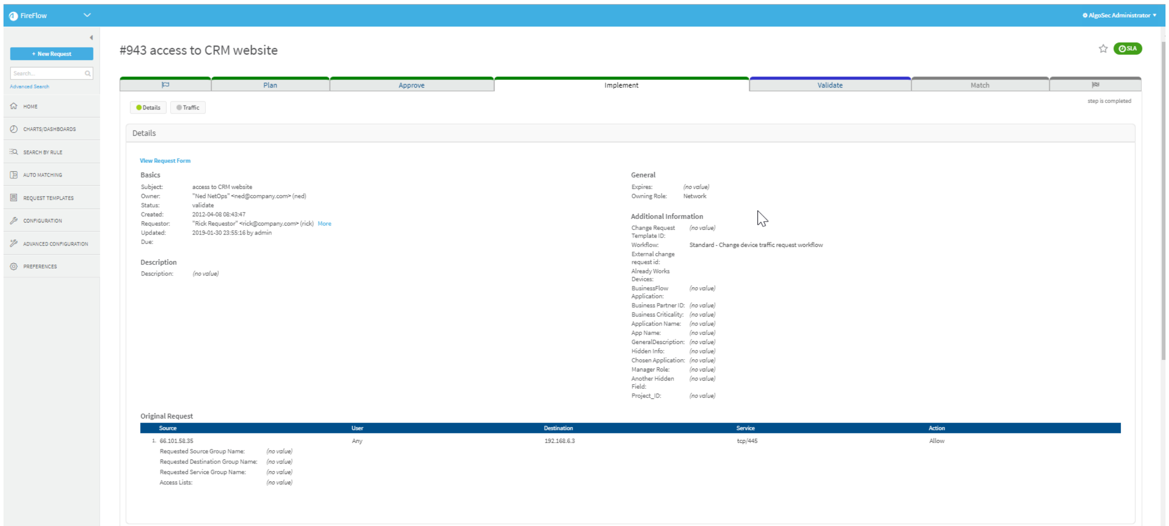
| | |
|---|---|
| **Relevant device or policy** | The device policy is displayed with the request's status, owner, and ID.<br>For Palo Alto and Check Point policies, the **View Policy** link appears.<br>For change requests that affect multiple devices or policies, each device appears in its own panel, and each panel contains all the information for the sub request. Clicking the panel reveals additional device information:<br>• **IP**. The device's IP address.<br>• **Latest Report**. The date of the device's latest AFA report, and a link to the report. |

2. To view change request information for a device, click ▶ next to the desired device.

   The change request information relevant to the device's stage is displayed below the device panel.

3. To view detailed information about the change request, click **Details**.

   The **Details** area appears.



#943 access to CRM website

Details

Basics

Subject: access to CRM website
Owner: "Ned NetOps" <ned@company.com> (ned)
Status: validate
Created: 2012-04-08 08:43:47
Requestor: "Rick Requestor" <rick@company.com> (rick) More
Updated: 2019-01-30 23:55:16 by admin
Due:

Description

Description: *(no value)*

General

Expires: *(no value)*
Owning Role: Network

Additional Information

Change Request Template ID: *(no value)*
Workflow: Standard - Change device traffic request workflow
External change request id:
Already Works Devices:
BusinessFlow Application: *(no value)*
Business Partner ID: *(no value)*
Business Criticality: *(no value)*
Application Name: *(no value)*
App Name: *(no value)*
GeneralDescription: *(no value)*
Hidden Info: *(no value)*
Chosen Application: *(no value)*
Manager Role: *(no value)*
Another Hidden Field: *(no value)*
Project_ID: *(no value)*

Original Request

| | Source | User | Destination | Service | Action |
|---|---|---|---|---|---|
| 1. | 66.101.58.35 | Any | 192.168.6.3 | tcp/445 | Allow |

Requested Source Group Name: *(no value)*
Requested Destination Group Name: *(no value)*
Requested Service Group Name: *(no value)*
Access Lists: *(no value)*

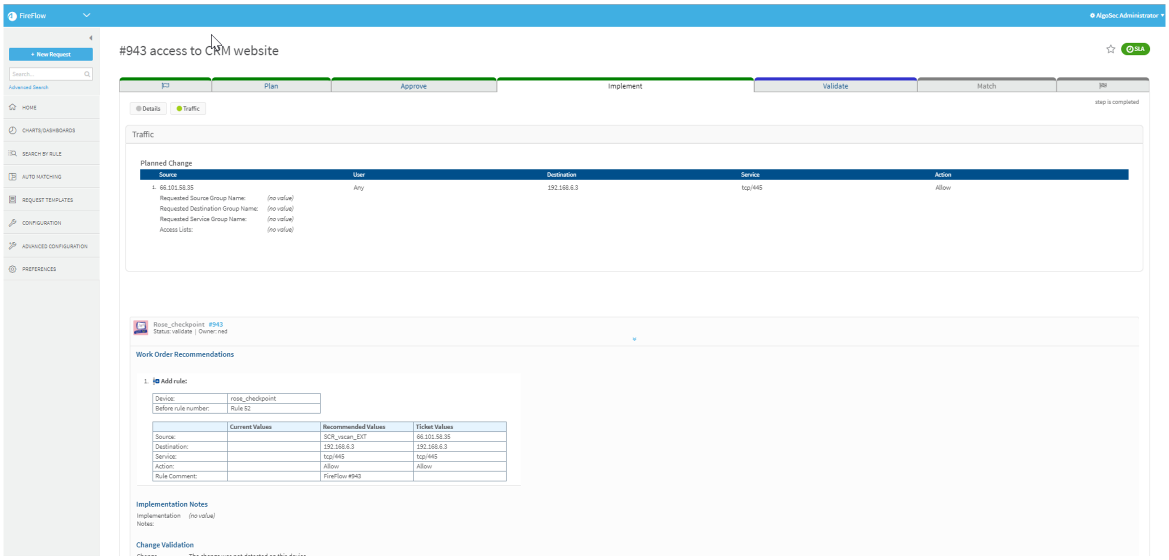
   For information about fields, see Details Fields (see Details Fields).

4. To view specific change request information relevant to the change request type,

click the button to the right of the **Details** button.

For a traffic change request, this will be the **Traffic** button, for an object change request, this will be the **Object** button, for rule removal or modification request this will be the **Rules** button, and for a web filtering request, this will be the **Web Filtering** button.

The relevant information appears.



#943 access to CRM website

Traffic

Planned Change

| | Source | User | Destination | Service | Action |
|---|---|---|---|---|---|
| 1. | 66.101.58.35 | Any | 192.168.6.3 | tcp/445 | Allow |

Requested Source Group Name: *(no value)*
Requested Destination Group Name: *(no value)*
Requested Service Group Name: *(no value)*
Access Lists: *(no value)*

Rose_checkpoint #943
Status: validate | Owner: ned

Work Order Recommendations

1. Add rule:

| | |
|---|---|
| Device: | rose_checkpoint |
| Before rule number: | Rule 52 |

| | Current Values | Recommended Values | Ticket Values |
|---|---|---|---|
| Source: | | SCR_vscan_EXT | 66.101.58.35 |
| Destination: | | 192.168.6.3 | 192.168.6.3 |
| Service: | | tcp/445 | tcp/445 |
| Action: | | Allow | Allow |
| Rule Comment: | | FireFlow #943 | |

Implementation Notes

Implementation Notes: *(no value)*

Change Validation

5. To view information about an AppViz application that is related to the change request, click **Business Application Information**. This includes the application diagram and the changes to the application flows which are being implemented with the change request. For details, see View business application details.

> **Note:** The **Business Application Information** button only appears for traffic change requests which were opened for the sake of an application in AppViz. The **Business Application Information** button is disabled for users who do not have the AppViz permissions required to view this information about this application.

6. To view previously calculated information, do one of the following:

| | |
|---|---|
| **View work order, risk check results, or validation results** | To view the work order, risk check results and/or validation results for a device, do the following:<br>a. Click ▶ next to the desired device to display the device's change request information.<br>Immediately below the device panel, a set of buttons appears that is relevant to the device's calculated information. These buttons may include **Work Order**, **Risk Check Results** and/or **Validation Results**.<br>If the information has not been calculated, the button will be disabled.<br>b. Click the desired button.<br>A window appears with the calculated information for the desired device. |
| **View initial planning results** | To view a change request's initial planning results in PDF format, do the following:<br>a. In the Change Request Lifecycle Status Bar, click **Plan**.<br>The read-only view of the **Plan** tab appears.<br>b. Click **Initial Plan results**.<br>The initial plan PDF appears.<br>**Note:** The Initial Plan results PDF will only appear for a change request once the Plan stage has been completed. The PDF file does not include the network map generated during Initial Planning.<br>The Initial Plan results PDF may not appear, depending on your FireFlow configuration. |

7. To view information about the SLA, hover over 🕘 SLA.

   The SLA information appears. For more details, see SLA Information Fields.

   **Note:** If the SLA icon is orange, an active SLO is expired.

### Change request statuses

Individual change requests might have any of the following statuses:

| | |
|---|---|
| **plan** | The change request has been assigned an owner and is in the **Plan** stage. |
| **already works** | The requested change already exists, and there is therefore no need to implement the change request. |
| **approve** | The change request is in the **Approve** stage and being checked for security risks. An information security user will decide whether to approve the change request, based on the check results. |
| **approved** | The change request is in the **Approve** stage has been approved by an information security user. |
| **create work order** | The change request is now in the **Implement** stage, and the work order is being planned. |
| **implement** | The change request is now in the **Implement** stage, and the required change is being implemented. |
| **validate** | The change request is now in the **Validate** stage. |
| **user accept** | The change request is now in the **Validate** stage, and the requestor has been asked to verify implementation success. |
| **user confirmed** | The change request is now in the **Validate** stage, and the requestor has marked the change as working, using the **Change Works** button.<br>**Note:** By default, the **user confirmed** status is not used, and when the requestor clicks the **Change Works** button, the change request automatically transitions to the **pending match** status. If desired, you can modify the workflow configuration to use this status. |
| **user disapproved** | The change request is now in the **Validate** stage, and the requestor has marked the change as not working, using the **Change Doesn't Work** button. |
| **requestor response** | The change request is in the **Validate** stage, and the requestor has reported the change implementation results via email. |
| **review** | The change request is in a second approval stage called "**Review**". |
| **notify requestors** | The rule removal request is in the **Approve** stage, and a rule removal notification will be sent to the rule's traffic requestors. |

| | |
|---|---|
| **pending response** | The rule removal request is in the **Approve** stage and awaiting the requestor's confirmation (and possibly the confirmation of other users) that the requested rule removal is approved. |
| **pending match** | The change request has been resolved and is now in the **Match** stage. |
| **matched** | During auto matching, a device change was matched to the change request; however, matching is not yet complete. |
| **resolved** | Auto matching is complete. |
| **rejected** | The change request was rejected. |
| **certified** | The change request was certified. |
| **deleted** | The change request was deleted. |

## Details Fields

Each change request includes the following details. The items displayed for you may differ, depending on your user permissions.

### Basics area

This area displays basic information about the change request.

| | |
|---|---|
| **Owner** | The change request owner's username and email address, in the format `username <email>`.<br>For example, "bobsnetops<bobsnetops@mycompany.com>".<br>If the change request has not yet been assigned an owner, this field displays "Not assigned yet". |
| **Status** | The change request's status. For details, see Change request statuses. |
| **Created** | The date and time when the change request was created. |

| | |
|---|---|
| **Requestor** | The usernames and email addresses of the requestors, in the format `"username" <email>`. For example, "johns" <johnsmith@mycompany.com>.<br>To view more information about the requestor, and links to other related change requests, click the **More** link. For information on the displayed areas and fields, see More Fields |
| **Updated** | The date and time when the change request was last updated, followed by the username of the person who last updated it. |
| **Due** | The date by which this change request should be resolved. This can be one of the following:<br>• A date<br>• **Not set:** No due date was set. |
| **Priority** | A number indicating this request's priority, where 0 indicates lowest priority. |
| **CC** | Email addresses to which the FireFlow system will send copies of all email messages regarding this request. |

### Relevant Devices area

This area lists all devices relevant to the change requests and a link to all devices with the same policy.

For AWS and Azure, all containers and instances/VMs relevant to the security group in the change request are listed.

### General area

This area displays general information about the change request.

| | |
|---|---|
| **Expires** | The date on which the change request will expire. |
| **Owning Role** | The role to which the change request is currently attributed. |

| | |
|---|---|
| **All Responsible Roles** | All roles responsible for the change request in its current lifecycle stage.<br>This field appears only for Parallel-Approval change requests, and only when there is more than one responsible role in the current lifecycle stage. |
| **Pending Responsible Roles** | The roles responsible for handling the change request in its current lifecycle stage, but which have not yet approved the change request.<br>This field appears only for Parallel-Approval change requests, and only when there is more than one responsible role in the current lifecycle stage. |

### Recertified Change Request

If the change request is a recertification request, this area appears displaying related change requests.

Each change request is represented by its ID number, followed by its owner, relevant device, and current status. For details, see Change request statuses.

To view a change request, click on its ID number.

### Additional Information area

This area displays additional information about the change request.

| | |
|---|---|
| **From Template** | The template used for the request on which this change request is based.<br>This field only appears if the Standard request template was not used. |
| **Change Request Template ID** | The ID of the change request's template. |
| **Workflow** | The workflow used for this change request. |
| **External change request id** | The ID number of a related change request in an external change management system that is integrated with FireFlow. |

| | |
|---|---|
| **Already Works Devices** | The devices on which the requested change is already implemented.<br>For example, if the change request is to allow a certain type of traffic, this field will list the devices on which that traffic is already allowed. |

### Links area

This area displays links between this change request and other change requests.

| | |
|---|---|
| **Refers to** | The ID numbers of change requests to which this change request refers, separated by spaces.<br>This field is optional. |
| **Referred to by** | The ID numbers of change requests that refer to the change request, separated by spaces.<br>This field is optional. |

### Original Request area

This area displays the values specified in the original request.

These fields are read-only.

| | |
|---|---|
| **Source** | The IP address, IP range, network, or device object. |
| **Destination** | The IP address, IP range, network, or device object. |
| **Service** | The device service or port for the connection. |
| **User** | The user for the connection.<br>This is only relevant for Check Point and Palo Alto devices. For all other devices, the field's value will always be **Any**. |
| **Application** | The network application for the connection.<br>This is only relevant for Palo Alto Devices. For all other devices, the field's value will always be **Any**. |

| | |
|---|---|
| **Action** | The device action to perform for the connection. This can be either of the following:<br>- **Allow:** Allow the connection.<br>- **Drop:** Block the connection. |
| **Source NAT** | The source NAT value to which the connection's source should be translated.<br>**Note:** If the **Source after NAT** field appears below this field, then this field displays the source NAT value *before* translation. |
| **Source after NAT** | The source NAT value after translation. |
| **Destination NAT** | The destination NAT value to which the connection's destination should be translated.<br>**Note:** If the **Destination after NAT** field appears below this field, then this field displays the destination NAT value *before* translation. |
| **Destination after NAT** | The destination NAT value after translation. |
| **Port Translation** | The port value to which the connection's port should be translated.<br>**Note:** If the **Port after Translation** field appears below this field, then this field displays the port value *before* translation. |
| **Port after Translation** | The port value after translation. |
| **NAT Type** | The type of NAT (**Static** or **Dynamic**). |
| **Requested action** | The requested action in a Rule Removal request (**Disable Rule** or **Remove Rule**). |

### More Fields

This area displays more details, such as about the requestor:

| | |
|---|---|
| **Full Name** | The requestor's full name. |
| **Mobile Phone** | The requestor's mobile telephone number. |
| **Home Phone** | The requestor's home telephone number. |
| **Work Phone** | The requestor's work telephone number. |
| **Pager Phone** | The requestor's pager telephone number. |
| **Email Address** | The requestor's email address. |
| **Comments about this user** | Comments about this requestor. |
| **This user's 10 highest priority change requests** | A list of the 10 highest priority change requests that this requestor created.<br>Each change request is represented by its ID number, followed by its current status. For details, see Change request statuses.<br>To view a change request, click on its number. |

## View business application details

The **Business Application Information** button appears for traffic change requests which were opened for the sake of an application in AppViz.

> **Note:** This button is disabled for users who do not have the AppViz permissions required to view this information about this application.

The application name appears as a link to the application in AppViz. The **Diagram** tab displays the fully interactive application diagram.

Selecting the **Changed Flow** tab displays the changes to the application's flows which are being implemented with the change request.

### SLA Information Fields

| | |
|---|---|
| Active SLA | A list of currently active SLAs, including their names, due dates, and the amount of time elapsed so far. |
| Completed SLA | A list of completed SLAs, including their names, the amount of time it took to complete them, and their current status. |
| Devices SLA | Click any of the devices to display its SLA information.<br>This field only appears for change requests that affect multiple devices. |

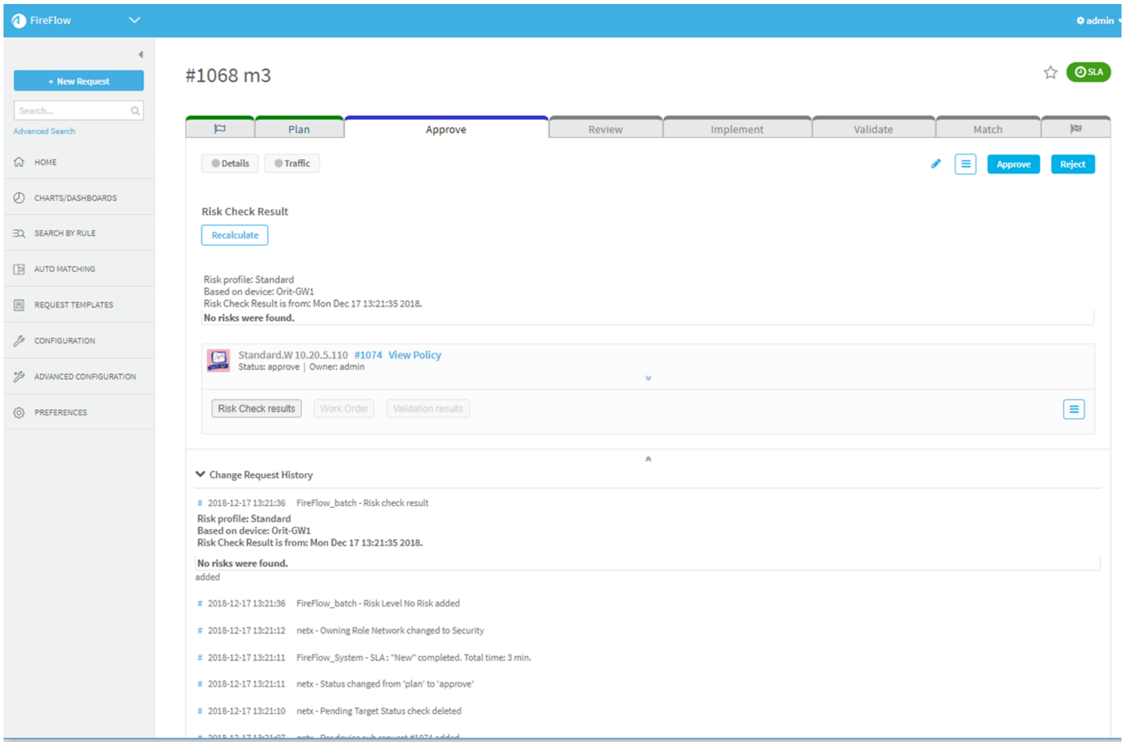
## View change request histories

View a change request's history, including all comments and replies associated with the change request.

### Do the following:

1. View the change request. For details, see View individual change requests.
2. Do one of the following:
    - Click to expand the **History** area. The history is displayed.
    - In the main menu on the left, click **History** under the change request number.

      The **Change Request History** appears displaying all comments and replies associated with this change request.



#1068 m3

Risk Check Result

Risk profile: Standard
Based on device: Orit-GW1
Risk Check Result is from: Mon Dec 17 13:21:35 2018.
**No risks were found.**

Standard.W 10.20.5.110 #1074 View Policy
Status: approve | Owner: admin

Change Request History

# 2018-12-17 13:21:36 FireFlow_batch - Risk check result
**Risk profile: Standard**
**Based on device: Orit-GW1**
**Risk Check Result is from: Mon Dec 17 13:21:35 2018.**
**No risks were found.**
added

# 2018-12-17 13:21:36 FireFlow_batch - Risk Level No Risk added

# 2018-12-17 13:21:12 netx - Owning Role Network changed to Security

# 2018-12-17 13:21:11 FireFlow_System - SLA : "New" completed. Total time: 3 min.

# 2018-12-17 13:21:11 netx - Status changed from 'plan' to 'approve'

# 2018-12-17 13:21:10 netx - Pending Target Status check deleted

# 2018-12-17 13:21:07 netx - Per device sub request #1074 added

For each comment/reply, the following information is displayed:

- **Brief header information,** including the date and time at which the comment/reply was created, the name of the user who created it, and its subject line.
- **The full text of the comment/reply**.

> **Note:** The full text will not appear if you limited the length of displayed messages. For information on configuring this setting, see Customizing General FireFlow Settings.

- **The size of the comment/reply in bytes.**

3. Click **Full headers** to display full header information for each comment/reply, at the top of the **History** area.

4. Click **Brief headers** to display brief header information for each comment/reply, at the top of the **History** area.
5. Click **Download** to view a comment/reply in plain text, next to the desired comment/reply.
6. To view an automatically generated email sent by the FireFlow system, next to the desired "FireFlow_System - Outgoing email recorded" history item, click **Show**.

The email and its full header information appear in a new window.

### Bookmark change requests

If you would like to keep track of a change request, you can bookmark it. The bookmarked change request will appear in your **Home** page's **Bookmarked Change Requests** list.

#### Do the following:

1. View the change request. For details, see View individual change requests.
2. In the top-right corner of the workspace, click the ☆ icon.

   The icon changes to ★ .

You can now view the bookmarked change request in your **Home** page's **Bookmarked Change Requests** list. For details, see View change requests on your home page.

## Search for change requests

This topic describes how to perform a simple search for change requests, as well as how to perform and manage advanced searches.

### Perform a simple search

This procedure describes how to perform a simple text based search for details in change request parameters or histories.

**Tip:** FireFlow also includes advanced search options. For details, see Search for change requests.

## Do the following:

1. In the main menu on the left, enter your search query in the **Search** field.

   Enter any of the following:

   - A change request ID number
   - Status
   - Queue
   - Owner name
   - Requestor email address
   - Subject

   To search across all change request histories, enter your search term using the following syntax:

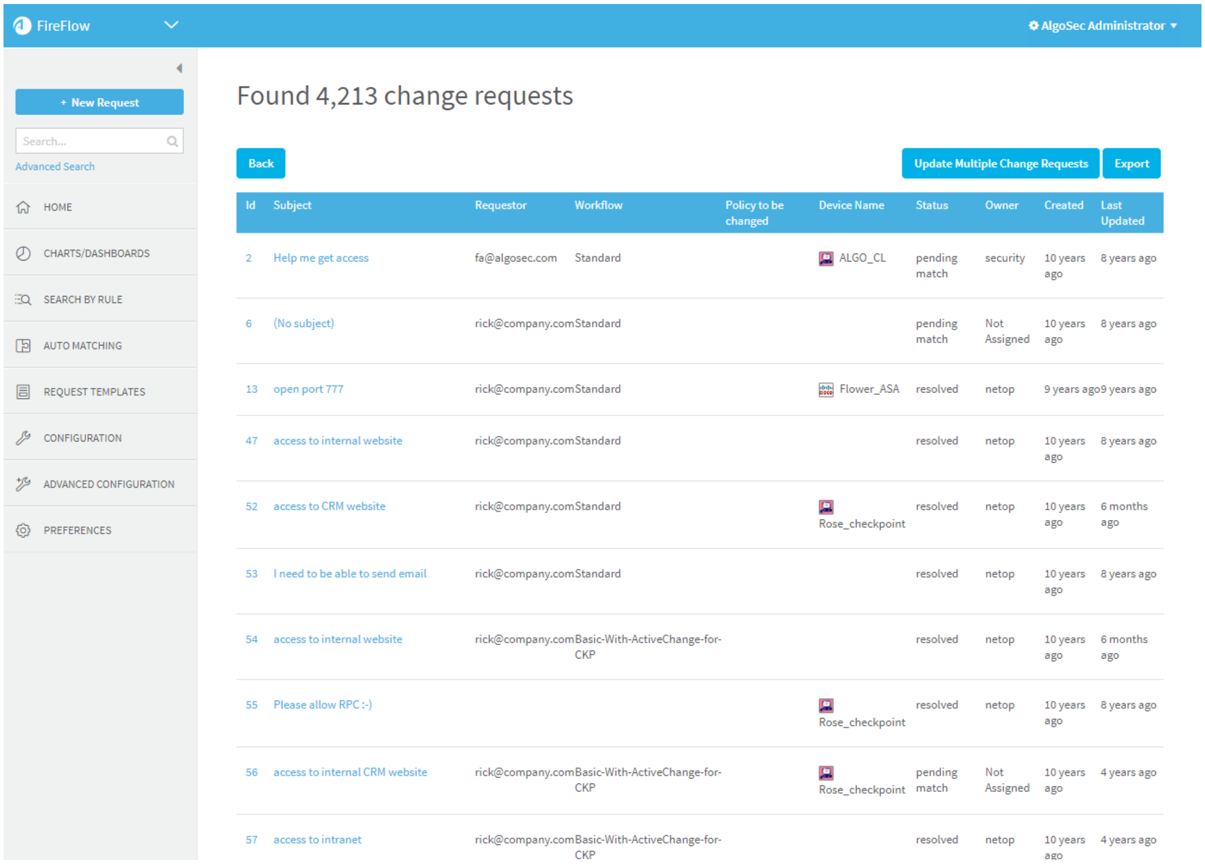
   ```
   fulltext:<search term>
   ```

   **Note:** Searching the full change request history can take a long time.

   For more details, see FireFlow simple search process.

2. Click 🔍 .

   The **Found** page appears displaying search results.



Found 4,213 change requests

| Id | Subject | Requestor | Workflow | Policy to be changed | Device Name | Status | Owner | Created | Last Updated |
|---|---|---|---|---|---|---|---|---|---|
| 2 | Help me get access | fa@algosec.com | Standard | | ALGO_CL | pending match | security | 10 years ago | 8 years ago |
| 6 | (No subject) | rick@company.com | Standard | | | pending match | Not Assigned | 10 years ago | 8 years ago |
| 13 | open port 777 | rick@company.com | Standard | | Flower_ASA | resolved | netop | 9 years ago | 9 years ago |
| 47 | access to internal website | rick@company.com | Standard | | | resolved | netop | 10 years ago | 8 years ago |
| 52 | access to CRM website | rick@company.com | Standard | | Rose_checkpoint | resolved | netop | 10 years ago | 6 months ago |
| 53 | I need to be able to send email | rick@company.com | Standard | | | resolved | netop | 10 years ago | 8 years ago |
| 54 | access to internal website | rick@company.com | Basic-With-ActiveChange-for-CKP | | | resolved | netop | 10 years ago | 6 months ago |
| 55 | Please allow RPC :-) | | | | Rose_checkpoint | resolved | netop | 10 years ago | 8 years ago |
| 56 | access to internal CRM website | rick@company.com | Basic-With-ActiveChange-for-CKP | | Rose_checkpoint | pending match | Not Assigned | 10 years ago | 4 years ago |
| 57 | access to intranet | rick@company.com | Basic-With-ActiveChange-for-CKP | | | resolved | netop | 10 years ago | 4 years ago |

Do one of the following:

- **To sort your results**, click the column heading that you want to sort by. Click the heading again to reverse the sort order.
- **To view a specific change request**, click the ID number or subject.

For more details, see Simple Search Results Columns.

### Simple Search Results Columns

Depending on your system configuration, your search results may include any of the following columns:

| | |
|---|---|
| **Id** | The change request ID number. |
| **Subject** | The change request subject. |
| **Requestor** | The requestors' email addresses. |

| | |
|---|---|
| **Workflow** | The change request's workflow.<br>For more details, see Request templates and workflows. |
| **Device Name** | The device for which this change request is relevant.<br>**Tip:** This field also includes cloud devices. For more details, see Amazon Web Services and Microsoft Azure "Devices". |
| **Status** | The change request's current status. |
| **Owner** | The change request's owner. |
| **Priority** | The change request's priority. |
| **Created** | The amount of time that has elapsed since the change request was created. |
| **Last Updated** | The amount of time that has elapsed since the change request was last updated. |

### FireFlow simple search process

FireFlow processes your query in the following order:

1. If your query contains a number, FireFlow checks whether any change request ID numbers match your query.
2. FireFlow checks whether your query starts with **fulltext**. If so, then FireFlow searches the full history of all change requests.
3. If your query contains an **@**, FireFlow checks whether any requestors' email addresses match your query.
4. FireFlow checks whether any **statuses** match your query.
5. FireFlow checks whether any **queues** match your query.
6. FireFlow checks whether any **owner names** match your query.
7. FireFlow checks whether any change requests' **Subject** fields match your query.

## Search by rule

This procedure describes how to search for all traffic change requests whose requested change intersects with a specific device rule.

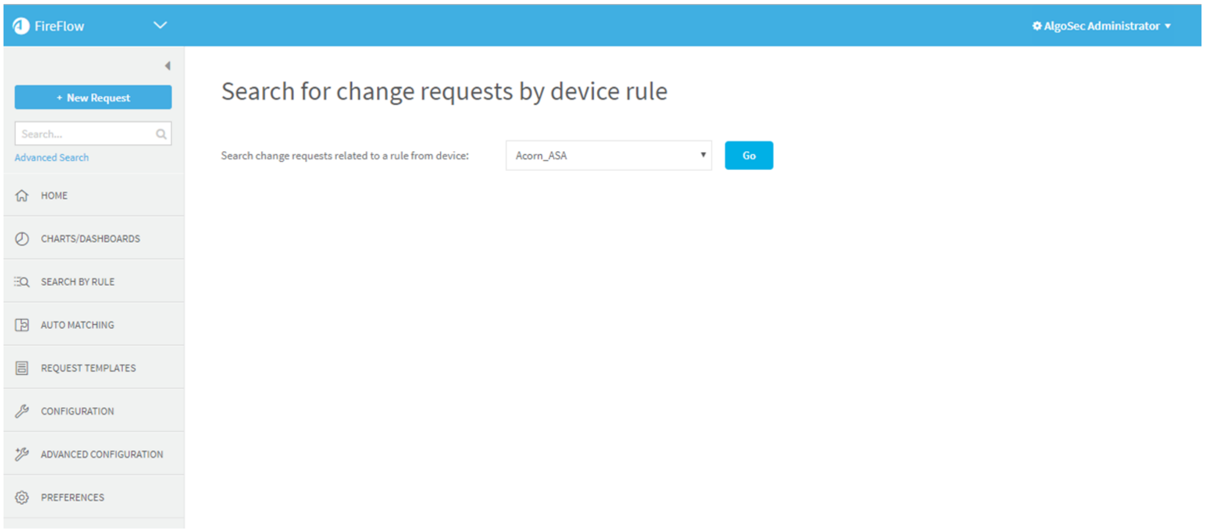
> **Note:** This feature supports new change requests created in FireFlow v6.0 and above. Change requests created in earlier versions are only partially supported and may not be returned in the search results.

> **Note:** This procedure can also be performed from within AFA reports.

### Do the following:

1. In the main menu, click **Search By Rule**.

   The **Search for change requests by device rule** page is displayed.

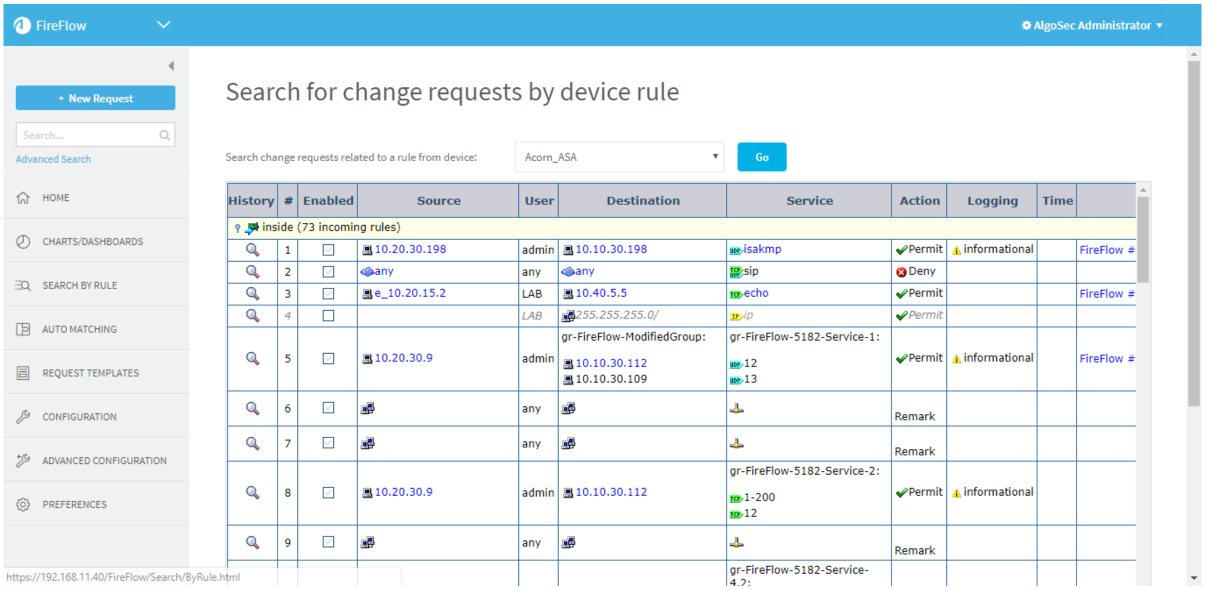


Search for change requests by device rule

Search change requests related to a rule from device: Acorn_ASA

2. Select the desired device from the drop-down list and click **Go**.

   The **Search for change requests by device rule** page appears displaying all rules and objects for the device.



Search for change requests by device rule

Search change requests related to a rule from device: Acorn_ASA ▾ Go

| History | # | Enabled | Source | User | Destination | Service | Action | Logging | Time | |
|---|---|---|---|---|---|---|---|---|---|---|
| inside (73 incoming rules) | | | | | | | | | | |
| 🔍 | 1 | ☑ | 10.20.30.198 | admin | 10.10.30.198 | isakmp | ✓Permit | ⚠ informational | | FireFlow # |
| 🔍 | 2 | ☑ | any | any | any | sip | ✖ Deny | | | |
| 🔍 | 3 | ☑ | e_10.20.15.2 | LAB | 10.40.5.5 | echo | ✓Permit | | | FireFlow # |
| 🔍 | 4 | □ | | LAB | 255.255.255.0/ | ip | ✓Permit | | | |
| 🔍 | 5 | ☑ | 10.20.30.9 | admin | gr-FireFlow-ModifiedGroup:<br>10.10.30.112<br>10.10.30.109 | gr-FireFlow-5182-Service-1:<br>12<br>13 | ✓Permit | ⚠ informational | | FireFlow # |
| 🔍 | 6 | ☑ | | any | | | Remark | | | |
| 🔍 | 7 | ☑ | | any | | | Remark | | | |
| 🔍 | 8 | ☑ | 10.20.30.9 | admin | 10.10.30.112 | gr-FireFlow-5182-Service-2:<br>1-200<br>12 | ✓Permit | ⚠ informational | | |
| 🔍 | 9 | ☑ | | any | | | Remark | | | |
| | | | | | | gr-FireFlow-5182-Service-4.2: | | | | |

To view all change requests related to a specific rule, in the **Policies** table, next to the desired rule, click 🔍.

3. The change requests related to the rule are displayed.

   **Note:** The search results include change requests that did not require policy changes (those that were marked as "Already Works").

   **Note:** If you selected a Check Point or Juniper NSM device, change requests are displayed for all devices that are installed with the same policy as the selected device.

## Define an advanced search

This procedure describes how to define an advanced search for FireFlow change requests.

**Tip:** Alternately, perform a simple search. For details, see Perform a simple search.

## Do the following:

1. In the **Query Builder** page's **Add Criteria** area, specify the search criteria.

   Do the following:

   a. In the **Aggregator** field, choose the aggregator to use between search criteria.

   b. To search according to criteria related to the device, the requested change, the planned change, and risk check results, do the following:

      i. In the **Queue** row, select **Firewalls**.

      ii. Click **Add these terms**.

      Additional rows appear in the **Add Criteria** area.

   c. For each row in the **Add Criteria** area, define your search criteria by selecting change request properties and operators and entering a value for each property.

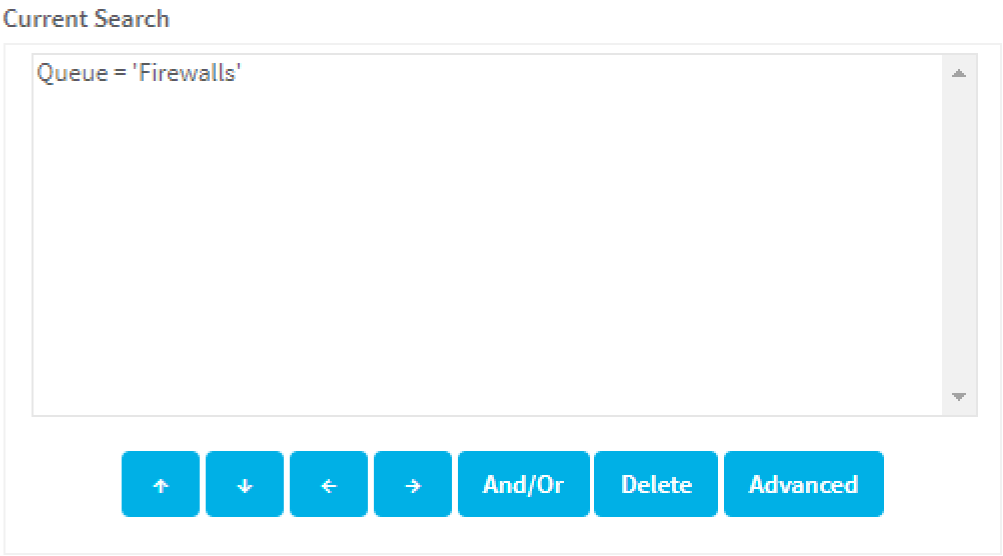
      For example: **Owner is johnS (John Smith)**

      For more details, see:

      - Advanced search fields
      - Advanced search operators

   d. Click **Add these terms**.

      The specified criterion is added to the **Current Search** area. The selected aggregator is used between the criteria.


Current Search

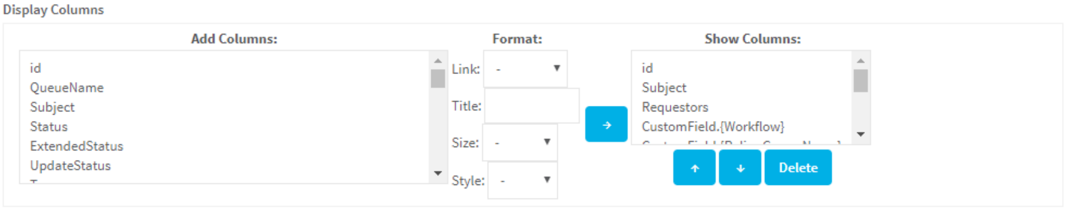
Queue = 'Firewalls'

Use the buttons in this dialog to do any of the following:

- **Move** a selected criterion up ↑ or down ↓
- **Increase** → or ← **decrease** indentation for a selected criterion
- **Toggle** the selected aggregator (and/or)
- **Delete** a selected criterion
- Perform an **advanced** query edit. For more details, see Advanced query edits.

2. Specify how the search results should appear, by doing the following:

   a. Scroll to the **Display Columns** area.


Display Columns

Add Columns:

id
QueueName
Subject
Status
ExtendedStatus
UpdateStatus

Format:

Link: -
Title:
Size: -
Style: -

Show Columns:

id
Subject
Requestors
CustomField.{Workflow}

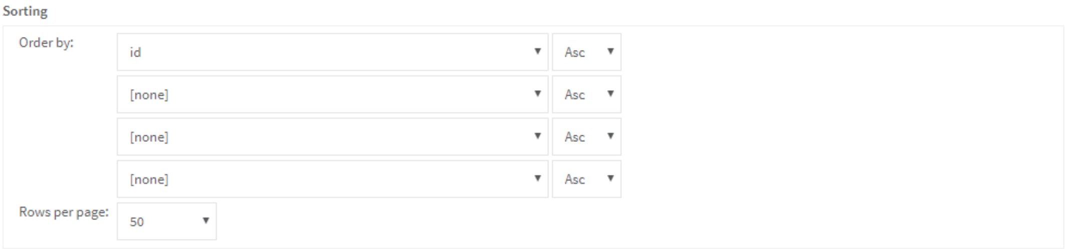
   b. For each column you want to appear in the search results, do the following:

    i. In the **Add Columns** box, select a column you want to appear.
    ii. Complete the fields in the **Format** area. For details, see [Advanced search column format fields]().
    iii. 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).

    iv. To move the column up or down in the box, select the column and click the ↑ or ↓ buttons.
    v. To delete the column, select it and click **Delete**.

  c. Scroll to the **Sorting** area.



Sorting

| | | |
|---|---|---|
| Order by: | id ▾ | Asc ▾ |
| | [none] ▾ | Asc ▾ |
| | [none] ▾ | Asc ▾ |
| | [none] ▾ | Asc ▾ |
| Rows per page: | 50 ▾ | |

  d. In the **Order by** area, specify the default sort order of the search results as follows:

    i. In the left-side fields, select one or more columns according to which the search results should be sorted.
    ii. In the right-side fields, select the sort order to use for each specified column: ascending (**Asc**) or descending (**Desc**).

  e. In the **Rows per page** field, select the number of search result rows that should appear in each page.

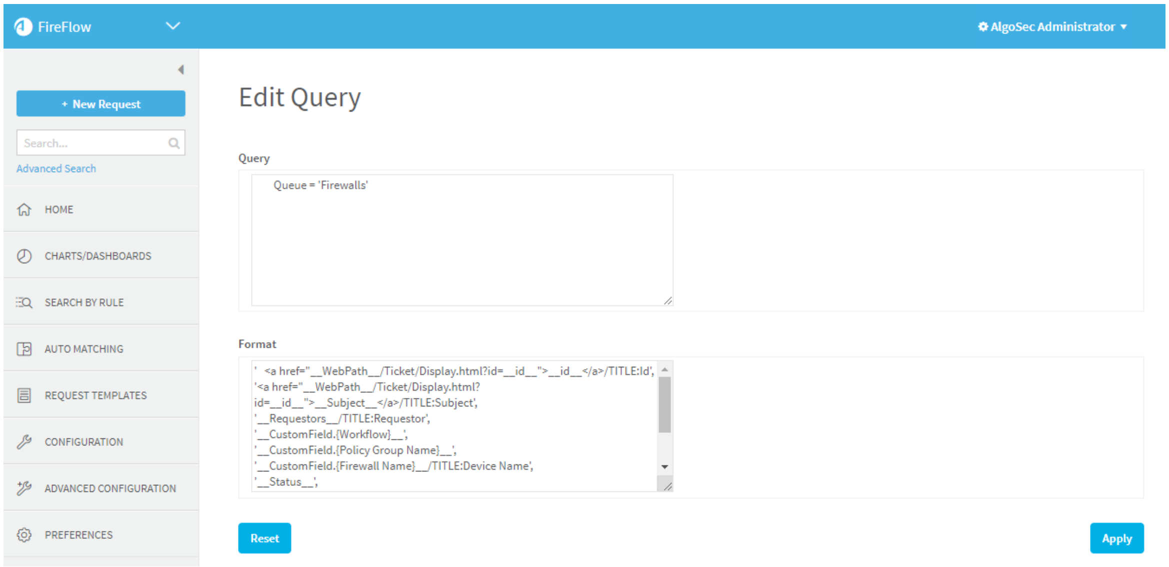
3. To remove all of your changes and define a new search, in the main menu, click **New Search**.

### Advanced query edits

To perform an advanced edit of the defined search, do the following:

1. In the **Current Search** area, click **Advanced**.

   The **Edit Query** page is displayed.



Edit Query

Query

```
Queue = 'Firewalls'
```

Format

```
'   <a href="__WebPath__/Ticket/Display.html?id=__id__">__id__</a>/TITLE:Id',
'<a href="__WebPath__/Ticket/Display.html?
id=__id__">__Subject__</a>/TITLE:Subject',
'__Requestors__/TITLE:Requestor',
'__CustomField.{Workflow}__',
'__CustomField.{Policy Group Name}__',
'__CustomField.{Firewall Name}__/TITLE:Device Name',
'__Status__',
```

2. In the **Query** text box, modify the search criteria as desired.
3. In the **Format** text box, modify the displayed columns as desired.
4. To remove your changes, click **Reset**.
5. Click **Apply**.

   The **Query Builder** page reappears with your changes.

### Advanced search fields

The following fields are available for advanced search queries in FireFlow:

| | |
|---|---|
| **id** | Type the change request ID number. |
| **Subject** | Type the change request subject. |

| | |
|---|---|
| **Content** | Type text that appears in the original change request description or in a comment or reply added to the change request. |
| **Content-Type** | Type the file type of an attachment attached to the change request. |
| **Filename** | Type the filename of an attachment for the change request. |
| **Status** | Select the change request status. |
| **Owner** | Select the user who is the current change request owner. |
| **Creator** | Select the user who is the change request creator. |
| **Last updated by** | Select the user who last updated the change request. |
| **Requestor EmailAddress** | Type the requestor's email address. |
| **Requestor Name** | Type the requestor's username. |
| **Requestor Full Name** | Type the requestor's full name. |
| **Requestor Nickname** | Type the requestor's nickname. |
| **Requestor Organization** | Type the requestor's organization. |
| **Requestor Address1** | Type the requestor's primary mailing address. |
| **Requestor Address2** | Type the requestor's secondary mailing address. |
| **Requestor WorkPhone** | Type the requestor's office telephone number. |
| **Requestor HomePhone** | Type the requestor's home telephone number. |
| **Requestor MobilePhone** | Type the requestor's mobile telephone number. |

| | |
|---|---|
| **Requestor PagerPhone** | Type the requestor's pager telephone number. |
| **Requestor id** | Type the requestor's ID. |
| **Cc EmailAddress** | Type the email address of a user who receives copies of email messages for the change request. |
| **Cc Name** | Type the username of a user who receives copies of email messages for the change request. |
| **Cc Full Name** | Type the full name of a user who receives copies of email messages for the change request. |
| **Cc Nickname** | Type the nickname of a user who receives copies of email messages for the change request. |
| **Cc Organization** | Type the organization of a user who receives copies of email messages for the change request. |
| **Cc Address1** | Type the primary mailing address of a user who receives copies of email messages for the change request. |
| **Cc Address2** | Type the secondary mailing address of a user who receives copies of email messages for the change request. |
| **Cc WorkPhone** | Type the office telephone number of a user who receives copies of email messages for the change request. |
| **Cc HomePhone** | Type the home telephone number of a user who receives copies of email messages for the change request. |
| **Cc MobilePhone** | Type the mobile telephone number of a user who receives copies of email messages for the change request. |
| **Cc PagerPhone** | Type the pager telephone number of a user who receives copies of email messages for the change request. |
| **Cc id** | Type the ID of a user who receives copies of email messages for the change request. |
| **Owner EmailAddress** | Type the owner's email address. |
| **Owner Name** | Type the owner's username. |

| | |
|---|---|
| **Owner Full Name** | Type the owner's full name. |
| **Owner Nickname** | Type the owner's nickname. |
| **Owner Organization** | Type the owner's organization. |
| **Owner Address1** | Type the owner's primary mailing address. |
| **Owner Address2** | Type the owner's secondary mailing address. |
| **Owner WorkPhone** | Type the owner's office telephone number. |
| **Owner HomePhone** | Type the owner's home telephone number. |
| **Owner MobilePhone** | Type the owner's mobile telephone number. |
| **Owner PagerPhone** | Type the owner's  pager telephone number. |
| **Owner id** | Type the owner's ID. |
| **Created** | Specify the date on which the change request was created, either by typing the date in YYYY-MM-DD format, or by clicking **Choose a date** and selecting the date in the calendar. |
| **Resolved** | Specify the date on which the change request was resolved, either by typing the date in YYYY-MM-DD format, or by clicking **Choose a date** and selecting the date in the calendar. |
| **Last Updated** | Specify the date on which the change request was last updated, either by typing the date in YYYY-MM-DD format, or by clicking **Choose a date** and selecting the date in the calendar. |
| **Due** | Specify the change request's due date, either by typing the date in YYYY-MM-DD format, or by clicking **Choose a date** and selecting the date in the calendar. |
| **Priority** | Type the change request's current priority. |
| **Initial Priority** | Type the change request's priority at the start of its lifecycle. |

| | |
|---|---|
| **Final Priority** | Type the change request's priority at the end of its lifecycle. |
| **RefersTo** | Type the ID numbers of change requests to which this change request refers, separated by spaces. |
| **ReferredToBy** | Type the ID numbers of change requests that refer to this change request, separated by spaces. |
| **SLA Name** | Type the name of the SLO currently used for the change request. |
| **SLA Due Date** | Specify the due date of the SLO currently used for this change request, by doing one of the following:<br>• Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>• Type the desired date in the field provided. You can use most relative and absolute formats, for example `yyyy-mm-dd`, `mm/dd/yyyy`, `Mon dd yyyy`, “next week”, and “now + 3 days”. |
| **SLA Status** | Select the status of the SLO currently used for this change request. |
| **SLA Elapsed Time** | Specify the total amount of elapsed time for this change request, as specified in the SLA, by typing the amount of time and then selecting the units of time. |
| **Expires** | Specify the date on which this change request will expire, by doing one of the following:<br>• Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>• Type the desired date in the field provided. You can use most relative and absolute formats, for example `yyyy-mm-dd`, `mm/dd/yyyy`, `Mon dd yyyy`, “next week”, and “now + 3 days”. |

| | |
|---|---|
| **Requested Source** | Type the IP address, IP range, network, device object, or DNS name of the connection source, as specified in the original request. |
| **Requested Action Type** | Type the action used in the change request's first row of traffic. This can be any of the following:<br>- **Allow**<br>- **Drop**<br>- **Mixed** |
| **Requested Destination** | Type the IP address, IP range, network, device object, or DNS name of the connection destination, as specified in the original request. |
| **Requested Service** | Type the device service or port for the connection, as specified in the original request. |
| **Requested Action** | Type the device action to perform for the connection, as specified in the original request. |
| **Requested Source NAT** | Type the source NAT value to which the connection's source should be translated, as specified in the original request. |
| **Ticket Template Name** | Type the name of the change request's template. |
| **Ticket Template ID** | Type the ID of the change request's template. |
| **Requested Destination NAT** | Type the destination NAT value to which the connection's destination should be translated, as specified in the original request. |
| **Requested Port Translation** | Type the port value to which the connection's port should be translated, as specified in the original request. |
| **Workflow** | Select the workflow assigned to the change request. |
| **Owning Role** | Type the user role that currently owns the change request. |
| **Requested NAT Type** | Enter the type of NAT (**Static** or **Dynamic**), as specified in the original request. |

| | |
|---|---|
| **Additional Responsible Roles** | Specify the user roles, other than the owning role, that are responsible for handling the change request in its current lifecycle stage. Select any of the following:<br>• A role name.<br>• **__USER_GROUPS__**. All roles of which you are a member.<br>To select multiple roles, hold down the Ctrl key while clicking on the desired roles. |
| **Pending Responsible Roles** | Specify the roles that are responsible for handling the change request in its current lifecycle stage, but which have not yet approved the change request. Select any of the following:<br>• A role name.<br>• **__USER_GROUPS__**. All roles of which you are a member.<br>To select multiple roles, hold down the Ctrl key while clicking on the desired roles. |
| **CMS ticket id** | Type the ID number of a related change request in an external change management system that is integrated with FireFlow. |
| **Firewall Name** | Type the name of the device. |
| **Firewall IP Address** | Type the IP address of the device. |
| **Firewall Brand** | Type the name of the device vendor. |
| **Firewall Management Server** | Type the name of the device management server. |
| **Firewall Policy** | Type the name of the device security policy. |
| **Firewall Last Report** | Type the name of last report generated for the device. |
| **Firewall Last Report Date** | Type the date and time at which the last report for this device was generated. |

| | |
|---|---|
| **Change Description** | Type the change description. |
| **Requested UserGroup** | Type the user or user group that should be allowed/denied access to a URL, as specified during the Request stage. |
| **Change UserGroup** | Type the user or user group that should be allowed/denied access to a URL, as planned during the Plan stage. |
| **Requested URL** | Type the URL that should be allowed/blocked, as specified during the Request stage. |
| **Change URL** | Type the URL that should be allowed/blocked, as planned during the Plan stage. |
| **Requested Category** | Type the URL's Web filtering category, as specified during the Request stage. |
| **Change Category** | Type the URL's Web filtering category, as planned during the Plan stage. |
| **Requested Web Action** | Select the device Web filtering action to perform for the connection, as specified during the Request stage. |
| **Change Web Action** | Select the device Web filtering action to perform for the connection, as planed during the Plan stage. |
| **Organization Methodology** | Select the organizational methodology to be used for implementing a Web filtering change request, as specified during the Approve stage. |
| **Category to Update** | Type the Web filtering category that should be updated, in order to allow/block the URL. |
| **Change Source** | Type the IP address, IP range, network, device object, or DNS name of the connection source, as planned during the Plan stage. |
| **Requested Object Action Type** | Type the device action to perform for the object, as specified during the Request stage. |
| **Change Object Action Type** | Type the device action to perform for the object, as planned during the Plan stage. |

| | |
|---|---|
| **Change Destination** | Type the IP address, IP range, network, device object, or DNS name of the connection destination, as planned during the Plan stage. |
| **Change Service** | Type the device service or port for the connection, as planned during the Plan stage. |
| **Change Action** | Type the device action to perform for the connection, as planned during the Plan stage. |
| **Change Source NAT** | Type the source NAT value to which the connection's source should be translated, as planned during the Plan stage. |
| **Change Destination NAT** | Type the destination NAT value to which the connection's destination should be translated, as planned during the Plan stage. |
| **Change Port Translation** | Type the port value to which the connection's port should be translated, as planned during the Plan stage. |
| **Change NAT Type** | Type the type of NAT (**Static** or **Dynamic**), as planned during the Plan stage. |
| **Change Implementation Notes** | Type words that appear in the change request's implementation notes, if the change request has completed the Implement stage. |
| **Request Risk Check Result** | Type the number and/or and severity of risks that implementation of the planned change would entail. |
| **Initial Plan Result** | Type the results of initial planning. |
| **Form Type** | Select the type of request used for the change request (**Traffic Change**, **Object Change**, or **Generic Change**). |
| **Change Validation Result** | Type the results of change validation. |
| **Risks Number** | Type the number of risks detected for the planned change, if the change request has completed the risk check in the Approve stage. |

| | |
|---|---|
| **Risks Details** | Type details about the risks detected for the planned change, if the change request has completed the risk check in the Approve stage. |
| **Translated Source** | Select the change request's source, as translated to IP addresses. |
| **Requested Object Action** | Select the requested action for an object change request (**AddIPsToObject** / **RemoveIPsFromObject** / **NewObject** / **DeleteObject**). |
| **Translated Destination** | Select the change request's destination, as translated to IP addresses. |
| **Change Object Action** | Select the action for an object change request, as specified during the Plan stage (**AddIPsToObject** / **RemoveIPsFromObject** / **NewObject** / **DeleteObject**). |
| **Translated Service** | Select the change request's service, as translated to ports. |
| **Requested Object Name** | Type an object's name, as specified in the original object change request. |
| **Automatically Implemented** | Select whether the requested change should be automatically implemented. |
| **Change Object Name** | Type an object's name, as specified for an object change request in the Plan stage. |
| **Already Works Firewalls** | Type the names of devices on which the requested change already works. |
| **Requested IPs To Add** | Type the IP addresses to add to an object, as specified in the original object change request. |
| **Change IPs To Add** | Type the IP addresses to add to an object, as specified for an object change request in the Plan stage. |
| **Requested IPs To Remove** | Type the IP addresses to remove from an object, as specified in the original object change request. |
| **Change IPs To Remove** | Type the IP addresses to remove from an object, as specified for an object change request in the Plan stage. |

| | |
|---|---|
| **Requested Object Scope** | Select the object scope, as specified in the original object change request. |
| **Change Object Scope** | Select the object scope, as specified for an object change request in the Plan stage. |
| **Is Work Order Editable** | Specify whether the work order is editable. |
| **Change Full Data** | Specify the change that has been matched to the change request's full data. |
| **Is Active Change Applicable** | Specify whether ActiveChange can be used to implement the requested change. |
| **Object Change Validation Result** | Type the results of object change validation. |
| **Create tickets from attachment** | Select whether the change request was created from a file. |
| **Affected Rules Result** | Type the device rules that are affected by a suggested object change request. |
| **Firewall Provider-1** | Type the name or IP address of the MDSM managing the device.<br>This field is relevant for Check Point devices only. |
| **Rule Removal Identifier** | Type the identifier of a rule removal request. |
| **Rule Removal Display Id** | Type the display ID of a rule to be removed via a rule removal request. |
| **Rule Removal Snippet** | Type a snippet of a rule to be removed via a rule removal request. |
| **Rule Removal Line Num** | Type the line number of a rule to be removed via a rule removal request. |
| **Rule Removal Rule Action** | Type the action of a rule to be removed via a rule removal request. |

| | |
|---|---|
| **Rule Removal Related Query** | Type a query related to a rule to be removed via a rule removal request. |
| **Rule Removal Related Tickets** | Type the ID numbers of change requests related to a rule removal request. |
| **Rule Removal Related Tickets Requestors** | Type the names of requestors who submitted change requests related to a rule removal request. |
| **Rule Removal Users to Notify** | Type the names of users to notify for a rule removal request. |
| **Requested Rule Removal Action** | Select a rule removal request's action. |
| **Change Rule Removal Action** | Select the action to which a rule removal request's original action was changed. |
| **Rule Removal Hit Count** | Type the number of times a rule to be removed via a rule removal request was used over a certain period of time. If desired, the period of time can be specified in the **Rule Removal Hit Count Duration** field. |
| **Rule Removal Hit Count Duration** | Type the number of days over which a rule to be removed via a rule removal request was used to block/allow connections. |
| **Rule Removal Last Used on** | Type the date on which a rule to be removed via a rule removal request was last used. |
| **Rule Removal First Log Date** | Type the date of oldest log that was consulted to obtain usage information about a rule to be removed via a rule removal request. |
| **Rule Removal Last Log Date** | Type the date of newest log that was consulted to obtain usage information about a rule to be removed via a rule removal request. |
| **Rule Removal Usage Info** | Type information about the usage of a rule that is to be removed. |

| | |
|---|---|
| **Rule Removal Ticket Origin** | Type the origin of a rule removal request. This can be any of the following:<br>• **Unused Rule**<br>• **Covered Rule**<br>• **Special Case Rule**<br>This field is relevant for change requests originating in AlgoSec Firewall Analyzer only. |
| **Rule Removal Show Related Tickets** | Type the IDs of change requests are related to a rule that is to be removed. |
| **Risk Level** | Type the change request's highest risk level, as determined by a risk check. |
| **Recertification Related Tickets Calculation Date** | Type the date on which related change requests will be recertified. |
| **Recertification Candidate Devices** | Type the names of devices for which change requests that are candidates for recertification were issued. |
| **Recertified Traffic Ticket** | Type the name of the traffic change request that is being recertified. |
| **Rule Removal Notify Not responded** | Type the names of related change requestors that have not yet responded regarding a rule removal request. |
| **Recertification Status** | Select the status of a recertification request. This can be any of the following:<br>• **Stand by:** Standing by for the change requestors' responses. This status continues until the responses are received, or the due date passes.<br>• **In process:** The change request is open.<br>• **Resolved:** The change request has been resolved. |
| **Application Default Services** | Type the protocol/port that the application uses by default (for example, tcp/80). |

| | |
|---|---|
| **Initial Plan Result For Allow Traffic** | Type the results of initial planning for a change request's Allow traffic. |
| **Initial Plan Result For Drop Traffic** | Type the results of initial planning for a change request's Drop traffic. |
| **Firewall Name for Traffic to be Allowed** | Type the name of the device for which traffic should be allowed, according to a change request. |
| **Firewall Name for Traffic to be Dropped** | Type the name of the device for which traffic should be blocked, according to a change request. |
| **Implementation Recommendations** | Type the Implementation Recommendations generated for a change request. |

### Advanced search operators

Use any of the following operators when performing an advanced search in FireFlow:

| Operator | Description |
|---|---|
| **less than** | Search for change requests in which the property in the left column is less than the number in the right column.<br>For example, if the criterion is **Id less than 7**, the search will return all change requests with ID numbers less than 7. |
| **equal to** | Search for change requests in which the property in the left column is equal to the number in the right column.<br>For example, if the criterion is **Id equal to 7**, the search will return the change request with ID number 7. |
| **greater than** | Search for change requests in which the property in the left column is greater than the number in the right column.<br>For example, if the criterion is **Id greater than 7**, the search will return all change requests with ID numbers greater than 7. |

| Operator | Description |
|---|---|
| **not equal to** | Search for change requests in which the property in the left column is not equal to the number in the right column.<br>For example, if the criterion is **Id not equal to 7**, the search will return all change requests with ID numbers other than 7. |
| **matches** | Search for change requests in which the property in the left column contains the value in the right column.<br>For example, if the criterion is **Subject matches Allow MS-RPC**, the search will return all change requests whose subject contains "Allow MS-RPC". |
| **doesn't match** | Search for change requests in which the property in the left column does not contain the value in the right column.<br>For example, if the criterion is **Subject matches Allow MS-RPC**, the search will return all change requests whose subjects do not contain "Allow MS-RPC". |
| **is** | Search for change requests in which the property in the left column matches exactly the value in the right column.<br>For example, if the criterion is **Status is resolved**, the search will return all change requests with the status "resolved". |
| **isn't** | Search for change requests in which the property in the left column does not match exactly the value in the right column.<br>For example, if the criterion is **Status isn't resolved**, the search will return all change requests with a status other than "resolved". |
| **before** | Search for change requests in which the property in the left column occurs before the date in the right column.<br>For example, if the criterion is **Created Before 2008-12-05**, the search will return all change requests that were created before December 5, 2008. |
| **on** | Search for change requests in which the property in the left column occurs on the date in the right column.<br>For example, if the criterion is **Created On 2008-12-05**, the search will return all change requests that were created on December 5, 2008. |

| Operator | Description |
|---|---|
| **after** | Search for change requests in which the property in the left column occurs after the date in the right column.<br>For example, if the criterion is **Created After 2008-12-05**, the search will return all change requests that were created after December 5, 2008. |

### Advanced search column format fields

Use the following fields to determine how advanced search results are displayed:

| | |
|---|---|
| **Link** | Specify whether items in the column should be linked, by selecting one of the following:<br>• **-**. Items in the column are not linked.<br>• **Take:** Clicking on an item in the column assigns you the relevant change request.<br>• **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:<br>• **-**. Items in the column appear in medium-sized text.<br>• **Small:** Items in the column appear in small-sized text.<br>• **Large:** Items in the column appear in large-sized text. |
| **Style** | Specify the font style of items in the column, by selecting one of the following:<br>• **-**. Items in the column appear in normal font.<br>• **Bold:** Items in the column appear in bold font.<br>• **Italic:** Items in the column appear in italicized font. |

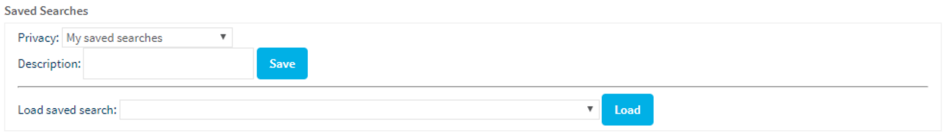
## Save an advanced search

Save an advanced search to load and run the same search again, or regularly display the search results on your FireFlow home page.

For more details, see Load a saved search.

## Do the following:

1. In the **Query Builder** page, define a search. For details, see Define an advanced search.
2. Scroll to the **Saved Searches** area.



Saved Searches

Privacy: My saved searches

Description:

Load saved search:

3. In the **Privacy** drop-down list, specify who should be allowed to load this search:

| | |
|---|---|
| **My saved searches** | Make this search available to yourself only. |
| **Admin's saved searches** | Make this search available to all administrators |
| **Controller's saved searches** | Make this search available to all controllers |
| **Network's saved searches** | Make this search available to all network operations users |
| **Security saved searches** | Make this search available to all information security users |
| **FireFlow's saved searches** | Make this search available to all FireFlow users. |

4. In the **Description** field, type a name for the search.
5. Click **Save**.

The search is saved and will be available to the specified user role for loading.

## Load a saved search

This procedure describes how to load a saved advanced search.

For more details, see Define an advanced search and Save an advanced search.

### Do the following:

1. In the **Query Builder** page, reveal the **Saved Searches** area.

   The **Saved Searches** area appears.

2. In the **Load saved search** drop-down list, select the search you want to load.
3. Click **Load**.

The search is loaded.

## Copy a saved search

If you want to create and save a new advanced search that is similar to an existing saved search, you can copy the saved search.

### Do the following:

1. Load the search you want to copy. For details, see Load a saved search.
2. Click **Save as New**.

   The **Description** field displays the name of the original search, followed by the word "copy".

   For example, "Resolved Change requests copy"

3. In the **Description** field, modify the search name as desired.
4. Modify the search criteria as desired. For details, see Define an advanced search.
5. Click **Update**.

The search is saved with the same privacy settings as the original search, and will be available to that user role for loading.

## Delete a saved search

Delete any advanced search that you've saved in FireFlow.

## Do the following:

1. Load the search you want to delete. For details, see Load a saved search.
2. Click **Delete**.

The search is deleted.

## Advanced search example

The following example describes a sample use case for an advanced search in FireFlow.

**Debbie**, a company employee, wants to know the status of a specific change request.

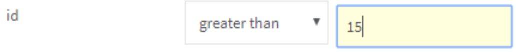
She calls **Ned**, a FireFlow administrator for help.

- Debbie cannot remember the change request ID number, aside that it was above **15**.
- Ned remembers handling the change request himself, and is certain that he did not reject it, but also does not have the specific ID.

Debbie has since hung up, but now Ned is concerned that he missed the expiration date and wants to be sure to handle it.

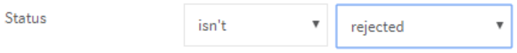
Ned does the following:

1. In FireFlow, he clicks **Advanced Search** in the main menu on the left.
2. On the **Query Builder** page, in the **Add Criteria** area, Ned defines the search query as follows:
   - Ned selects the **AND** aggregator
   - In the **ID** row, Ned selects the **greater than** operator, and enters a value of **15**.



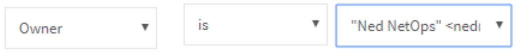
id greater than ▾ 15

   - In the **Status** row, Ned selects the **isn't** operator and then selects the **rejected** value from the dropdown on the right.



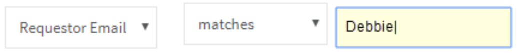
Status isn't rejected

- In the **Owner** row, Ned selects the is operator and enters **Ned** as the value.



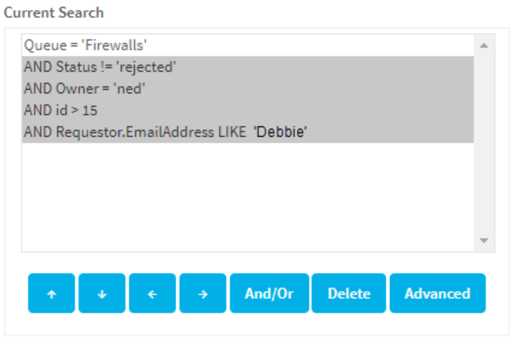
Owner is "Ned NetOps" <nedı

- In the **Requestor EmailAddress** row, Ned switches the field to **Requestor RealName**, selects the **matches** operator, and then enters **Debbie** as the value.



Requestor Email matches Debbie|

3. Ned clicks **Add these terms** to add the specified criteria to the **Current search** area.



Current Search

```
Queue = 'Firewalls'
AND Status != 'rejected'
AND Owner = 'ned'
AND id > 15
AND Requestor.EmailAddress LIKE 'Debbie'
```

4. In the **Display columns** area, Ned does the following:

   a. Selects **Due** in the **Add Columns** box.

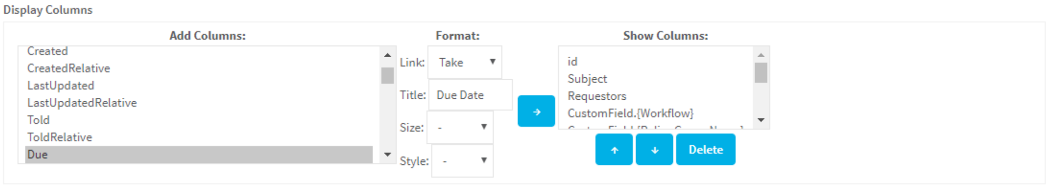
   b. Selects **Take** in the **Link** drop-down list.

   c. Enters **Due Date** in the **Title** field.

   d. Selects **Large** in the **Size** drop-down list.

   e. Selects **Bold** in the **Style** drop-down list.

   f. Clicks → to add the columns to the **Show Columns** box on the right.



Display Columns

Add Columns:

Created
CreatedRelative
LastUpdated
LastUpdatedRelative
Told
ToldRelative
Due

Format:

Link: Take
Title: Due Date
Size: -
Style: -

Show Columns:

id
Subject
Requestors
CustomField.{Workflow}

f. Ned clicks **Search** to start searching for Debbie's change request.

# Advanced change request edits

**Relevant for: Network operations, information security, and administrator users**

This topic describes how to perform advanced tasks with change requests.

## Assign change requests to users

By default, change requests are assigned to specific users, as configured for the template and workflow.

Manually assign a change request to a different user to make that user the owner instead.

> **Note:** This action is the equivalent of the user clicking **Take** in the change request.

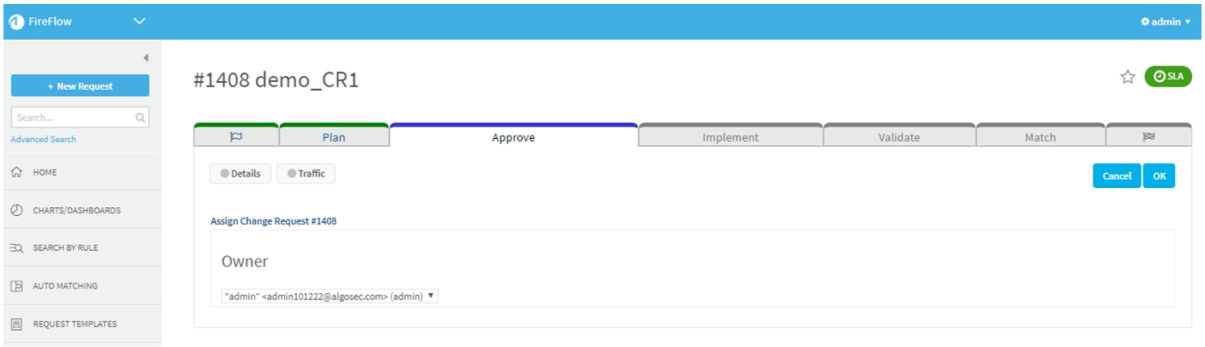
### Do the following:

1. View the change request. For details, see View change requests.

2. At the top of the workspace, click ≡ , and then click **Assign**.

   > **Note:** The list of options available in the drop-down list may be changed by an administrator, by editing a workflow's available actions.

   The **Assign Change Request** area appears.



#1408 demo_CR1

Assign Change Request #1408

Owner

"admin" <admin101222@algosec.com> (admin)

3. In the **Owner** drop-down list, select the person who should be assigned as the change request's owner.
4. Click **OK**.

The change request is assigned to the selected user.

## Edit change requests

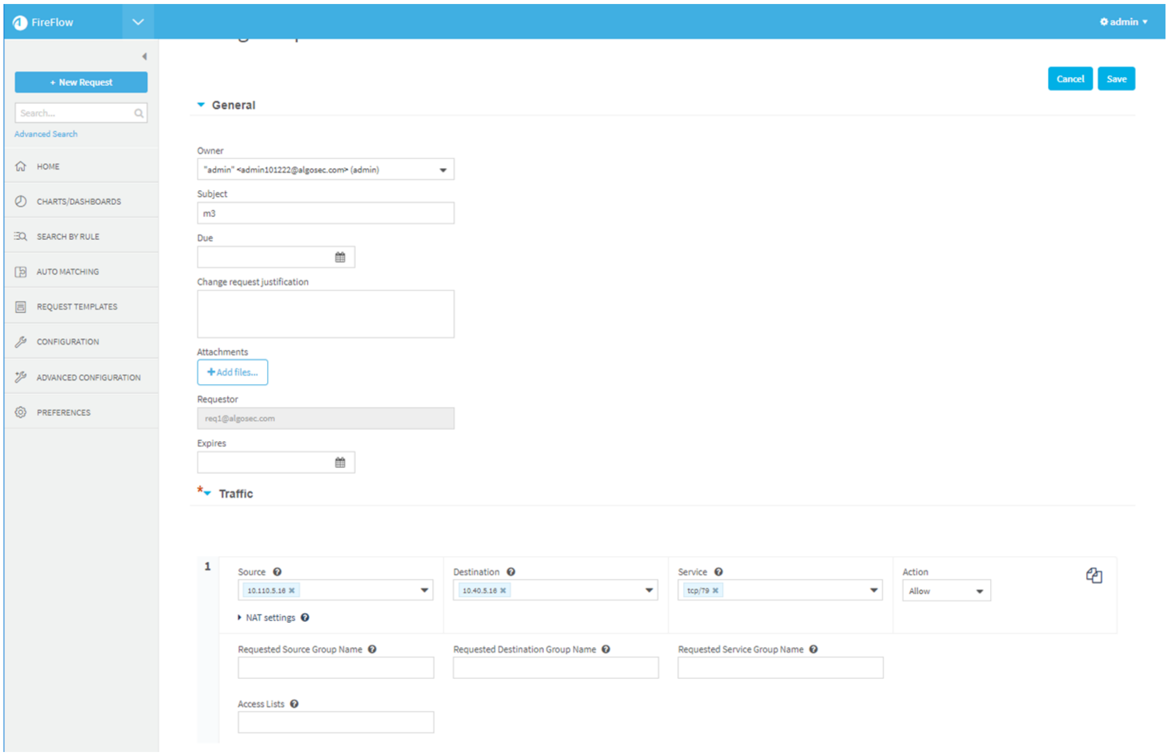
This procedure describes how to edit a change request, such as when you want to change a rule name, related devices or groups, or other details, depending on the type of request.

### Do the following:

1. View the change request. For details, see View change requests
2. Click ✎**Edit**.

   The change request appears with editable fields, depending on the request template you used.

   For example:



General

Owner: "admin" <admin101222@algosec.com> (admin)

Subject: m3

Due

Change request justification

Attachments

Requestor: req1@algosec.com

Expires

Traffic

1

Source: 10.110.5.16

NAT settings

Destination: 10.40.5.16

Service: tcp/79

Action: Allow

Requested Source Group Name

Requested Destination Group Name

Requested Service Group Name

Access Lists

3. Edit the fields as needed, and then click **Save Changes** or **OK**, depending on your request template.

   For more details, see Change request field references.

## Duplicate a change request

Duplicate a change request to create a new one with similar details to an existing request.

### Do the following:

1. View the change request you want to duplicate. For details, see View change requests.

2. At the top of the page, click ☰ , and then click **Duplicate**.

   **Note:** The list of option available in the drop-down list may be changed by an

> administrator, by editing a workflow's available actions.

A new window opens displaying the **Create a New Change Request** page.

The fields are filled in with the original change request's request details and subject. There is no owner assigned to the change request.

3. Modify the fields as needed. For details, see Change request field references.
4. Click **Next**.

The new change request is created.

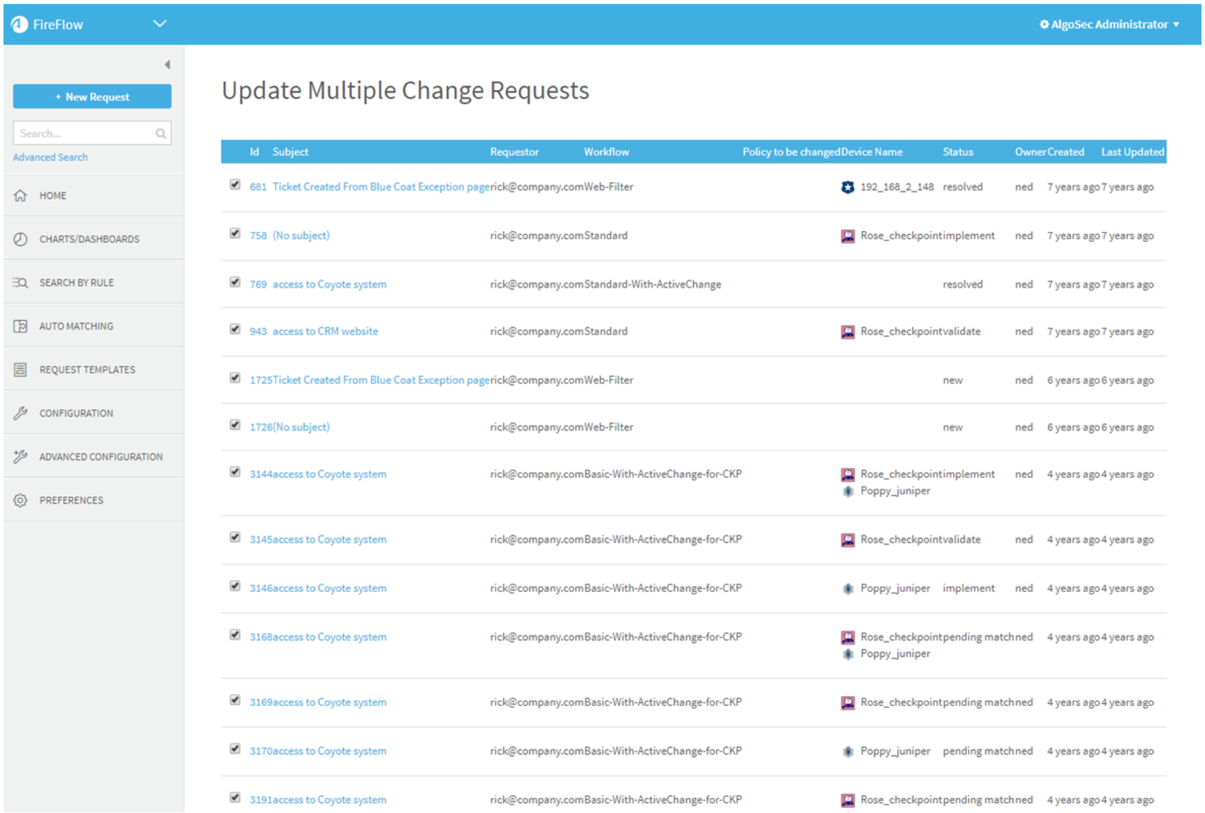
## Update multiple change requests

Update multiple change requests simultaneously, such as when you want to change the owner on several requests.

### Do the following:

1. Perform an advanced search for the change requests you want to update. For details, see Search for change requests.
2. Click **Update Multiple Change Requests**.

   The **Update Multiple Change Requests** page is displayed.



Update Multiple Change Requests

| | Id | Subject | Requestor | Workflow | Policy to be changed | Device Name | Status | Owner | Created | Last Updated |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | 681 | Ticket Created From Blue Coat Exception page | rick@company.com | Web-Filter | | 192_168_2_148 | resolved | ned | 7 years ago | 7 years ago |
| ☑ | 758 | (No subject) | rick@company.com | Standard | | Rose_checkpoint | implement | ned | 7 years ago | 7 years ago |
| ☑ | 769 | access to Coyote system | rick@company.com | Standard-With-ActiveChange | | | resolved | ned | 7 years ago | 7 years ago |
| ☑ | 943 | access to CRM website | rick@company.com | Standard | | Rose_checkpoint | validate | ned | 7 years ago | 7 years ago |
| ☑ | 1725 | Ticket Created From Blue Coat Exception page | rick@company.com | Web-Filter | | | new | ned | 6 years ago | 6 years ago |
| ☑ | 1726 | (No subject) | rick@company.com | Web-Filter | | | new | ned | 6 years ago | 6 years ago |
| ☑ | 3144 | access to Coyote system | rick@company.com | Basic-With-ActiveChange-for-CKP | | Rose_checkpoint<br>Poppy_juniper | implement | ned | 4 years ago | 4 years ago |
| ☑ | 3145 | access to Coyote system | rick@company.com | Basic-With-ActiveChange-for-CKP | | Rose_checkpoint | validate | ned | 4 years ago | 4 years ago |
| ☑ | 3146 | access to Coyote system | rick@company.com | Basic-With-ActiveChange-for-CKP | | Poppy_juniper | implement | ned | 4 years ago | 4 years ago |
| ☑ | 3168 | access to Coyote system | rick@company.com | Basic-With-ActiveChange-for-CKP | | Rose_checkpoint<br>Poppy_juniper | pending match | ned | 4 years ago | 4 years ago |
| ☑ | 3169 | access to Coyote system | rick@company.com | Basic-With-ActiveChange-for-CKP | | Rose_checkpoint | pending match | ned | 4 years ago | 4 years ago |
| ☑ | 3170 | access to Coyote system | rick@company.com | Basic-With-ActiveChange-for-CKP | | Poppy_juniper | pending match | ned | 4 years ago | 4 years ago |
| ☑ | 3191 | access to Coyote system | rick@company.com | Basic-With-ActiveChange-for-CKP | | Rose_checkpoint | pending match | ned | 4 years ago | 4 years ago |

The search results appear at the top of the page.

3. In the search results, select the change requests you want to update, or click **Check All** to select all items shown.

4. Complete the rest of the fields and needed, and then click **Update**.

   All fields are optional.

### Update Multiple Change Requests

| | |
|---|---|
| **Make Owner** | Select the user to assign as the change requests' owner. |
| **Add Cc** | Type the email addresses to which the FireFlow system should send copies of all email messages regarding these change requests, separated by commas.<br>These email addresses will be added to the change requests' existing Cc list. |

| | |
|---|---|
| **Remove Cc** | Type the email addresses to which the FireFlow system should *no longer* send copies of email messages regarding these change requests, separated by commas.<br>These email addresses will be removed from the change requests' existing Cc list. |
| **Make subject** | Type the title that should be assigned to the change requests. |
| **Make priority** | Type a number indicating the change requests' priority, where 0 indicates lowest priority. |
| **Make Status** | Select a status to assign the change requests. |
| **Make date Due** | Specify the due date with which to mark these change requests, by doing one of the following:<br>• Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>• Type the desired date in the field provided. You can use most relative and absolute formats, for example `yyyy-mm-dd`, `mm/dd/yyyy`, `Mon dd yyyy`, “next week”, and “now + 3 days”. |
| **Make date Resolved** | Specify the date with which to mark these change requests as having been resolved on, by doing one of the following:<br>• Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>• Type the desired date in the field provided. You can use most relative and absolute formats, for example `yyyy-mm-dd`, `mm/dd/yyyy`, `Mon dd yyyy`, “next week”, and “now + 3 days”. |

### Edit fields

This area enables you to add or delete values in specific fields of the selected change requests.

- **To add a value to a field:** In the relevant field's row, in the **Add values** column, type the value you want to add.
- **To delete a value from a field:** In the relevant field's row, in the **Delete values** column, type the value you want to delete.

The relevant values for each field are listed below.

| | |
|---|---|
| **Expires** | Specify the date on which this change request will expire, by doing one of the following:<br>• Click 📅, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**.<br>• Type the desired date in the field provided. You can use most relative and absolute formats, for example `yyyy-mm-dd`, `mm/dd/yyyy`, `Mon dd yyyy`, “next week”, and “now + 3 days”. |
| **Owning Role** | The user role to which the change requests should be assigned.<br>This field is read-only. |
| **All Responsible Roles** | The user roles, other than the owning role, that should be responsible for handling the change requests in their current lifecycle stage.<br>This field is relevant only for Parallel-Approval change requests, and it is read-only. |
| **Pending Responsible Roles** | The roles that are responsible for handling the change request in its current lifecycle stage, but which have not yet approved the change request.<br>This field is relevant only for Parallel-Approval change requests, and it is read-only. |
| **External change request id** | Type the ID number of a related change request in an external change management system that is integrated with FireFlow. |
| **Implementation Notes** | Type notes on how to implement the planned change. |

### Edit links

| | |
|---|---|
| **Merge into** | Type the ID number of the change request into which the selected change requests' data should be merged. |
| **Refers to** | Type the ID numbers of change requests to which the selected change requests refer, separated by spaces. |
| **Referred to by** | Type the ID numbers of change requests that refer to the selected change requests, separated by spaces. |

### Add comments or replies to selected change requests

This area enables you to add a comment or reply to the change requests.

| | |
|---|---|
| Update Type | Specify the type of message you want to add to the change requests, by selecting one of the following:<br>• **Comment (not sent to requestors):** Your comment will be added to the change requests' history and sent as an email message to the change requests' owners.<br>• **Reply to requestors:** Your reply will be added to the change requests' history and sent as an email message to both the change requests' owners and the requestors. |
| Subject | Type the subject of the message. |
| Attach | To attach files to your message, do one of the following:<br>• Type the path to the file in the field provided.<br>• Click **Browse**, browse to the desired file, and click **Open**. |
| Message | Type your message. |

## Modify a change request's status

If needed, you can change a change request's lifecycle stage, instantly moving it forward to a later stage without completing the intervening stages, or returning it to an earlier, already completed stage.

### Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click ≡ , then click the desired stage.

   The change request moves to the desired stage.

**Note:** The list of option available in the drop-down list may be changed by an administrator, by editing a workflow's available actions.

## Delete a change request

If it is no longer necessary to handle a specific change request, you can delete it from all users' **Home** pages.

**Note:** Deleted change requests are *not* removed from the FireFlow system. You can still view them, given the change request ID; however, they will no longer appear in **Home** pages or in search results.

**Tip:** To delete multiple change requests simultaneously, update the relevant change requests and set their status to **deleted**. For details, see Update multiple change requests.

### Do the following:

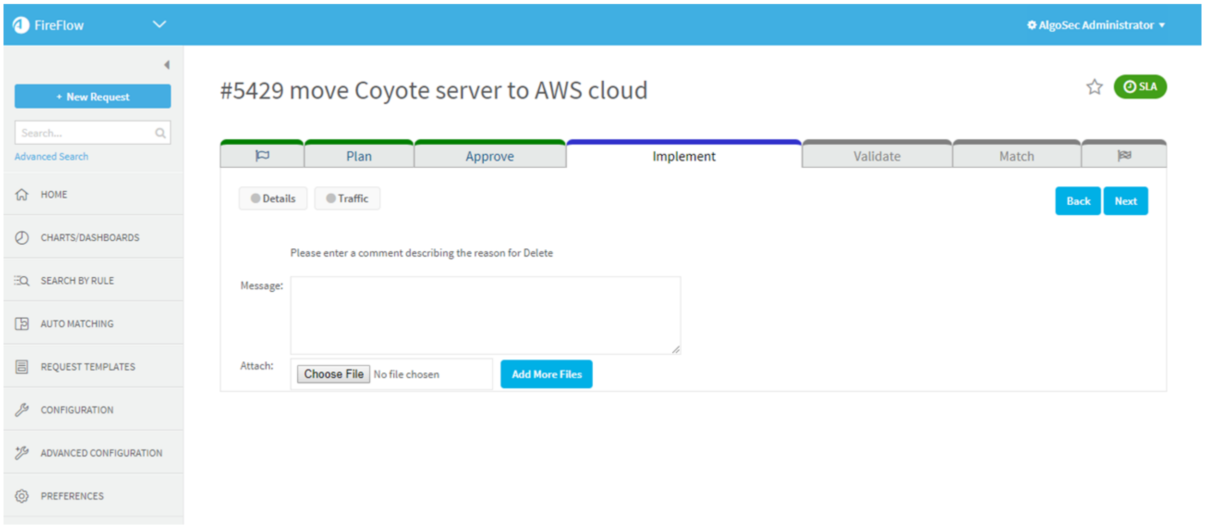
1. View the change request. For details, see View change requests.
2. At the top of the page, click ≡ , then click **Delete**.

   A confirmation message appears.

   **Note:** The list of option available in the drop-down list may be changed by an administrator, by editing a workflow's available actions.

3. Click **OK**.

   The **Delete Change Request** page is displayed.



#5429 move Coyote server to AWS cloud

Please enter a comment describing the reason for Delete

Message:

Attach: No file chosen

4. In the **Message** text box, type your comment.

5. Attach any files needed to your comment. Do one of the following:

| | |
|---|---|
| **Attach files** | To attach files to your comment, in the **Attach** field, do one of the following:<br>• Type the path to the file in the field provided.<br>• Click **Browse**, browse to the desired file, and click **Open**. |
| **Attach more files** | To add more attachments, click **Add More Files** and repeat the previous step. A check box appears, representing the previously added attachment. |
| **Remote attachments** | To remove an attachment, select the check box next to the attachment.<br>The selected attachment will be removed upon completing this procedure. |

6. Click **Next**.

The email message is sent to the requestor, and the change request is deleted from users' **Home** pages.

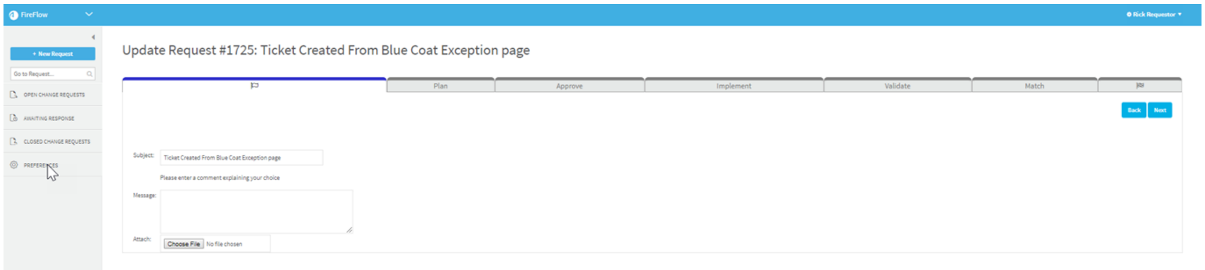
## Comment on change requests

Comment on a change request at any stage throughout the change request's lifecycle. Your comment will be added to the change request's history and sent as an email message to the change request's owner.

### Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click ☰, and then click **Comment**.

   The **Update Request** page is displayed.

   Update Request #1725: Ticket Created From Blue Coat Exception page

   Subject: Ticket Created From Blue Coat Exception page

   Please enter a comment explaining your choice

   Message:

   Attach: No file chosen

   The **Subject** field displays the change request name. The original history item appears in a text box.
3. If desired, modify the **Subject** field to describe the subject of your comment.
4. To attach a file to your comment, do one of the following:
   - In the **Attach** field, type the path to the file.
   - Click **Browse**, browse to the desired file, and click **Open**.
5. In the **Message** text box, type your comment.
6. Click **Next**.

The Requestors Web Interface displays the change request, and your comment appears in the **History** area.

Your comment is sent as an email message to the change request's current owner.

## Respond to change requests

This topic describes how to respond to emails you receive from FireFlow, as well as specific guidelines for responding to rule removal and drop traffic requests.

### Respond to FireFlow emails

Over the course of a change request's lifecycle, you will receive email messages from the FireFlow system.

The **Subject** line of these email messages will include the change request ID in the format: **[FireFlow #<number>]**

For example: **[FireFlow #49]**

Reply to these emails, or write a new email to the FireFlow system directly.

In order for FireFlow to associate your email with the change request, you must include the same ID in the email subject.

For example, if your change request ID is **[FireFlow #49]**, your Subject line might be:

**RE:[FireFlow #49] Access to LAN** or **[FireFlow #49] Everything works fine now**.

### Reply to a change request

Reply to a change request from within FireFlow at any stage in the lifecycle. Your reply will be added to the change request's history and sent as an email message to both the change request's owner and the requestor.

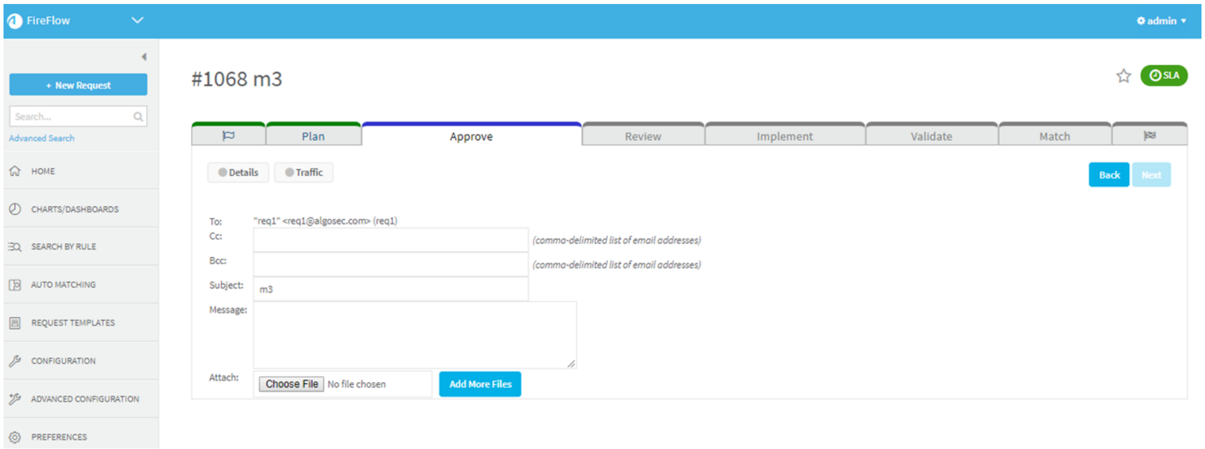
#### Do the following:

1. View the change request. For details, see View change requests.
2. At the top of the page, click ≡ , and then click **Reply**.

   > **Note:** The list of option available in the drop-down list may be changed by an

> administrator, by editing a workflow's available actions.

The reply page is displayed.



#1068 m3

To: "req1" <req1@algosec.com> (req1)

Cc:

Bcc:

Subject: m3

Message:

Attach:

3. Complete the fields as needed, and then click **Next**.

   Your reply is sent as an email message to the requestor and the change request's current owner.

Reply page fields

The following fields are available when replying to a change request from within FireFlow:

| | |
|---|---|
| **To** | The change requestor's email address is displayed.<br>This field is read-only; however, you can send the message to additional people by filling in the **Cc** and **Bcc** fields. |

| | |
|---|---|
| **Cc** | Specify the email addresses of people who should receive a carbon copy of this message, by doing one or more of the following:<br>• In the text box, type the desired email addresses. Email addresses must be separated by commas. For example, "susanb@mycompany.com, johns@mycompany.com" In all future replies to this change request's history items, a check box will appear for each of the specified email addresses, in both the **Cc** and **Bcc** areas.<br>• If check boxes appear under the text box, select the desired email addresses. |
| **Bcc** | Specify the email addresses of people who should receive a blind carbon copy of this message, by doing one or more of the following:<br>• In the text box, type the desired email addresses. Email addresses must be separated by commas. For example, "susanb@mycompany.com, johns@mycompany.com" In all future replies to this change request's history items, a check box will appear for each of the specified email addresses, in both the **Cc** and **Bcc** areas.<br>• If check boxes appear under the text box, select the desired email addresses. |
| **Subject** | Type the subject of the message.<br>By default, this field displays the change request name. |
| **Message** | Type your message. |
| **Attach** | To attach files to your message, do one of the following:<br>• Type the path to the file in the field provided.<br>• Click **Browse**, browse to the desired file, and click **Open**.<br>To add more attachments, click **Add More Files**.<br>To remove an attachment, select the check box next to the attachment. The selected attachment will be removed upon sending the message. |

## Respond to rule removal and drop traffic requests

**Relevant for: Network operations users**

When handling rule removal or drop traffic requests, requestors of related change requests will be notified and given the opportunity to confirm or decline the change.

These notifications have due dates. If you do not respond by the due date, the change is considered to be confirmed.

> **Note:** To determine a change request's stage, view the change request as described in Viewing Change Requests. The stage is indicated by the Change Request Lifecycle Status Bar.

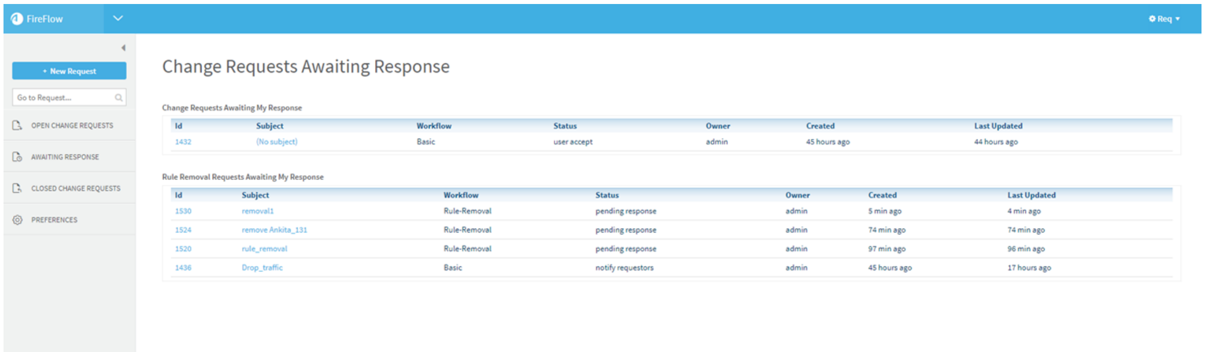
Do one of the following:

### Respond to rule removal requests

Do the following:

1. In the main menu, click **Awaiting Response**.

   The **Change Requests Awaiting Response** page is displayed.

   Change Requests Awaiting Response

   Change Requests Awaiting My Response

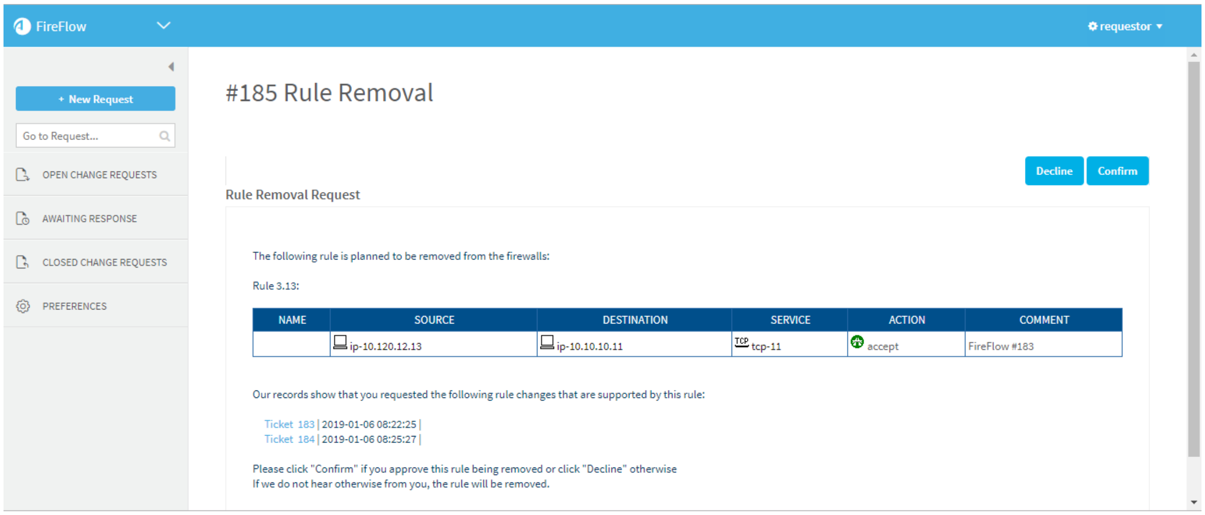
   | Id | Subject | Workflow | Status | Owner | Created | Last Updated |
   |---|---|---|---|---|---|---|
   | 1432 | (No subject) | Basic | user accept | admin | 45 hours ago | 44 hours ago |

   Rule Removal Requests Awaiting My Response

   | Id | Subject | Workflow | Status | Owner | Created | Last Updated |
   |---|---|---|---|---|---|---|
   | 1530 | removal1 | Rule-Removal | pending response | admin | 5 min ago | 4 min ago |
   | 1524 | remove Ankita_131 | Rule-Removal | pending response | admin | 74 min ago | 74 min ago |
   | 1520 | rule_removal | Rule-Removal | pending response | admin | 97 min ago | 96 min ago |
   | 1436 | Drop_traffic | Basic | notify requestors | admin | 45 hours ago | 17 hours ago |

2. In the **Rule Removal Requests Awaiting My Response** list, click the change request.

   The **Rule Removal Request** page is displayed.



#185 Rule Removal

Rule Removal Request

The following rule is planned to be removed from the firewalls:

Rule 3.13:

| NAME | SOURCE | DESTINATION | SERVICE | ACTION | COMMENT |
|---|---|---|---|---|---|
| | ip-10.120.12.13 | ip-10.10.10.11 | tcp-11 | accept | FireFlow #183 |

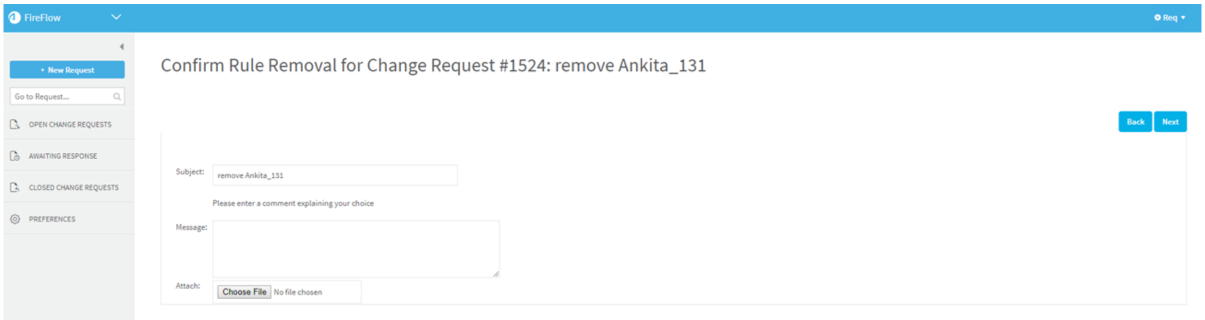
Our records show that you requested the following rule changes that are supported by this rule:

Ticket 183 | 2019-01-06 08:22:25 |
Ticket 184 | 2019-01-06 08:25:27 |

Please click "Confirm" if you approve this rule being removed or click "Decline" otherwise
If we do not hear otherwise from you, the rule will be removed.

3. At the top of the page, click **Confirm** to approve the rule deletion or **Decline** to decline the rule deletion.

   The **Confirm Rule Removal** or **Decline Rule Removal** page is displayed.



Confirm Rule Removal for Change Request #1524: remove Ankita_131

Subject: remove Ankita_131

Please enter a comment explaining your choice

Message:

Attach: No file chosen

4. Modify the **Subject** field to describe the subject of your comment.
5. To attach a file to your comment, do one of the following:
   - In the **Attach** field, type the path to the file.
   - Click **Browse**, browse to the desired file, and click **Open**.
6. In the **Message** text box, type your comment.
7. Click **Next**.

The Requestors Web Interface displays the change request, and your comment appears in the **History** area.

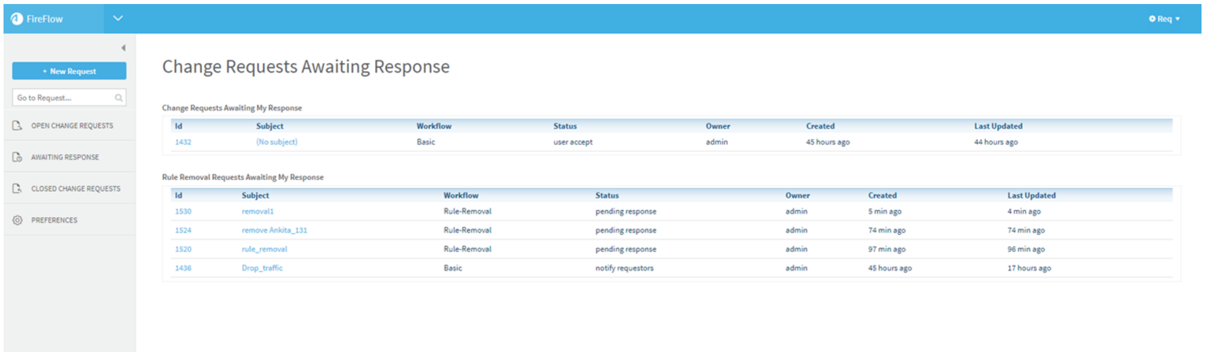
Your comment is sent as an email message to the change request's current owner.

## Respond to drop traffic requests

Do the following:

1. In the main menu, click **Awaiting Response**.

   The **Change Requests Awaiting Response** page is displayed.

   Change Requests Awaiting Response

   Change Requests Awaiting My Response

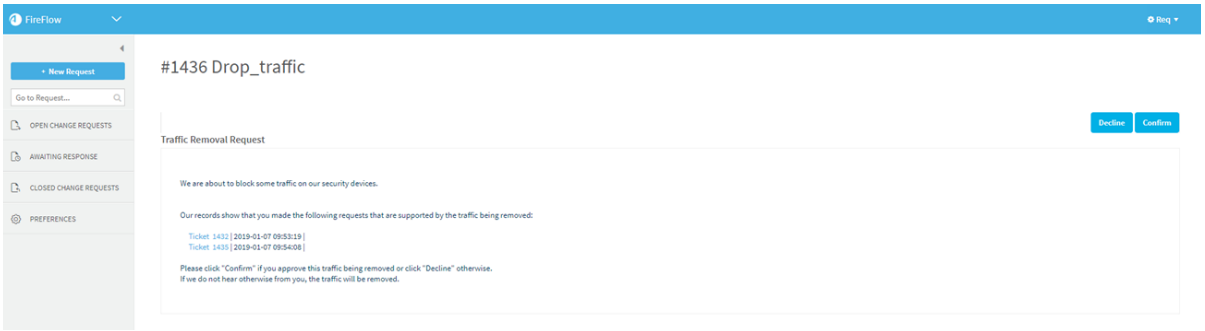
   | Id | Subject | Workflow | Status | Owner | Created | Last Updated |
   |---|---|---|---|---|---|---|
   | 1432 | (No subject) | Basic | user accept | admin | 45 hours ago | 44 hours ago |

   Rule Removal Requests Awaiting My Response

   | Id | Subject | Workflow | Status | Owner | Created | Last Updated |
   |---|---|---|---|---|---|---|
   | 1530 | removal1 | Rule-Removal | pending response | admin | 5 min ago | 4 min ago |
   | 1524 | remove Ankita_131 | Rule-Removal | pending response | admin | 74 min ago | 74 min ago |
   | 1520 | rule_removal | Rule-Removal | pending response | admin | 97 min ago | 96 min ago |
   | 1436 | Drop_traffic | Basic | notify requestors | admin | 45 hours ago | 17 hours ago |

2. In the **Change Requests Awaiting My Response** list, click the change request.

   The **Traffic Removal Request** page is displayed.

   #1436 Drop_traffic

   Traffic Removal Request

   We are about to block some traffic on our security devices.

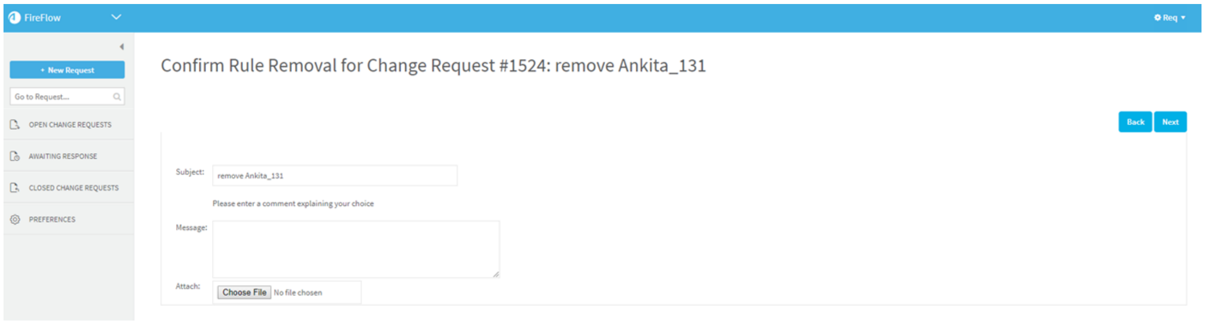
   Our records show that you made the following requests that are supported by the traffic being removed:

   Ticket 1432 | 2019-01-07 09:53:19 |
   Ticket 1435 | 2019-01-07 09:54:08 |

   Please click "Confirm" if you approve this traffic being removed or click "Decline" otherwise.
   If we do not hear otherwise from you, the traffic will be removed.

3. At the top of the page, click **Confirm** to approve the rule deletion or **Decline** to decline the rule deletion.

   The **Confirm Rule Removal** or **Decline Rule Removal** page is displayed.



Confirm Rule Removal for Change Request #1524: remove Ankita_131

Subject: remove Ankita_131

Please enter a comment explaining your choice

Message:

Attach: No file chosen

4. Modify the **Subject** field to describe the subject of your comment.
5. To attach a file to your comment, do one of the following:
    - In the **Attach** field, type the path to the file.
    - Click **Browse**, browse to the desired file, and click **Open**.
6. In the **Message** text box, type your comment.
7. Click **Next**.

The Requestors Web Interface displays the change request, and your comment appears in the **History** area.

Your comment is sent as an email message to the change request's current owner.

## Manage generic change requests

This topic describes the default process for working with generic change requests.

For more details, see Generic change workflow.

### Do the following:

| User type | Step | Reference |
|---|---|---|
| **Requestor or privileged user** | Submit a change request using the **120: Generic request** template. | Request changes |

| User type | Step | Reference |
|---|---|---|
| **Information security user** | Initiate a manual check to determine whether there would be any risks entailed in implementing the requested change. | Perform a manual risk check |
| **Information security user** | Do one of the following:<br>• Approve the change request and send it on to the next stage.<br>• Reject the change request and send it back to planning.<br>• Reject the change request and close it. | Approve, reject, or return to planning |
| **Network operations user** | Implement the requested changes on the security device. | Implement changes |
| **Network operations users** | Notify the requestor that the requested changes were implemented. | Notify change requestors |
| **Original requestor** | Verify that the requested change was implemented and the desired result was achieved. | Verify change request results |
| **Network operations user** | Do one of the following:<br>• If the requestor indicates that the implemented changes achieved the desired result specified in the change request, resolve the change request.<br>• If the requestor indicates that the implemented changes did *not* achieve the desired result specified in the change request, re-initiate the Implement stage and repeat change validation until the change is successful.<br>**Note:** If the requestor does not respond, you can choose to resolve the change request anyway. | Approve, reject, or return to planning |

# Manage traffic change requests

This topic describes the default process for working with various types of traffic change requests.

## Manage basic traffic change requests

The following table describes the default process for working with most traffic change requests.

For more details, see Traffic change workflow.

### Do the following:

| User type | Step | Reference |
|---|---|---|
| **Requestor or privileged user** | Create a change request using the **Basic**, **Standard, 110: Multi-Approval Request**, or **150: Parallel-Approval Request** template. | Request changes |
| **Network operations user** | Perform initial planning for the change request.<br>FireFlow will generate a separate change request for each device or policy to be modified. | Initial planning |
| **Drop actions** | | |
| **Network operations user** | If the change request includes a "Drop" action, do the following:<br>1. Search for any change requests for traffic will be blocked by the new **Drop** action.<br>2. Notify the requestors of these change requests that the traffic is slated to be blocked.<br>FireFlow sends an email to the selected requestors. The requestors have until the change request's due date to respond. | Manage requestor notifications |
| **Requestors** | Respond via email message or via the requestors web interface. | Respond to change requests |

| User type | Step | Reference |
|---|---|---|
| **Network operations user** | Re-notify requestors if needed, and review responses from requestors. | Implement changes |
| **Allow actions** | | |
| **Information security user** | If the change request includes an "Allow" action, FireFlow initiates a risk check to determine whether implementing the change specified in the change request would introduce risks. | Examine risk check results |
| **Information security user** | Do one of the following:<br>• **Approve the change request and send it on to the next stage.**<br>FireFlow creates a work order that consists of a list of recommendations for implementing the requested change.<br>• **Reject the change request.**<br>The change request returns to the Plan stage, and you can perform initial planning again.<br>• **Reject and close the change request.**<br>An email message is sent to the requestor, indicating that the request is denied. The change request's lifecycle is ended, and no further user action is required. | Approve planned changes |
| **Multi-Approval or Parallel-Approval workflow** | | |
| **Controller** | If the change request uses the Multi-Approval or Parallel-Approval workflow, review the change request. | Review change requests |
| **All change requests** | | |
| **Network operations user** | Edit the work order as needed. | Edit work orders |

| User type | Step | Reference |
|---|---|---|
| **Network operations user** | Implement changes manually or with ActiveChange. | Implement changes<br>Implement changes with ActiveChange |
| **Network operations user** | FireFlow initiates validation of the implemented device policy changes against the change request. | Validate changes |
| **Network operations user** | Do one of the following:<br>• If validation indicates that the implemented changes achieved the desired result specified in the change request, notify the requestor that the requested changes were implemented.<br>• If validation indicates that the implemented changes did *not* achieve the desired result specified in the change request, re-initiate the Implement stage and repeat change validation until the change is successful. | Notify change requestors<br>Resolve or return change requests |
| **Requestors** | Verify that the requested change was implemented and the desired result was achieved | Verify change request results |
| **Network operations user** | If the requestor indicates that the implemented changes achieved the desired result specified in the change request, resolve the change request.<br>If the requestor indicates that the implemented changes did *not* achieve the desired result specified in the change request, re-initiate the Implement stage and repeat change validation until the change is successful.<br>**Note:** If the requestor does not respond, you can choose to resolve the change request anyway. | Resolve or return change requests |

## Manage IPv6 traffic change requests

The following table describes the default process for working with IPv6 traffic change requests.

For more details, see IPv6 traffic change workflow.

### Do the following:

| User type | Step | Reference |
|---|---|---|
| **Requestor or privileged user** | Create a a change request using the **170: Traffic Change Request (IPv6)** template. | Request changes |
| **Network operations user** | Select devices for the change request.<br>If multiple devices were selected, FireFlow will generate a separate change request for each device or policy to be modified. | Initial planning |
| **Information security user** | Do one of the following:<br>- **Approve the change request and send it on to the next stage.**<br>FireFlow creates a work order that consists of a list of recommendations for implementing the requested change.<br>- **Reject the change request.**<br>The change request returns to the Plan stage, and you can perform initial planning again.<br>- **Reject and close the change request.**<br>An email message is sent to the requestor, indicating that the request is denied. The change request's lifecycle is ended, and no further user action is required. | Approve planned changes |
| **Network operations user** | Edit the work order. | Edit work orders |

| User type | Step | Reference |
|---|---|---|
| **Network operations user** | Implement the changes manually or with ActiveChange. | Implement changes<br>Implement changes with ActiveChange |
| **Network operations user** | Notify the requestor that the requested changes were implemented. | Notify change requestors |
| **Requestors** | Verify that the requested change was implemented and the required result was achieved. | Validate changes |
| **Network operations user** | If the requestor indicates that the implemented changes achieved the desired result specified in the change request, resolve the change request.<br>If the requestor indicates that the implemented changes did *not* achieve the desired result specified in the change request, re-initiate the Implement stage and repeat change validation until the change is successful.<br>**Note:** If the requestor does not respond, you can choose to resolve the change request anyway. | Resolve or return change requests |

## Manage Multicast traffic change requests

The following table describes the default process for working with multicast traffic change requests.

For more details, see Multicast traffic change workflow.

## Do the following:

| User type | Step | Reference |
|---|---|---|
| **Requestor or privileged user** | Submit a change request using the **180: Traffic Change Request (Multicast)** template. | Request changes |
| **Network operations user** | Select devices for the change request.<br>If multiple devices were selected, FireFlow will generate a separate change request for each device or policy to be modified. | Initial planning |
| **Information security user** | Do one of the following:<br>- **Approve the change request and send it on to the next stage.**<br>FireFlow creates a work order that consists of a list of recommendations for implementing the requested change.<br>- **Reject the change request.**<br>The change request returns to the Plan stage, and you can perform initial planning again.<br>- **Reject and close the change request.**<br>An email message is sent to the requestor, indicating that the request is denied. The change request's lifecycle is ended, and no further user action is required. | Approve planned changes |
| **Network operations user** | Edit the work order. | Edit work orders |
| **Network operations user** | Implement the changes manually or with ActiveChange. | Implement changes<br>Implement changes with ActiveChange |

| User type | Step | Reference |
|---|---|---|
| **Network operations user** | Notify the requestor that the requested changes were implemented. | Notify change requestors |
| **Requestors** | Verify that the requested change was implemented and the required result was achieved. | Validate changes |
| **Network operations user** | If the requestor indicates that the implemented changes achieved the desired result specified in the change request, resolve the change request.<br>If the requestor indicates that the implemented changes did *not* achieve the desired result specified in the change request, re-initiate the Implement stage and repeat change validation until the change is successful.<br>**Note:** If the requestor does not respond, you can choose to resolve the change request anyway. | Resolve or return change requests |

## Manage automatic traffic change requests

The following table describes the default process for working with automatic traffic change requests.

### Do the following:

| User type | Step | Reference |
|---|---|---|
| **Requestor or privileged user** | Submit a change request using the **115: Automatic Traffic Change Request** template. | Request changes |

| User type | Step | Reference |
|---|---|---|
| **Network operations user** | Perform initial planning for the change request.<br>**Note:** If the requestor specified all relevant device(s) in the change request form, the change request continues through this stage without confirmation.<br>FireFlow will generate a separate change request for each device or policy to be modified. | Initial planning |
| **Information security user** | FireFlow initiates a risk check to determine whether implementing the change specified in the change request would introduce risks. | Examine risk check results |
| **Information security user** | If the risk check does not produce any **critical** or **high** risks, it is approved automatically, and the change request continues on to the Implement stage.<br>Otherwise, do one of the following:<br>- **Approve the change request and send it on to the next stage.**<br>FireFlow creates a work order that consists of a list of recommendations for implementing the requested change.<br>- **Reject the change request.**<br>The change request returns to the Plan stage, and you can perform initial planning again.<br>- **Reject and close the change request.**<br>An email message is sent to the requestor, indicating that the request is denied. The change request's lifecycle is ended, and no further user action is required. | Approve planned changes |

| User type | Step | Reference |
|---|---|---|
| **Network operations user** | The work order is implemented on the devices automatically, but validation of the changes cannot occur until the devices are analyzed by **AlgoSec Firewall Analyzer**.<br>You can wait for the devices to be analyzed via scheduled monitoring, or you can expedite validation by manually anayzing the relevant devices. | |
| **Network operations user** | FireFlow initiates validation of the changes implemented on the device or policy against the change request. | Validate changes |
| **Network operations user** | If the validation indicates that the implemented changes achieved the desired result specified in the change request, resolve the change request.<br>If the validation indicates that the implemented changes did *not* achieve the desired result specified in the change request, re-initiate the Implement stage and repeat change validation until the change is successful. | Resolve or return change requests |
| **Requestor** | Verify that the requested change was implmemented. | Validate changes |
| **Network operations user** | If the requestor indicates that the implemented changes achieved the desired result specified in the change request, resolve the change request.<br>If the requestor indicates that the implemented changes did *not* achieve the desired result specified in the change request, re-initiate the Implement stage and repeat change validation until the change is successful.<br>**Note:** If the requestor does not respond, you can choose to resolve the change request anyway. | Resolve or return change requests |

## Manage object change requests

This topic describes how to manage single, multiple, and object removal change requests.

## Manage single-device object change requests

This procedure describes how to manage a single-device object change request.

For more details, see Object change workflow.

### Do the following:

| User type | Step | Reference |
|---|---|---|
| **Any privileged user** | Do one of the following:<br>- Submit an object removal request in AlgoSec Firewall Analyzer.<br>- Create a change request using the **130: Object Change Request** template. | Submit an object removal request from AFA<br>Request changes |
| **Information security user** | Search for rules that would be affected by the requested object change. | Find affected rules |
| **Information security user** | Do one of the following:<br>- **Approve the change request and send it on to the next stage.**<br>FireFlow creates a work order that consists of a list of recommendations for implementing the requested change.<br>- **Reject the change request.**<br>The change request returns to the Plan stage, and you can perform initial planning again.<br>- **Reject and close the change request.**<br>An email message is sent to the requestor, indicating that the request is denied. The change request's lifecycle is ended, and no further user action is required. | Approve planned changes |
| **Network operations user** | Edit the work order. | Edit work orders |

| User type | Step | Reference |
|---|---|---|
| **Network operations user** | Implement the requested changes on the security device according to the work order, by using the relevant management system (for example, Check Point Dashboard or Juniper NSM) to implement the changes. | Implement changes |
| **Network operations user** | FireFlow initiates validation of the implemented device policy changes against the change request. | Validate changes |
| **Network operations user** | If the implemented changes achieved the desired result specified in the change request, notify the requestor that the requested changes were implemented.<br>If the implemented changes achieved the desired result specified in the change request, notify the requestor that the requested changes were implemented.<br>If the implemented changes did *not* achieve the desired result specified in the change request, re-initiate the Implement stage and repeat change validation until the change is successful. | Notify change requestors<br>Resolve or return change requests |
| **Network operations user** | Once the changes have been successfully validated, resolve the change request. | Resolve or return change requests |

## Manage multi-device object change requests

This procedure describes how to manage a multi-device object change request.

For more details, see Multi-device object change workflow.

## Do the following:

| User type | Step | Reference |
|---|---|---|
| **Any privileged user** | Do one of the following:<br>- Submit a multi device object change request from the FireFlow REST API.<br>- Submit a multi-device object change request by editing an object in AppViz.<br>**Note:** Editing an object in AppVizonly opens a multi-device object change request when AppChange is licensed and this behavior is configured. | |
| **Information security user** | Search for rules that would be affected by the requested object change. | Find affected rules |
| **Information security user** | Do one of the following:<br>- **Approve the change request and send it on to the next stage.**<br>FireFlow creates a work order that consists of a list of recommendations for implementing the requested change.<br>- **Reject the change request.**<br>The change request returns to the Plan stage, and you can perform initial planning again.<br>- **Reject and close the change request.**<br>An email message is sent to the requestor, indicating that the request is denied. The change request's lifecycle is ended, and no further user action is required. | Approve planned changes |
| **Network operations user** | Edit the work order. | Edit work orders |

| User type | Step | Reference |
|---|---|---|
| **Network operations user** | Implement the requested changes on the security device according to the work order, by using the relevant management system (for example, Check Point Dashboard or Juniper NSM) to implement the changes. | Implement changes |
| **Network operations user** | FireFlow initiates validation of the implemented device policy changes against the change request. | Validate changes |
| **Network operations user** | If the implemented changes achieved the desired result specified in the change request, notify the requestor that the requested changes were implemented.<br>If the implemented changes achieved the desired result specified in the change request, notify the requestor that the requested changes were implemented.<br>If the implemented changes did *not* achieve the desired result specified in the change request, re-initiate the Implement stage and repeat change validation until the change is successful. | Notify change requestors<br>Resolve or return change requests |
| **Network operations user** | Once the changes have been successfully validated, resolve the change request. | Resolve or return change requests |

## Submit an object removal request from AFA

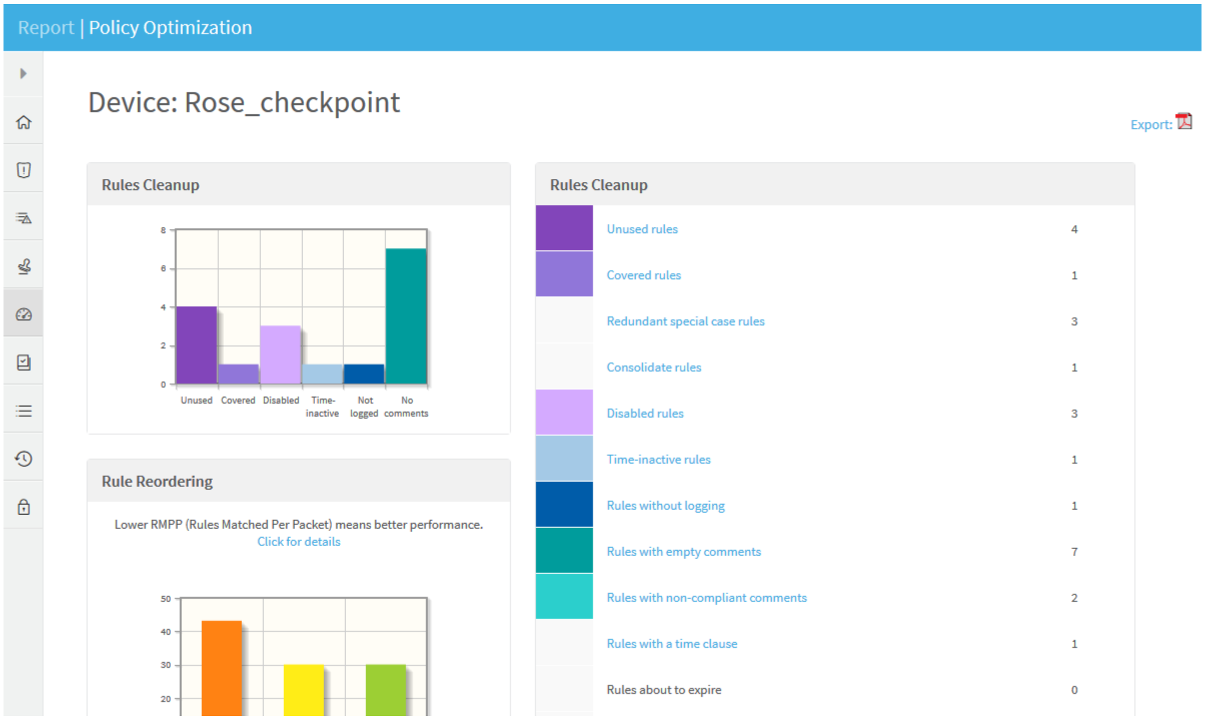
When viewing the **PolicyOptimization** page of a device report in AFA, you can submit an **Object Change** request to remove unattached, empty, and unrouted objects within rules, in the device's policy.

### Do the following:

1. If you're currently in FireFlow, switch to AFA. For details, see Logins and other basics.
2. Browse to and view your device's device report.

3. Click the **PolicyOptimization** tab.

   The **Policy Optimization** page is displayed.



Report | Policy Optimization

Device: Rose_checkpoint

Export:

Rules Cleanup

Rules Cleanup

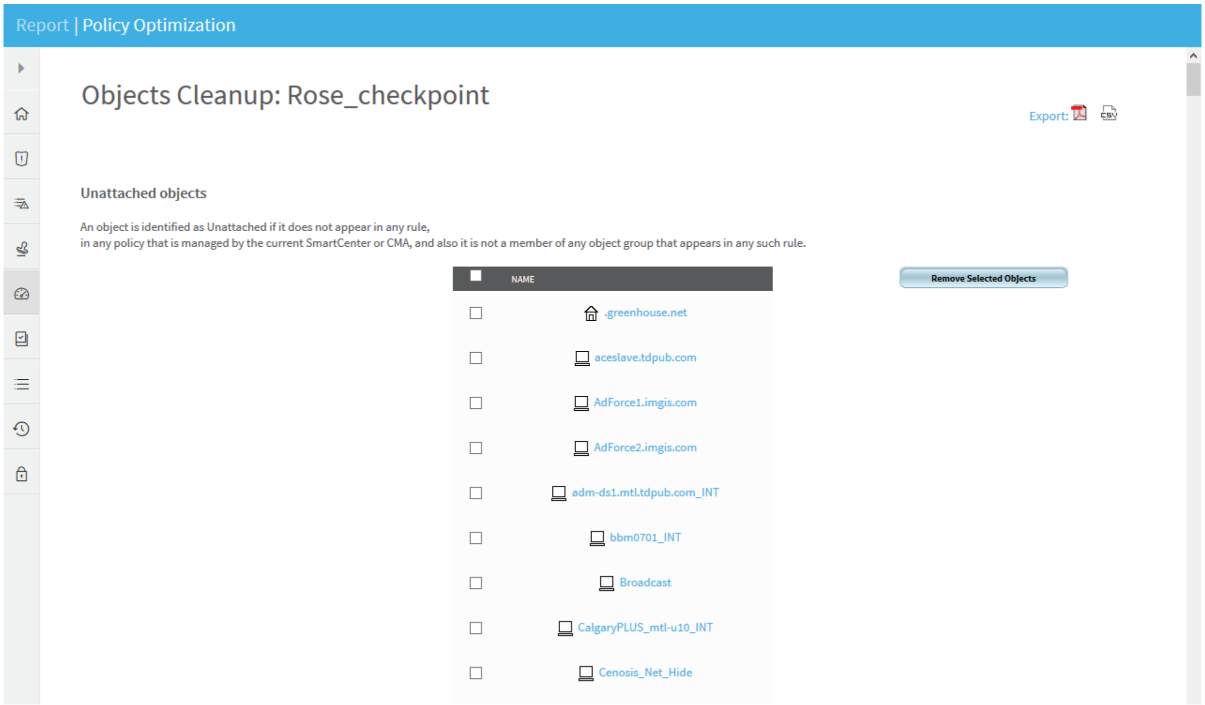
| | | |
|---|---|---|
| 🟪 | Unused rules | 4 |
| 🟪 | Covered rules | 1 |
| | Redundant special case rules | 3 |
| | Consolidate rules | 1 |
| 🟪 | Disabled rules | 3 |
| 🟦 | Time-inactive rules | 1 |
| 🟦 | Rules without logging | 1 |
| 🟦 | Rules with empty comments | 7 |
| 🟦 | Rules with non-compliant comments | 2 |
| | Rules with a time clause | 1 |
| | Rules about to expire | 0 |

Rule Reordering

Lower RMPP (Rules Matched Per Packet) means better performance.
Click for details

Click on one of the supported object categories (**Unattached objects**, **Unattached global objects**, **Empty objects**, and **Unrouted object within rules**).

The objects in the selected category are displayed.



Objects Cleanup: Rose_checkpoint

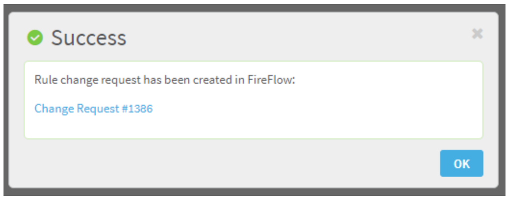
Unattached objects

An object is identified as Unattached if it does not appear in any rule, in any policy that is managed by the current SmartCenter or CMA, and also it is not a member of any object group that appears in any such rule.

| □ | NAME |
|---|---|
| □ | .greenhouse.net |
| □ | aceslave.tdpub.com |
| □ | AdForce1.imgis.com |
| □ | AdForce2.imgis.com |
| □ | adm-ds1.mtl.tdpub.com_INT |
| □ | bbm0701_INT |
| □ | Broadcast |
| □ | CalgaryPLUS_mtl-u10_INT |
| □ | Cenosis_Net_Hide |

4. Do one of the following:
   - In the first column, select the check boxes next to the objects you want to remove.
   - To select all objects, select the check box in the table heading.
5. Click **Remove Selected Objects**.

   A confirmation message appears with a link to the change request.



Rule change request has been created in FireFlow:

Change Request #1386

If desired, the change request's fields may be modified later on. For details, see Advanced change request edits.

**Note:** When you remove more than one object, one change request is opened with multiple object lines.

6. Click **OK.**

# Manage rule removal requests

This topic describes how to manage rule removal requests in FireFlow or from AFA.

## Manage rule removal requests from FireFlow

This procedure describes how to manage rule removal requests using the default workflow.

For more details, see Rule removal workflow.

### Do the following:

| User type | Step | Reference |
|---|---|---|
| **Any privileged user** | Do one of the following:<br>- Submit a rule removal request in AlgoSec Firewall Analyzer.<br>- Create a change request using the **140: Rule Removal Request** template. | Submit a rule removal request from AFA<br>Request changes |
| **Network operations user** | Search for change requests whose traffic intersects that of the rules selected for removal/disablement. | Find related change requests |
| **Network operations user** | Notify the requestors of these change requests that the rules are slated for removal/disablement.<br>FireFlow sends an email to the selected requestors. The requestors have until the rule removal request's due date to respond. | Notify change requestors |
| **Requestor** | Respond via email message or via the requestors web interface. | Respond to change requests |

| User type | Step | Reference |
|---|---|---|
| **Network operations user** | Do one of the following:<br>- Extend the due date of the change request, giving users more time to respond.<br>- Re-notify the requestors.<br>- View responses received from requestors. | Manage requestor notifications |
| **Network operations user** | Once the requestors responses have been received, do one of the following:<br>- **Approve the change request and send it on to the next stage.**<br>FireFlow creates a work order that consists of a list of recommendations for implementing the requested change.<br>- **Reject and close the change request.**<br>An email message is sent to the requestor, indicating that the request is denied. The change request's lifecycle is ended, and no further user action is required. | Approve planned changes |
| **Network operations user** | Edit the work order. | Edit work orders |
| **Network operations user** | Implement the requested changes on the security device according to the work order, by using the relevant management system (for example, Check Point Dashboard or Juniper NSM) to implement the changes. | Implement changes<br>Implement changes with ActiveChange |
| **Network operations user** | FireFlow initiates validation of the implemented device policy changes against the change request. | Validate changes |

| User type | Step | Reference |
|---|---|---|
| **Network operations user** | Do one of the following:<br>• If validation indicates that the specified rules were removed/disabled, resolve the change request.<br>• If validation indicates that the specified rules were *not* removed/disabled, re-initiate the Implement stage and repeat change validation until the change is successful. | Resolve or return change requests |

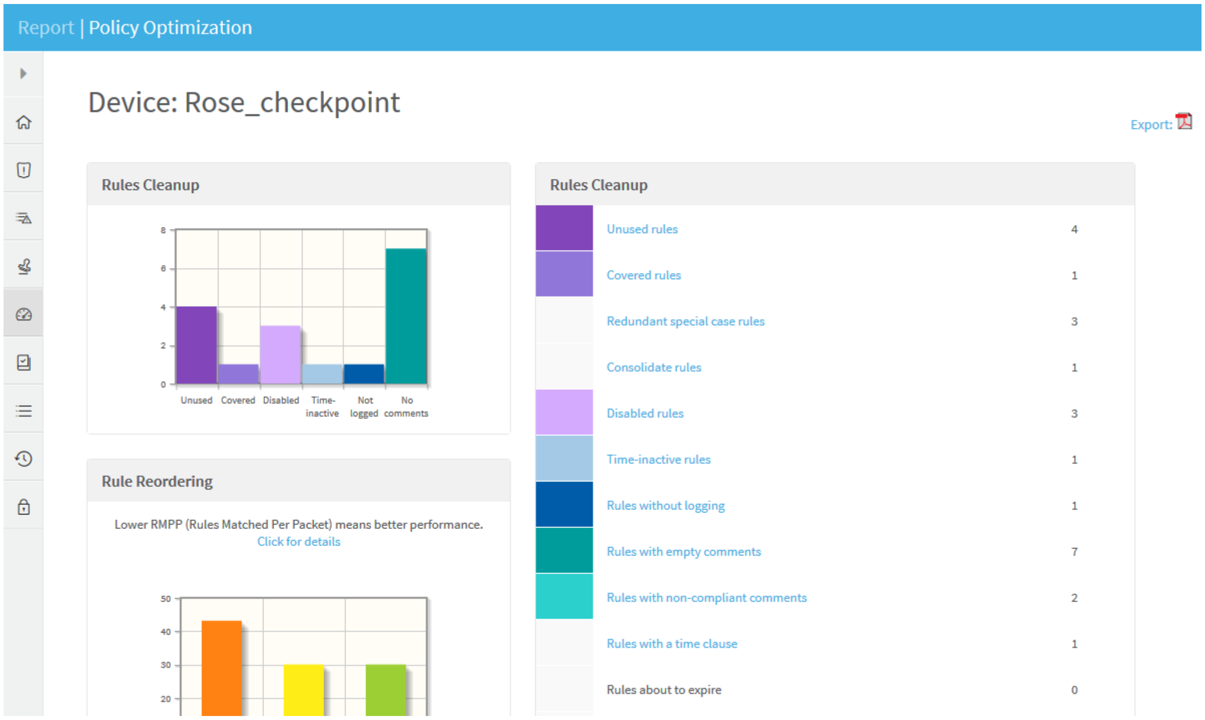
## Submit a rule removal request from AFA

When viewing the **PolicyOptimization** page of a device report in AFA, you can submit a **Rule Removal** request to disable redundant, unused, covered, and unrouted rules in the device's policy.

### Do the following:

1. If you're currently in FireFlow, switch to AFA. For details, see Logins and other basics.
2. Browse to and view your device's device report.
3. Click the **Policy Optimization** tab.

   The **Policy Optimization** page is displayed.



Report | Policy Optimization

Device: Rose_checkpoint

Export:

Rules Cleanup

Rules Cleanup

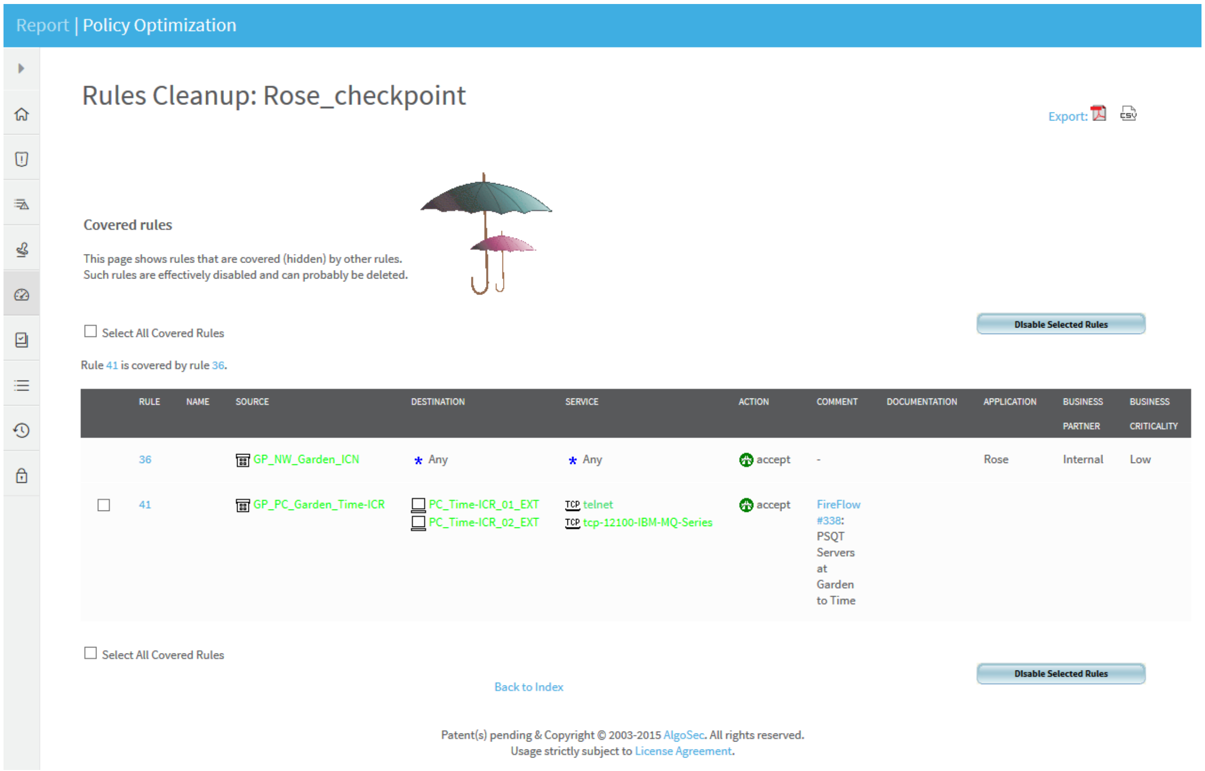
| | | |
|---|---|---|
| 🟪 | Unused rules | 4 |
| 🟪 | Covered rules | 1 |
| | Redundant special case rules | 3 |
| | Consolidate rules | 1 |
| 🟪 | Disabled rules | 3 |
| 🟦 | Time-inactive rules | 1 |
| 🟦 | Rules without logging | 1 |
| 🟩 | Rules with empty comments | 7 |
| 🟦 | Rules with non-compliant comments | 2 |
| | Rules with a time clause | 1 |
| | Rules about to expire | 0 |

Rule Reordering

Lower RMPP (Rules Matched Per Packet) means better performance.
Click for details

4. Click on one of the supported rule categories (**Unused rules**, **Covered rules**, **Redundant special case rules**, and **Unrouted rules**).

   The rules in the selected category are displayed.



Report | Policy Optimization

## Rules Cleanup: Rose_checkpoint

Export:

**Covered rules**

This page shows rules that are covered (hidden) by other rules.
Such rules are effectively disabled and can probably be deleted.

☐ Select All Covered Rules

Disable Selected Rules

Rule 41 is covered by rule 36.

| | RULE | NAME | SOURCE | DESTINATION | SERVICE | ACTION | COMMENT | DOCUMENTATION | APPLICATION | BUSINESS PARTNER | BUSINESS CRITICALITY |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 36 | | GP_NW_Garden_ICN | * Any | * Any | accept | - | | Rose | Internal | Low |
| ☐ | 41 | | GP_PC_Garden_Time-ICR | PC_Time-ICR_01_EXT<br>PC_Time-ICR_02_EXT | TCP telnet<br>TCP tcp-12100-IBM-MQ-Series | accept | FireFlow #338: PSQT Servers at Garden to Time | | | | |

☐ Select All Covered Rules

Disable Selected Rules

Back to Index

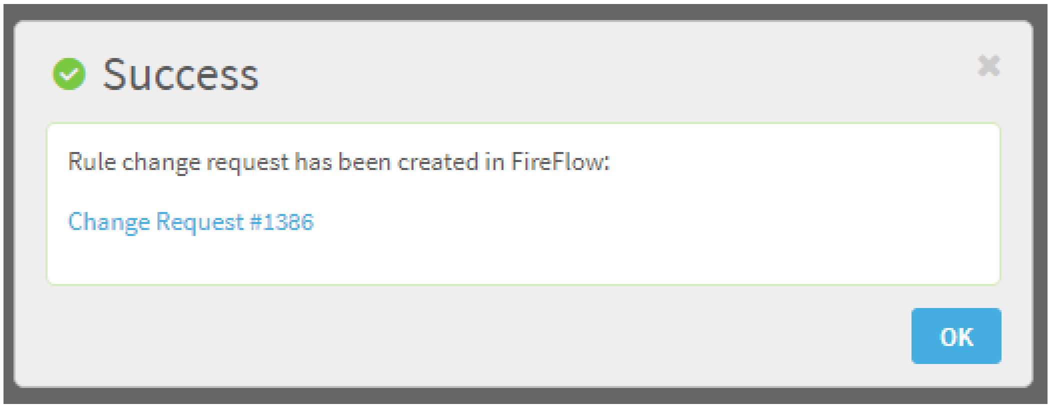
Patent(s) pending & Copyright © 2003-2015 AlgoSec. All rights reserved.
Usage strictly subject to License Agreement.

5. Do one of the following:

   - In the first column, select the check boxes next to the rules you want to disable.
   - To select all rules, select **Select All Covered Rules** / **Select All Unused Rules** / **Select All Special Case Rules**.

6. Click **Disable Selected Rules**.

   A confirmation message appears with a link to the change request.



Success

Rule change request has been created in FireFlow:

Change Request #1386

OK

> **Note:** A single change request is created to handle all rules selected for disabling. To modify the change request's fields, see For details, see Advanced change request edits.

7. Click **OK**.

## Manage rule modification requests

This topic describes how to manage a rule modification request using the default workflow.

For more details, see Rule modification workflow.

### Do the following:

| User type | Step | Reference |
|---|---|---|
| **Any privileged user** | Create a change request using the **145: Rule Modification Request** template. | Request changes |
| **Drop action requests** | | |
| **Network operations user** | Search for change requests whose traffic will be blocked by the "Drop" action. | Find related change requests |
| **Network operations user** | Notify the requestors of these change requests that the traffic is slated to be blocked.<br>FireFlow sends an email to the selected requestors. The requestors have until the change request's due date to respond. | Manage requestor notifications |
| **Requestor** | Respond via email message or via the requestors web interface. | Respond to change requests |
| **Network operations user** | Do any of the following:<br>• Re-notify the requestors.<br>• View responses received from requestors. | Manage requestor notifications |

| User type | Step | Reference |
|---|---|---|
| **Allow action requests** | | |
| **Information security user** | If the change request includes an "Allow" action, FireFlow initiates a risk check, to determine whether implementing the change specified in the change request would introduce risks. | Examine risk check results |
| **Information security user** | Do one of the following:<br>- **Approve the change request and send it on to the next stage.**<br>FireFlow creates a work order that consists of a list of recommendations for implementing the requested change.<br>- **Reject the change request.**<br>The change request returns to the Plan stage, and you can perform initial planning again.<br>- **Reject and close the change request.**<br>An email message is sent to the requestor, indicating that the request is denied. The change request's lifecycle is ended, and no further user action is required. | Approve planned changes |
| **Network operations user** | If the rule has changed while the change request was being processed, Re-Plan the change request. | Re-plan a rule modification request |
| **Network operations user** | Edit the work order. | Edit work orders |
| **Network operations user** | Implement the requested changes on the security device according to the work order, by using the relevant management system (for example, Check Point Dashboard or Juniper NSM) to implement the changes. | Implement changes |
| **Network operations user** | FireFlow initiates validation of the implemented device policy changes against the change request. | Validate changes |

| User type | Step | Reference |
|---|---|---|
| **Network operations user** | If validation indicates that the specified rule was modified, resolve the change request.<br>If validation indicates that the specified rule was *not* modified, re-initiate the Implement stage and repeat change validation until the change is successful. | Resolve or return change requests |

## Manage web filtering change requests

This topic describes how to manage a web filtering change request using the default workflow.

For more details, see Web filtering change workflow.

### Do the following:

| User type | Step | Reference |
|---|---|---|
| **Requestor** | Submit a change request in the Requestors Web Interface using the **160: WebFilter-Change Request (Blue Coat)** template. | Request changes |
| **Network operations user** | Perform initial planning for the change request.<br>If multiple devices were selected, FireFlow will generate a separate change request for each device or policy to be modified. | Initial planning |
| **Information security user** | Do one of the following:<br>- **Approve the change request and send it on to the next stage.**<br>FireFlow creates a work order that consists of a list of recommendations for implementing the requested change.<br>- **Reject the change request.**<br>The change request returns to the Plan stage, and you can perform initial planning again. | Approve planned changes |

| User type | Step | Reference |
|---|---|---|
| **Network operations user** | Choose an organizational methodology to use for implementing the requested change, and edit the work order. | Select an organization method and edit work orders for web filtering change requests |
| **Network operations user** | Implement the requested changes on the security device according to the work order, by using the relevant management system (for example, Check Point Dashboard or Juniper NSM) to implement the changes. | Implement changes |
| **Network operations user** | Compose an email message in FireFlow, notifying the requestor that the requested changes were implemented. | Notify change requestors |
| **Requestor** | Verify that the specified URL has been allowed or blocked as required. | Verify change request results |
| **Network operations user** | If the requestor indicates that the implemented changes achieved the desired result specified in the change request, resolve the change request.<br>If the requestor indicates that the implemented changes did *not* achieve the desired result specified in the change request, re-initiate the Implement stage and repeat change validation until the change is successful.<br>**Note:** If the requestor does not respond, you can choose to resolve the change request anyway. | Resolve or return change requests |

## Manage re-certification requests

This topic describes how to manage recertification requests using the default workflow.

For more details, see Re-certification workflow.

Do the following:

| User type | Step | Reference |
|---|---|---|
| **Network operations user** | Create a recertification request for an expired traffic change request that added Allow traffic. | Re-certify traffic |
| **Network operations user** | Search for change requests whose traffic intersects that of the Allow traffic added by the expired traffic change request. | Find related change requests |
| **Network operations user** | Notify the requestors of these change requests that the Allow traffic is slated for removal. | Notify change requestors |
| **Network operations user** | FireFlow sends an email to the selected requestors. The requestors have until the recertification request's due date to respond. | |
| **Requestor** | Respond via an email message.<br>**Note:** Responding via the web interface is not an option for recertification requests. | Respond to change requests |
| **Network operations user** | Do any of the following:<br>Extend the due date of the request, giving users more time to respond.<br>Re-notify the requestors.<br>View responses received from requestors | Manage requestor notifications |

| User type | Step | Reference |
|---|---|---|
| **Network operations user** | Once the requestors responses have been received, do one of the following:<br>- If the requestors' responses indicate that the Allow traffic should be removed, plan the rule's removal.<br>FireFlow creates a work order that consists of a list of recommendations for implementing the requested change.<br>- If the requestors' responses indicate that the Allow traffic should *not* be removed, certify the traffic.<br>An email message is sent to the requestor, indicating that the request is denied. The change request's lifecycle is ended, and no further user action is required. | Certify or plan traffic removal |
| **Network operations user** | Edit the work order. | Edit work orders |
| **Network operations user** | Implement the requested changes on the security device according to the work order, by using the relevant management system (for example, Check Point Dashboard or Juniper NSM) to implement the changes. | Implement changes |
| **Network operations user** | FireFlow initiates validation of the implemented device policy changes against the change request. | Verify change request results |
| **Network operations user** | Do one of the following:<br>- If validation indicates that the Allow traffic was removed, resolve the change request.<br>- If validation indicates that the Allow traffic was *not* removed, re-initiate the Implement stage and repeat change validation until the change is successful. | Resolve or return change requests |

# Manage verbatim requests

This topic describes how to manage verbatim change requests, which add multiple rules in bulk.

## Do the following:

| User type | Step | Reference |
|---|---|---|
| **Any privileged user** | Create a change request using the **190: Verbatim Rule Addition** template.<br>FireFlow will generate a change request to add the group of rules to the specified device, and the change request moves to the plan stage.<br>Confirm the selected traffic by clicking the **Create Work Order** button. | Request changes |
| **Network operations user** | Edit the work order. | Edit work orders |
| **Network operations user** | Implement the requested changes on the security device according to the work order, | Implement changes<br>Implement changes with ActiveChange |
| **Network operations user** | Verify that the requested change was implemented and the desired result was achieved. | Verify change request results |
| **Network operations user** | Do one of the following:<br>• If the implemented changes achieved the desired result specified in the change request, resolve the change request.<br>• If the implemented changes did *not* achieve the desired result specified in the change request, re-initiate the Implement stage and repeat change validation until the change is successful. | Resolve or return change requests |

# Reports, charts, and dashboards

This section describes how to create and manage FireFlow reports, charts, and dashboards.

▶Creating Charts and Dashboards: Watch to learn about creating FireFlow charts and dashboards.

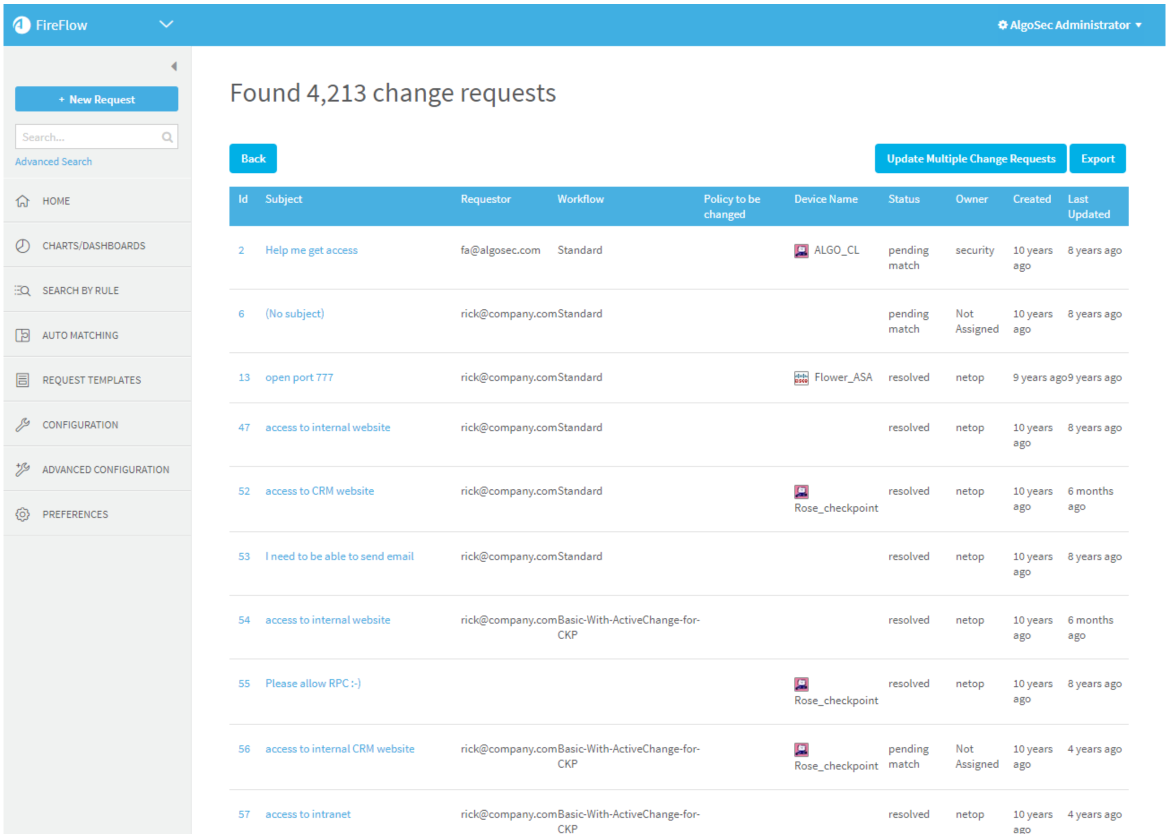
## Generate a FireFlow report

FireFlow enables you to generate reports for a set of change requests.

### Do the following:

1. Perform an advanced search for the change requests you want to include in the report. For details, see Search for change requests.

   The **Found** page appears displaying the report.



Found 4,213 change requests

| Id | Subject | Requestor | Workflow | Policy to be changed | Device Name | Status | Owner | Created | Last Updated |
|---|---|---|---|---|---|---|---|---|---|
| 2 | Help me get access | fa@algosec.com | Standard | | ALGO_CL | pending match | security | 10 years ago | 8 years ago |
| 6 | (No subject) | rick@company.com | Standard | | | pending match | Not Assigned | 10 years ago | 8 years ago |
| 13 | open port 777 | rick@company.com | Standard | | Flower_ASA | resolved | netop | 9 years ago | 9 years ago |
| 47 | access to internal website | rick@company.com | Standard | | | resolved | netop | 10 years ago | 8 years ago |
| 52 | access to CRM website | rick@company.com | Standard | | Rose_checkpoint | resolved | netop | 10 years ago | 6 months ago |
| 53 | I need to be able to send email | rick@company.com | Standard | | | resolved | netop | 10 years ago | 8 years ago |
| 54 | access to internal website | rick@company.com | Basic-With-ActiveChange-for-CKP | | | resolved | netop | 10 years ago | 6 months ago |
| 55 | Please allow RPC :-) | | | | Rose_checkpoint | resolved | netop | 10 years ago | 8 years ago |
| 56 | access to internal CRM website | rick@company.com | Basic-With-ActiveChange-for-CKP | | Rose_checkpoint | pending match | Not Assigned | 10 years ago | 4 years ago |
| 57 | access to intranet | rick@company.com | Basic-With-ActiveChange-for-CKP | | | resolved | netop | 10 years ago | 4 years ago |

2. Do any of the following:

| | |
|---|---|
| **Generate a chart based on the report** | Generate a pie or bar chart that is based on a specific change request attribute, such as change request owner or due date.<br>For details, see Generate FireFlow charts. |
| **Export the report to spreadsheet format** | Export a report to a .tsv file that can be viewed in Excel, for example. The report is presented in table format and includes a pre-defined set of change request attributes.<br>Click **Export** > **Spreadsheet**. |
| **Export a report to RSS format** | Click **Export** > **RSS**. |

# Generate FireFlow charts

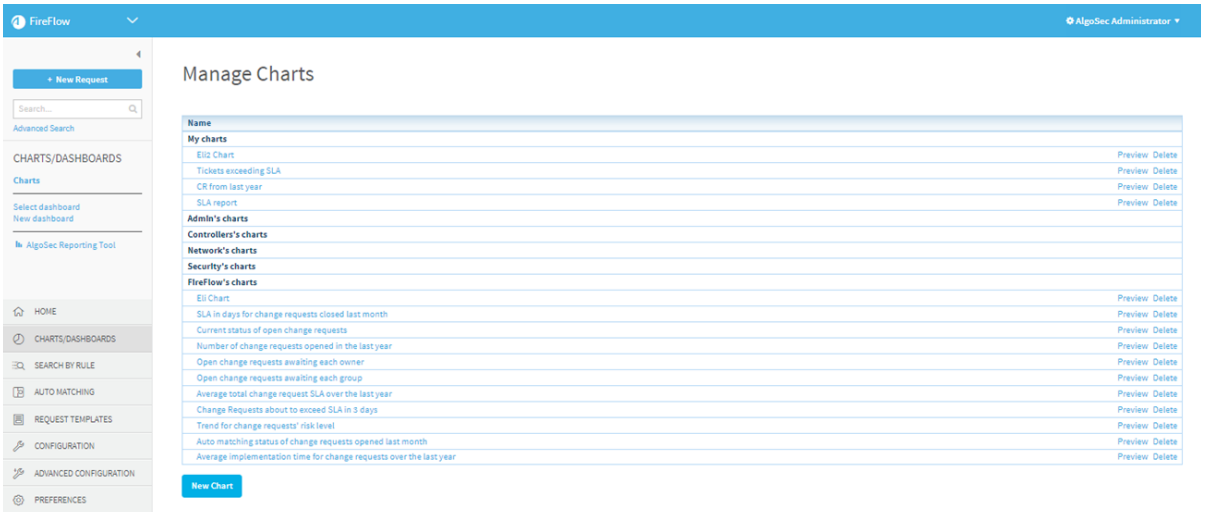
Generate a pie or bar chart that is based on a specific change request attribute.

The chart can be made available to you only, certain user roles, or system-wide. Furthermore, it can be displayed in your **Home** page.

## Do the following:

1. Generate a report. For details, see Generate a FireFlow report.
2. In the main menu, click **Charts/Dashboards**.

   The **Manage Charts** page is displayed.

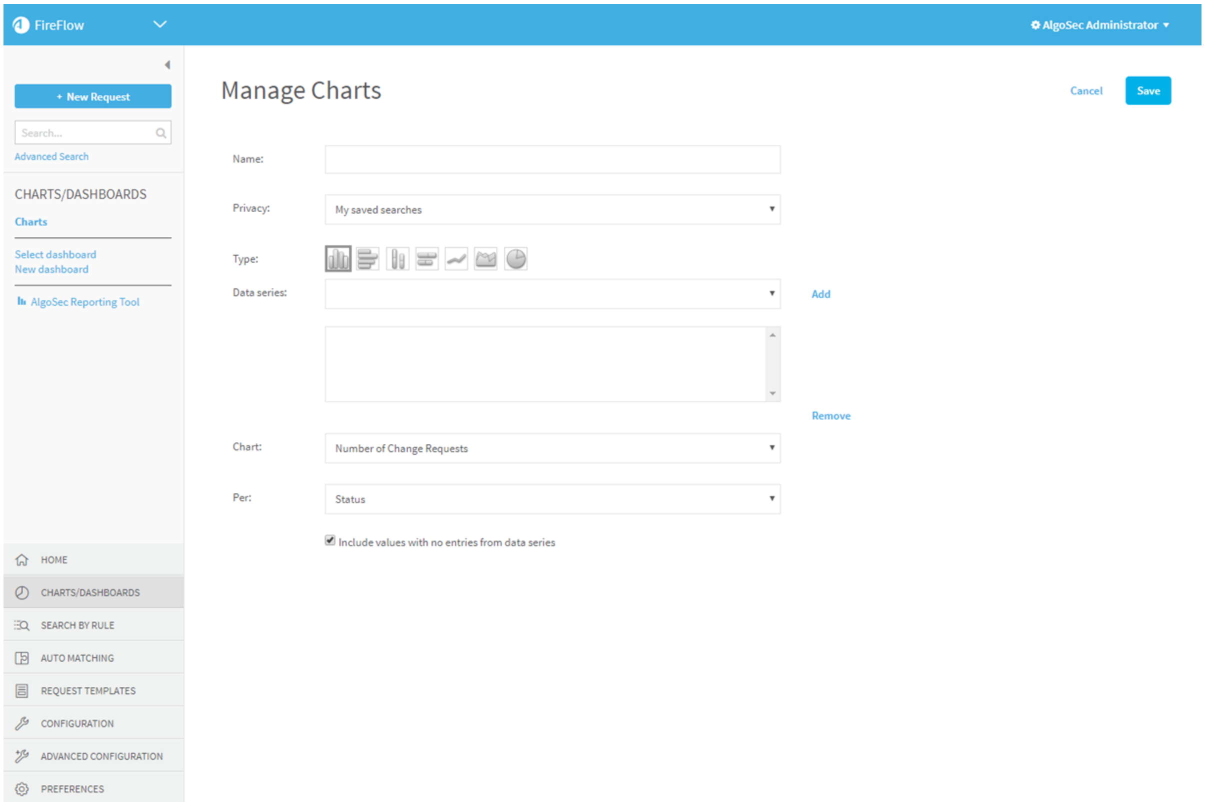


Manage Charts

| Name | |
|---|---|
| **My charts** | |
| Eli2 Chart | Preview Delete |
| Tickets exceeding SLA | Preview Delete |
| CR from last year | Preview Delete |
| SLA report | Preview Delete |
| **Admin's charts** | |
| **Controllers's charts** | |
| **Network's charts** | |
| **Security's charts** | |
| **FireFlow's charts** | |
| Eli Chart | Preview Delete |
| SLA in days for change requests closed last month | Preview Delete |
| Current status of open change requests | Preview Delete |
| Number of change requests opened in the last year | Preview Delete |
| Open change requests awaiting each owner | Preview Delete |
| Open change requests awaiting each group | Preview Delete |
| Average total change request SLA over the last year | Preview Delete |
| Change Requests about to exceed SLA in 3 days | Preview Delete |
| Trend for change requests' risk level | Preview Delete |
| Auto matching status of change requests opened last month | Preview Delete |
| Average implementation time for change requests over the last year | Preview Delete |

3. Click **New Chart**.

   New fields are displayed.



Manage Charts

Name:

Privacy: My saved searches

Type:

Data series:

Chart: Number of Change Requests

Per: Status

☑ Include values with no entries from data series

4. Configure the fields as needed. For details, see Chart details fields.

5. Click **Save**.

   The chart is displayed.

6. Click **Done**.

### Chart details fields

| Name | Description |
|---|---|
| **Name** | Type a name for the chart. |

| Name | Description |
|---|---|
| **Privacy** | Specify who should be allowed to view this chart, by selecting one of the following:<br>• **My saved searches:** The chart is available only to you.<br>• **Admin's saved searches:** The chart is available to all administrators.<br>• **Controllers' saved searches:** The chart is available to all controllers.<br>• **Network's saved searches:** The chart is available to all network operations users.<br>• **Security's saved searches:** The chart is available to all information security users.<br>• **FireFlow's saved searches:** The chart is available to all FireFlow users. |
| **Type** | Select the chart type.<br>For more details, see Chart types. |
| **Data series** | Select the report you generated, then click **Add**.<br>The report is listed in the box below.<br>**Note:** You can add multiple reports, for any chart type except pie.<br>To remove a report, click **Remove**. |
| **Chart** | Select the value on which to base the chart. This can be any of the following:<br>• **Number of Tickets** - The number of change requests<br>• A user-defined custom field<br>• The average elapsed time in minutes for a configured SLO |

| Name | Description |
|---|---|
| **Per** | Select the change request attribute on which to base the chart. This can be any of the following:<br>• A change request attribute. For more details, see Change request attributes.<br>• A user-defined custom field<br>• A configured SLO |
| **Include values with no entries from data series** | Select this option to include values of zero in the chart.<br>For example, if you select this option when charting the number of change requests per status, and no change requests currently have the "approve" status, then the resultant chart will include the "approve" status with the value zero. If you do not select this option, the "approve" status will be omitted from the chart. |

### Chart types

| This icon... | Represents this chart type... |
|---|---|
| 📊 | Vertical bar chart with grouped bars |
| ☰ | Horizontal bar chart with grouped bars |
| 📊 | Vertical bar chart with stacked bars |
| ☰ | Horizontal bar chart with stacked bars |
| 📈 | Line chart |
| ▨ | Area chart |
| ◔ | Pie chart |

### Change request attributes

| Select this option... | To generate the chart per... |
|---|---|
| Status | Status. For more details, see View change requests. |
| Auto Matching Status | Change request's "match status", (for example, new, recheck, perfect match, id match, etc). |
| Owner Name | Owner name. |
| Owner EmailAddress | Owner email address. |
| Owner RealName | Owner full name. |
| Owner Nickname | Owner nickname. |
| Owner Organization | Owner organization. |
| Owner Lang | Owner language. |
| Owner City | Owner city. |
| Owner Country | Owner country. |
| Owner Timezone | Owner time zone. |
| Creator Name | Creator name. |
| Creator EmailAddress | Creator email address. |
| Creator RealName | Creator full name. |
| Creator Nickname | Creator nickname. |
| Creator Organization | Creator organization. |
| Creator Lang | Creator language. |
| Creator City | Creator city. |
| Creator Country | Creator country. |
| Creator Timezone | Creator time zone. |
| LastUpdatedBy Name | Name of the user who last updated the change request. |

| Select this option... | To generate the chart per... |
|---|---|
| LastUpdatedBy EmailAddress | Email address of the user who last updated the change request. |
| LastUpdatedBy RealName | Full name of the user who last updated the change request. |
| LastUpdatedBy Nickname | Nickname of the user who last updated the change request. |
| LastUpdatedBy Organization | Organization of the user who last updated the change request. |
| LastUpdatedBy Lang | Language of the user who last updated the change request. |
| LastUpdatedBy City | City of the user who last updated the change request. |
| LastUpdatedBy Country | Country of the user who last updated the change request. |
| LastUpdatedBy Timezone | Time zone of the user who last updated the change request. |
| Requestor Name | Requestor name. |
| Requestor EmailAddress | Requestor email address. |
| Requestor RealName | Requestor full name. |
| Requestor Nickname | Requestor nickname. |
| Requestor Organization | Requestor organization. |
| Requestor Lang | Requestor language. |
| Requestor City | Requestor city. |
| Requestor Country | Requestor country. |
| Requestor Timezone | Requestor time zone. |
| Cc Name | Name of the user who last updated the change request. |

| Select this option… | To generate the chart per… |
|---|---|
| Cc EmailAddress | Email address of a user who receives copies of email messages for the change request. |
| Cc RealName | Full name of a user who receives copies of email messages for the change request. |
| Cc Nickname | Nickname of a user who receives copies of email messages for the change request. |
| Cc Organization | Organization of a user who receives copies of email messages for the change request. |
| Cc Lang | Language of a user who receives copies of email messages for the change request. |
| Cc City | City of a user who receives copies of email messages for the change request. |
| Cc Country | Country of a user who receives copies of email messages for the change request. |
| Cc Timezone | Time zone of a user who receives copies of email messages for the change request. |
| Admin Name | Admin name. |
| Admin EmailAddress | Admin email address. |
| Admin RealName | Admin full name. |
| Admin Nickname | Admin nickname. |
| Admin Organization | Admin organization. |
| Admin Lang | Admin language. |
| Admin City | Admin city. |
| Admin Country | Admin country. |
| Admin Timezone | Admin time zone. |
| DueDaily | Change requests due on each date, including change requests for which no due date is set. |

| Select this option... | To generate the chart per... |
|---|---|
| DueOnDay | Change requests due on a specific date. |
| DueMonthly | Change requests due each month, including change requests for which no due date is set. |
| DueInMonth | Change requests due in a specific month. |
| DueAnnually | Change requests due each year, including change requests for which no due date is set. |
| ResolvedDaily | Change requests resolved on each date, including change requests that have not yet been resolved. |
| ResolvedOnDay | Change requests resolved on a specific date. |
| ResolvedMonthly | Change requests resolved each month, including change requests that have not yet been resolved. |
| ResolvedInMonth | Change requests resolved in a specific month. |
| ResolvedAnnually | Change requests resolved each year, including the number of change requests that have not yet been resolved. |
| CreatedDaily | Change requests created on each date. |
| CreatedOnDay | Change requests created on a specific date. |
| CreatedMonthly | Change requests created each month. |
| CreatedInMonth | Change requests created in a specific month. |
| CreatedAnnually | Change requests created each year. |
| LastUpdatedDaily | Change requests that were last updated on each date. |
| LastUpdatedOnDay | Change requests last updated on a specific date. |
| LastUpdatedMonthly | Change requests that were last updated in each month. |
| LastUpdatedInMonth | Change requests that were last updated in a specific month. |
| LastUpdatedAnnually | Change requests that were last updated in each year. |

# View FireFlow charts

This procedure describes how to view FireFlow charts that are already generated.

## Do the following:

1. In the main menu, click **Charts/Dashboards**, then click **Charts**.

   The **Manage Charts** page is displayed.

2. Click **Preview** next to the desired chart.

   The chart is displayed.

3. To view the number of items represented by a bar in a bar chart, hover the mouse over the desired bar.

# Edit a FireFlow chart

This procedure describes how to edit FireFlow charts that are already generated.

1. In the main menu, click **Charts/Dashboards**, then click **Charts**.

   The **Manage Charts** page is displayed.

2. Click on the name of the desired chart.

   The chart's details are displayed.

3. Modify the fields as needed. For details, see Chart details fields.

4. Click **Save**.

   The chart is displayed.

5. Click **Done**.

# Delete a FireFlow chart

This procedure describes how to delete FireFlow charts.

## Do the following:

1. In the main menu, click **Charts/Dashboards**, then click **Charts**.

   The **Manage Charts** page is displayed.

2. Click **Delete** next to the desired chart.

   The chart is deleted.

# Add dashboards to FireFlow

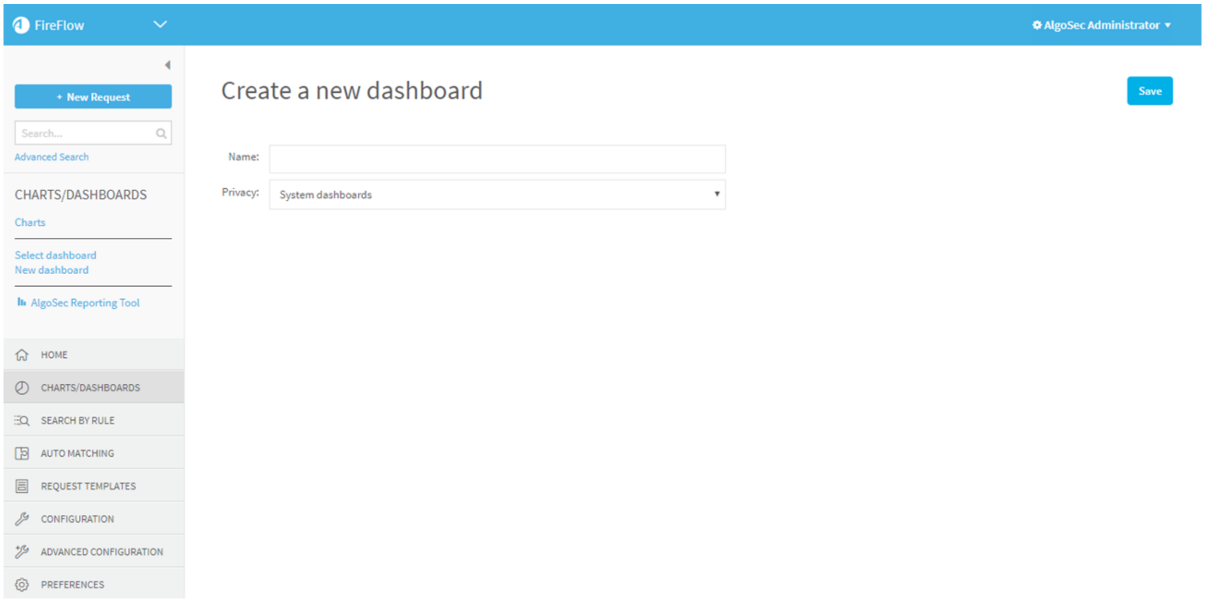
FireFlow enables you to create custom pages displaying a specific set of search results, charts, and other elements. These pages are called *dashboards*, and they can be made available to single users, certain roles, or system-wide.

In addition, users can be subscribed to dashboards, so that they periodically receive the dashboard's content via email.

## Do the following:

1. In the main menu, click **Charts/Dashboards**, then click **New dashboard**.

   The **Create a new dashboard** page is displayed.

   Create a new dashboard

   Name:

   Privacy: System dashboards

2. In the **Name** field, type a name for the dashboard.

3. In the **Privacy** drop-down list, specify who should be allowed to load this dashboard:

    - **My dashboards:** to make the dashboard available only to yourself.
    - **Admin's dashboards:** to make the dashboard available to all administrators.
    - **Controllers' dashboards:** to make the dashboard available to all controllers.
    - **Network's dashboards:** to make the dashboard available to all network operations users.
    - **Security's dashboards:** to make the dashboard available to all information security users.
    - **System dashboards:** to make the dashboard available to all users.

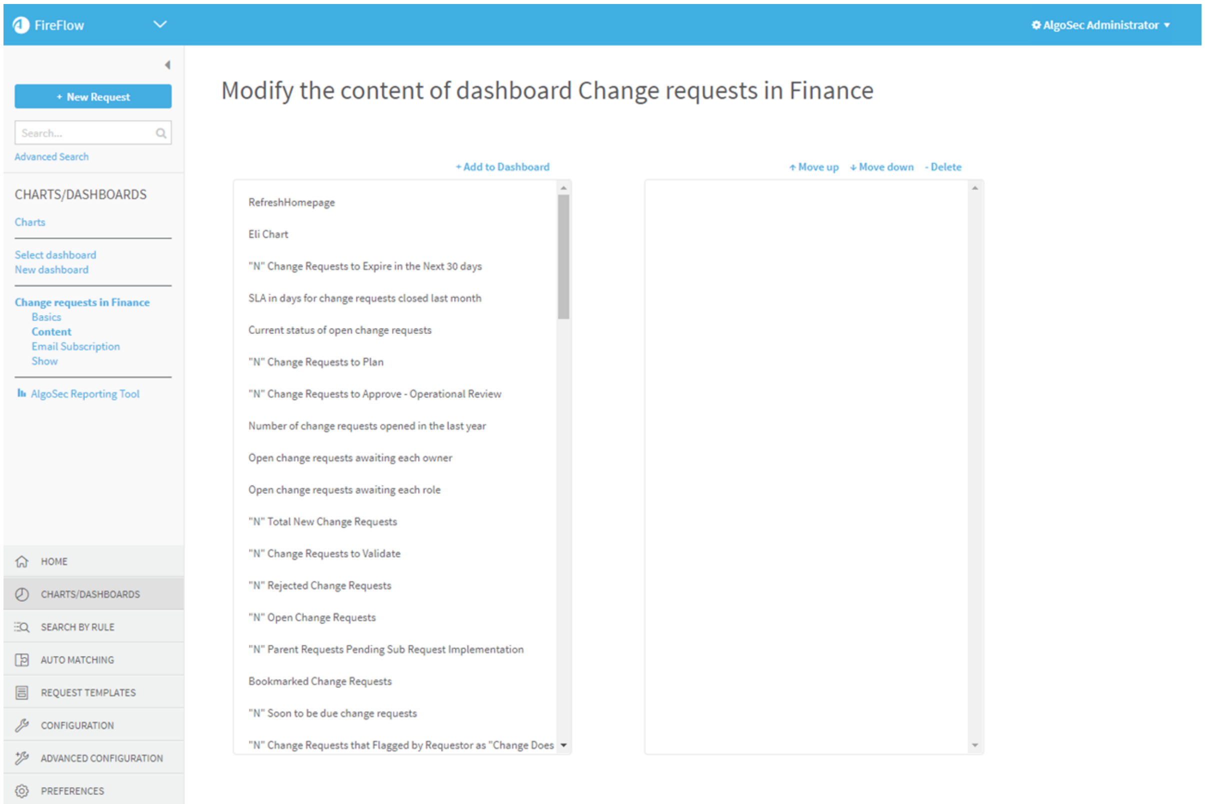
    **Note:** The **Privacy** list includes all of the user roles to which you belong. Therefore, some of the above options may not appear in the list, or additional options may appear.

4. Click **Save**.

    The dashboard is saved and appears in the main menu.

5. In the main menu, under the dashboard's name, click **Content**.

    The **Modify the content of dashboard** page is displayed.



Modify the content of dashboard Change requests in Finance

RefreshHomepage
Eli Chart
"N" Change Requests to Expire in the Next 30 days
SLA in days for change requests closed last month
Current status of open change requests
"N" Change Requests to Plan
"N" Change Requests to Approve - Operational Review
Number of change requests opened in the last year
Open change requests awaiting each owner
Open change requests awaiting each role
"N" Total New Change Requests
"N" Change Requests to Validate
"N" Rejected Change Requests
"N" Open Change Requests
"N" Parent Requests Pending Sub Request Implementation
Bookmarked Change Requests
"N" Soon to be due change requests
"N" Change Requests that Flagged by Requestor as "Change Does

6. For each element you want to add to the dashboard, do the following:

   a. In the **Available** list box, select the element you want to add.

      For more details, see Dashboard 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 dashboard.

   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.

### Dashboard elements

| Select this element… | To add this to the dashboard… |
|---|---|
| RefreshHomepage | Controls for refreshing the page. |
| Bookmarked Change Requests | A list of change requests that the user bookmarked. |
| "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. |
| "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 Validate | Pre-defined search results consisting of a list of change requests in the system that are currently in the Validate stage. |
| "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 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" Requests Pending Sub Request Implementation | Pre-defined search results consisting of a list of requests in the system that are currently in the Implement stage and awaiting implementation of the relevant devices and policies. |
| "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 Controllers group | Pre-defined search results consisting of a list of change requests in the system that are owned by the Controllers role. |
| "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 dashboard... |
|---|---|
| "N" Open Change Requests | Pre-defined search results consisting of a list of change requests in the system that are currently open. |
| "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" 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. |
| My Change Requests | Pre-defined search results consisting of a list of change requests in the system that are owned by you. |
| "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 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" 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" 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 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 Pending Sub Requests Implementation | Pre-defined search results consisting of a list of recertification requests in the system that are currently in the Implement stage and awaiting implementation of the relevant devices and policies. |

| Select this element... | To add this to the dashboard... |
|---|---|
| Change Requests about to exceed SLA (in 3 days) | Pre-defined search results consisting of a list of change requests in the system that will exceed their SLA within 3 days. |
| "N" Change Requests that 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 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 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 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" Resolved Change Requests | Pre-defined search results consisting of a list of change requests in the system that have been resolved. |
| "N" Change Requests to Create Work Order | Pre-defined search results consisting of a list of change requests in the system that are currently in the Implement stage and awaiting a work order to be created. |
| "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 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. |

| Select this element... | To add this to the dashboard... |
|---|---|
| "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 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" 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 Validate | Pre-defined search results consisting of a list of recertification requests in the system that are currently in the Validate stage. |
| "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 required the addition of Allow traffic to a device’s policy, and which are currently expired. |
| Unowned Change Requests | Pre-defined search results consisting of a list of change requests in the system that currently have no owner. |
| "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. |
| Changes Without Request | Pre-defined search results consisting of a list of all detected device changes for which a matching change request was not found. |
| Change <-> Change Request Mismatch | Pre-defined search results consisting of a list of all device changes that do not match the approved changes specified in the associated change request. |

| Select this element... | To add this to the dashboard... |
|---|---|
| Changes Wider than Request | Pre-defined search results consisting of a list of all device changes that are more extensive than the approved changes specified in the associated change request. |
| Change Requests Partially Implemented | Pre-defined search results consisting of a list of all change requests that call for more extensive changes than those actually implemented. |
| *Saved Search Name* | A custom search that was saved, and which is available to your user role. For more details, see Search for change requests. |
| *Chart Name* | A chart that is available to your user role. |
| Search for chart *Chart Name* | A custom search on which a certain chart is based. |

## View FireFlow dashboards

You can view the following dashboards:

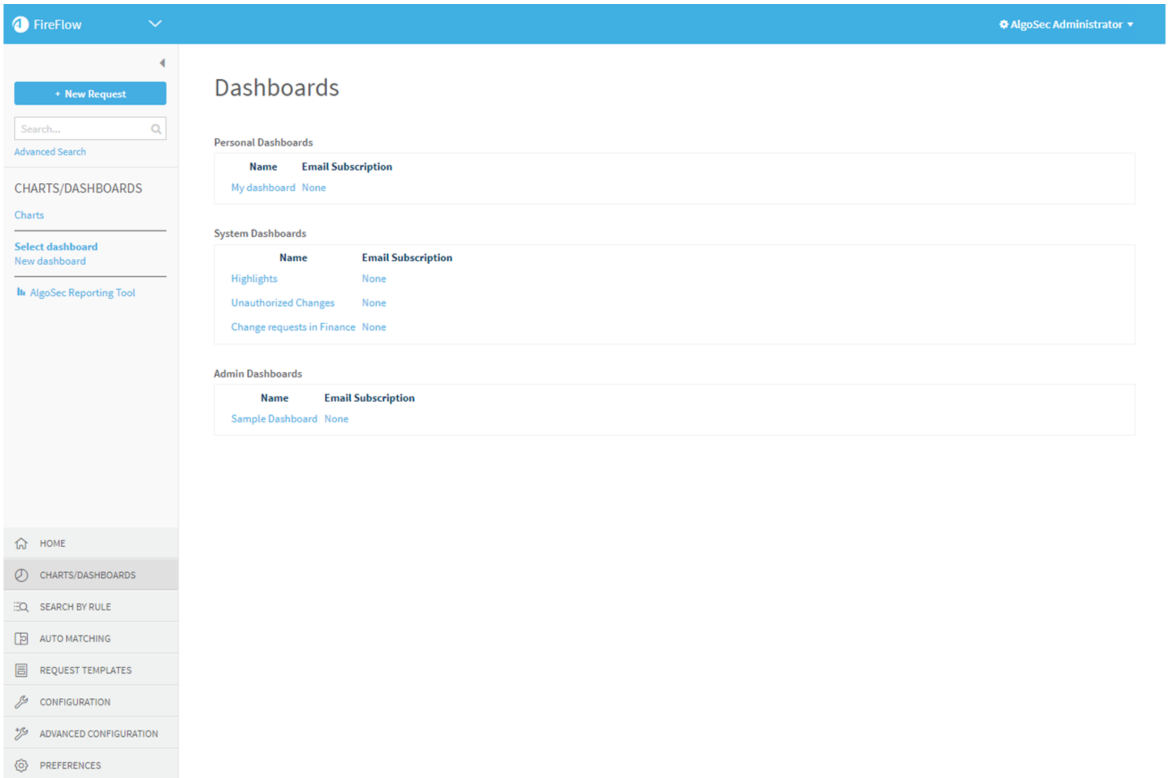
- Personal dashboards
- Dashboards that are available to your user role(s)
- System dashboards

### View all your dashboards

Do the following:

- In the main menu, click **Charts/Dashboards**, then click **Select dashboard**.

  A list of all dashboards available to you is displayed.



Dashboards

Personal Dashboards

| Name | Email Subscription |
|---|---|
| My dashboard | None |

System Dashboards

| Name | Email Subscription |
|---|---|
| Highlights | None |
| Unauthorized Changes | None |
| Change requests in Finance | None |

Admin Dashboards

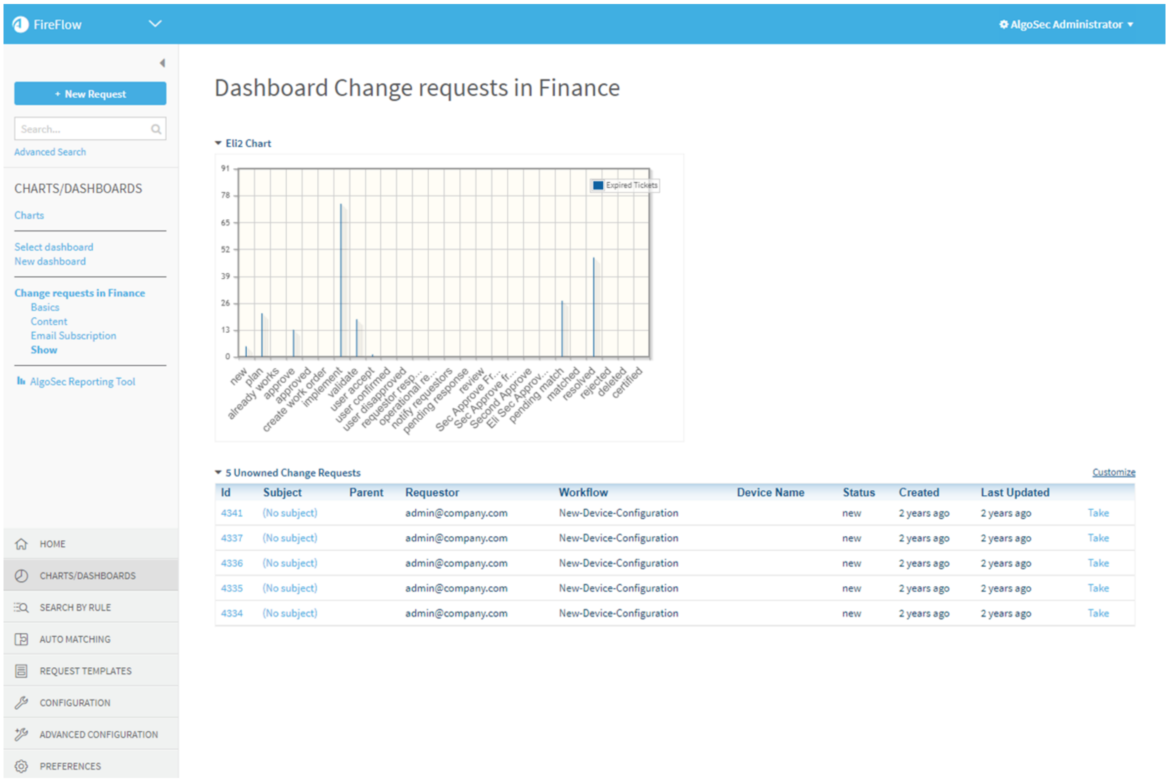
| Name | Email Subscription |
|---|---|
| Sample Dashboard | None |

## View a single dashboard

Do one of the following:

- View all dashboards as described in the previous procedure, then in the workspace, click on the name of the desired dashboard.

  The **Dashboard** page appears displaying the dashboard.



Dashboard Change requests in Finance

5 Unowned Change Requests

| Id | Subject | Parent | Requestor | Workflow | Device Name | Status | Created | Last Updated | |
|---|---|---|---|---|---|---|---|---|---|
| 4341 | (No subject) | | admin@company.com | New-Device-Configuration | | new | 2 years ago | 2 years ago | Take |
| 4337 | (No subject) | | admin@company.com | New-Device-Configuration | | new | 2 years ago | 2 years ago | Take |
| 4336 | (No subject) | | admin@company.com | New-Device-Configuration | | new | 2 years ago | 2 years ago | Take |
| 4335 | (No subject) | | admin@company.com | New-Device-Configuration | | new | 2 years ago | 2 years ago | Take |
| 4334 | (No subject) | | admin@company.com | New-Device-Configuration | | new | 2 years ago | 2 years ago | Take |

- In the main menu, click **Home**, then click the name of the desired dashboard.

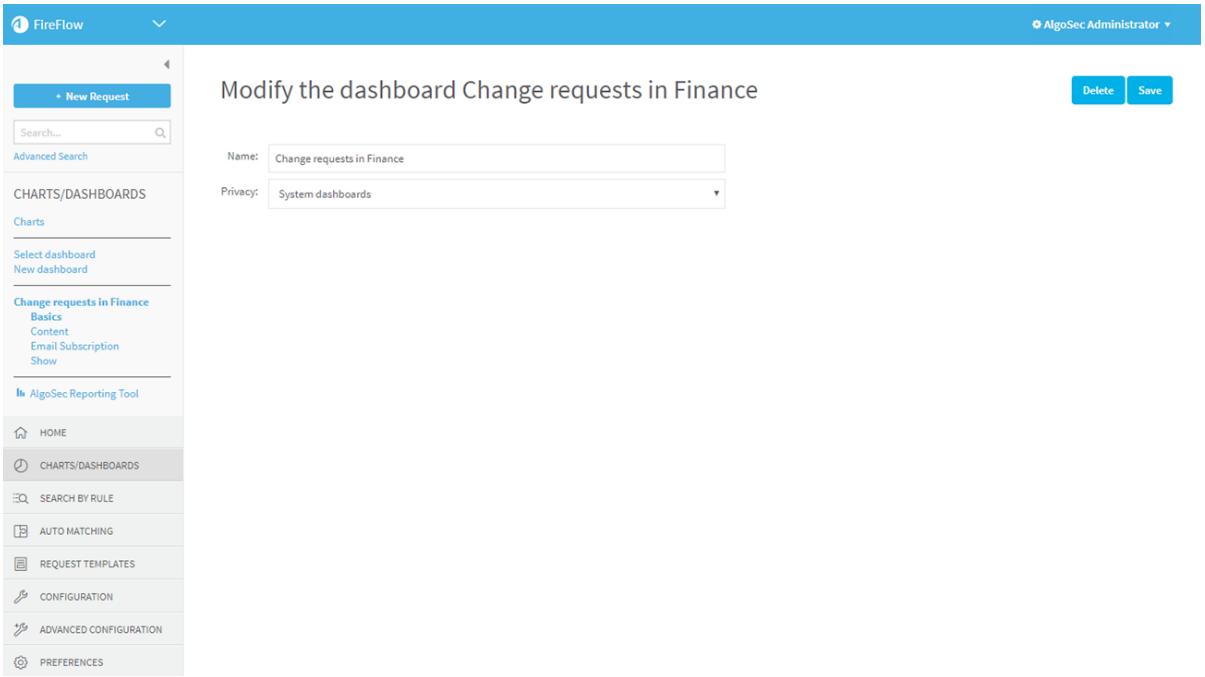
> **Note:** FireFlow lists up to seven dashboards in the main menu. If more than seven dashboards are configured, and the desired dashboard is listed, click **More** in the main menu.

## Edit a FireFlow dashboard

Do the following:

1. View the desired dashboard. For details, see View FireFlow dashboards .
2. In the main menu, under the dashboard's name, click **Basics**.

   The **Modify the dashboard** page is displayed.



Modify the dashboard Change requests in Finance

Name: Change requests in Finance

Privacy: System dashboards

3. In the **Name** field, type a name for the dashboard.
4. In the **Privacy** drop-down list, specify who should be allowed to load this dashboard:
   - **My dashboards:** to make the dashboard available only to yourself.
   - **Admin's dashboards:** to make the dashboard available to all administrators.
   - **Controllers' dashboards:** to make the dashboard available to all controllers.
   - **Network's dashboards:** to make the dashboard available to all network operations users.
   - **Security's dashboards:** to make the dashboard available to all information security users.
   - **System dashboards:** to make the dashboard available to all users.

   **Note:** The **Privacy** list includes all of the user roles to which you belong. Therefore, some of the above options may not appear in the list, or additional options may appear.

5. Click **Save**.

6. In the main menu, under the dashboard's name, click **Content**.

   The **Modify the content of dashboard** page is displayed.

7. For each element you want to add to the dashboard, do the following:

   a. In the **Available** list box, select the element you want to add.

      For more details, see Dashboard 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 dashboard.

   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.

## Manage email subscriptions to dashboards

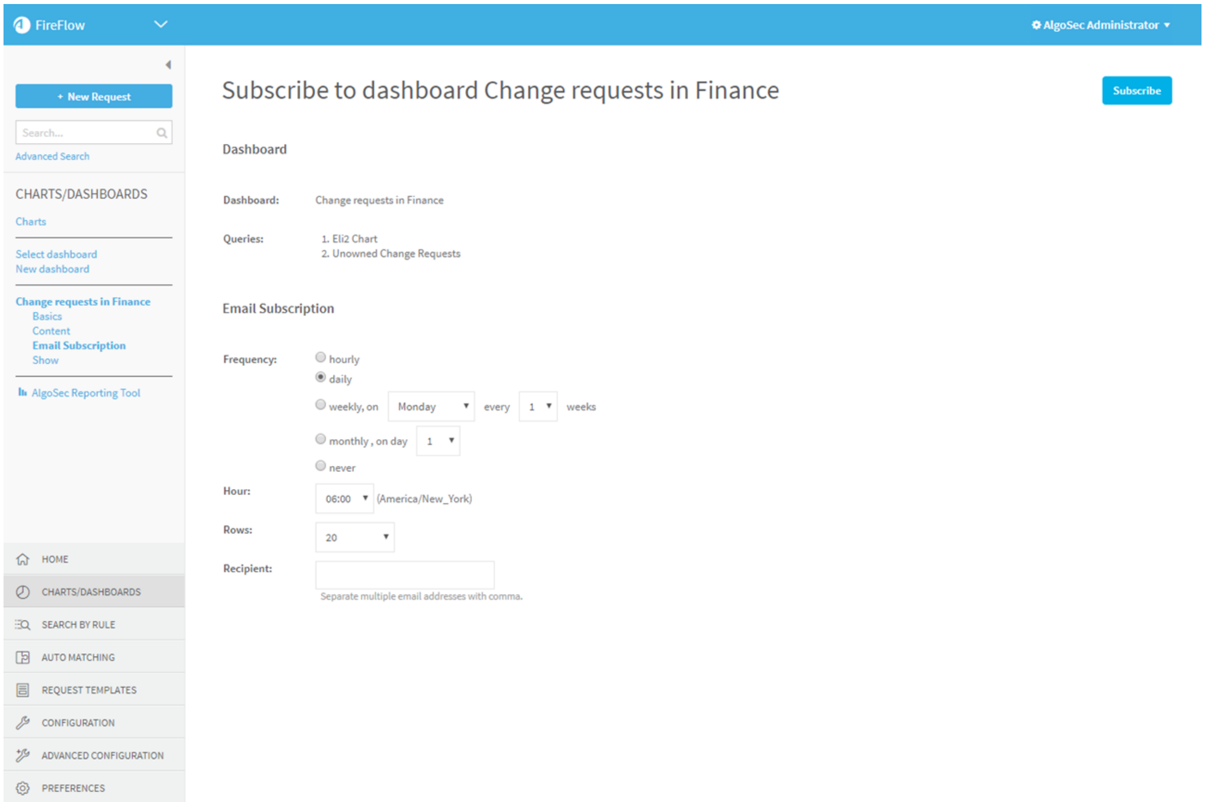
By default, when you create a dashboard, you are automatically subscribed to it, and emails containing the dashboard's content will be sent to the email address associated with your account. If desired, you can configure FireFlow to send these emails to other recipients, and/or change the frequency and time at which these emails are sent.

### Do the following:

1. View the desired dashboard. For details, see View FireFlow dashboards .

2. In the main menu, click **Email Subscription**.

   The **Subscribe to dashboard** page is displayed.



Subscribe to dashboard Change requests in Finance

Dashboard

Dashboard: Change requests in Finance

Queries:
1. Eli2 Chart
2. Unowned Change Requests

Email Subscription

Frequency:
○ hourly
● daily
○ weekly, on Monday every 1 weeks
○ monthly , on day 1
○ never

Hour: 06:00 (America/New_York)

Rows: 20

Recipient:

Separate multiple email addresses with comma.

3. Complete the fields as needed. For details, see Email subscription fields.
4. Click **Subscribe** or **Save**.

### Email subscription fields

| In this field... | Do this... |
|---|---|
| Frequency | Specify how often emails containing dashboard content should be sent. This can have the following values:<br>• **hourly**. Emails will be sent once an hour.<br>• **daily**. Emails will be sent once a day.<br>• **weekly**. Emails will be sent once every specified number of weeks on the specified day.<br>• **monthly**. Emails will be sent once a month on the specified day of the month.<br>• **never**. Emails will not be sent. |

| In this field... | Do this... |
|---|---|
| Hour | Select the hour in the displayed time zone, at which emails containing dashboard content should be sent.<br>**Note:** The time zone can be configured in your user settings. For details, see Configure user preferences. |
| 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 dashboard contents should be sent. The email addresses must be separated by commas.<br>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 a FireFlow dashboard

Delete dashboards no longer in use.

### Do the following:

1. View the desired dashboard. For details, see View FireFlow dashboards .
2. In the main menu, under the dashboard's name, click **Basics**.

   The **Modify the dashboard** page is displayed.
3. Click **Delete**.

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

The dashboard is deleted.

## Access the AlgoSec Reporting Tool from FireFlow

Create new FireFlow dashboards using the AlgoSec Reporting tool.

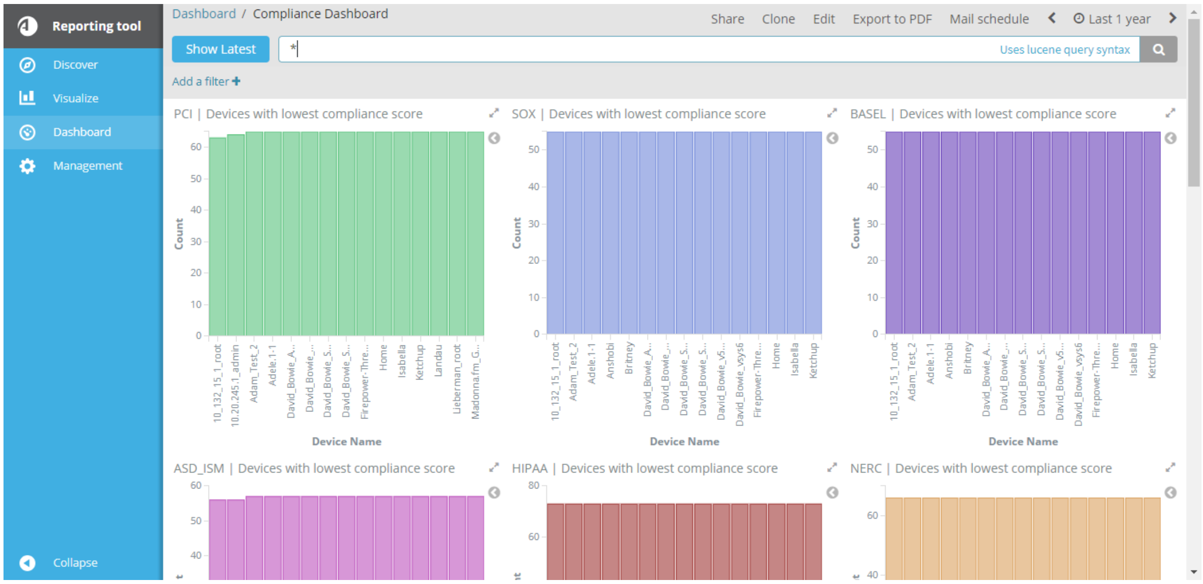
## Do the following:

1. In the main menu, click **Charts/Dashboards**.

   The **Manage Charts** page appears.

2. In the main menu, click **More Dashboards**.

   ART appears in a new tab.



# Configure user preferences

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

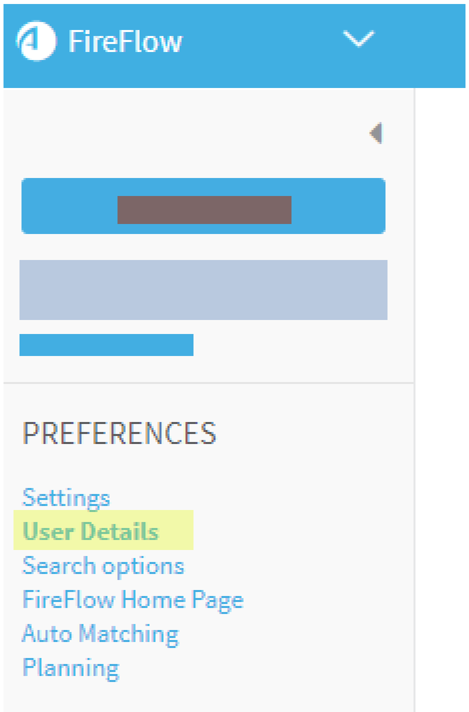
## Access the Preferences page

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:

   
   [redacted]

   > **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.<br>This field is read-only. |
| **Full Name** | Your full name.<br>This field is read-only. |
| **Nickname** | Type your nickname. |
| **Language** | Select the desired FireFlow interface language.<br>All fields will be displayed in the selected language. |
| **Timezone** | Select the time zone in which you are located.<br>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.

# Send us feedback

Let us know how we can improve your experience with the User Guide.

Email us at: techdocs@algosec.com

**Note:** For more details not included in this guide, see the online ASMS Tech Docs.