algosec

AlgoSec FireFlow

Requestor Guide

Legal Notices

Proprietary & Confidential Information

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
- Validate changes
- 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:
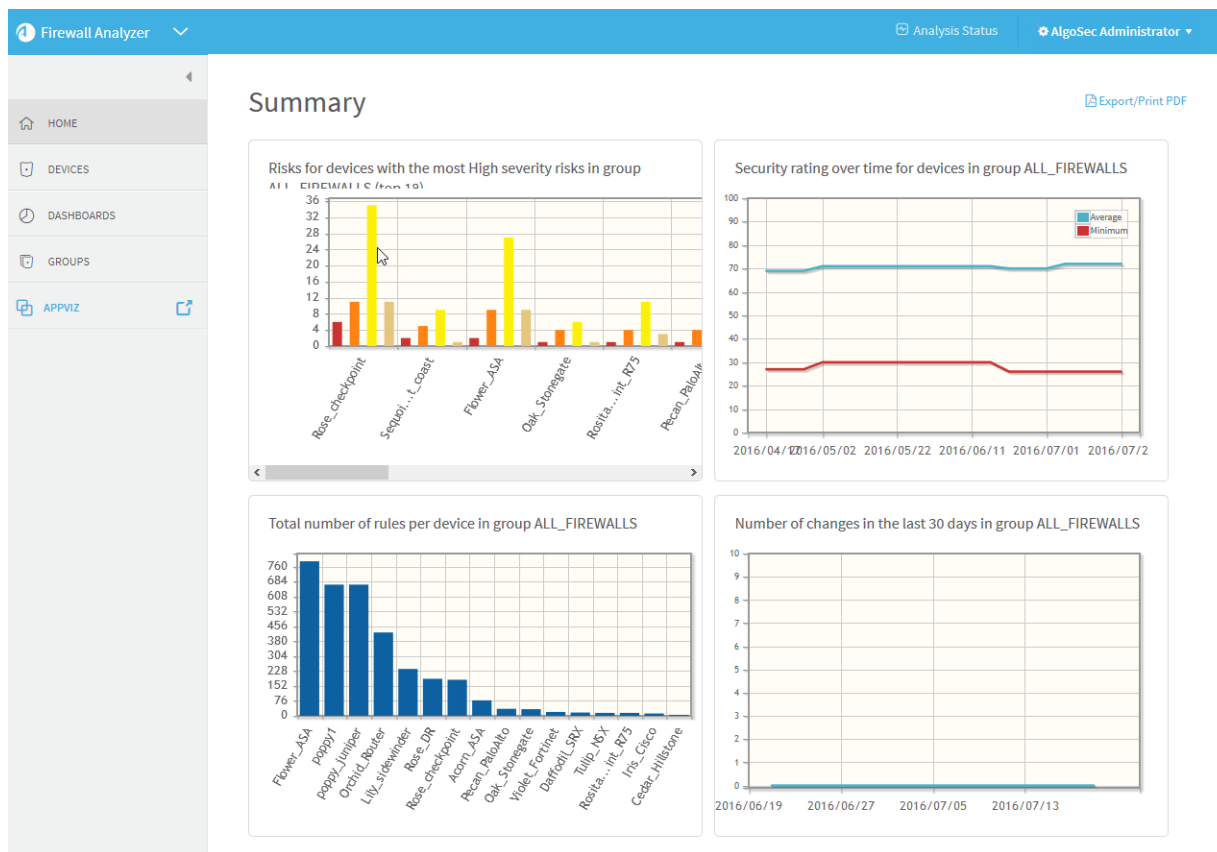
Switch ASMS products

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.
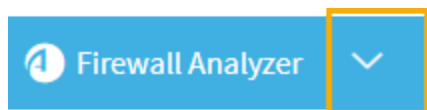
If you are an administrator for any of these products, the relevant administration menu is available from your user dropdown at the top-right:
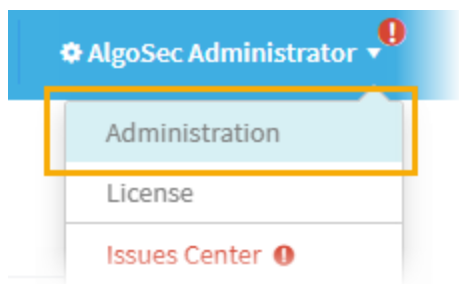
> **Note:** CloudFlow is now accessible from inside ASMS. Click the dropdown at the top-left and select **CloudFlow**.
>
>
>
> For more details, see our CloudFlow Help Center.
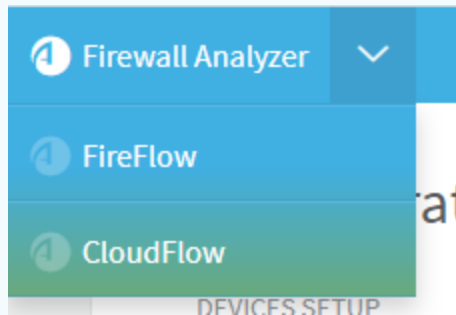
Adjust your screen space

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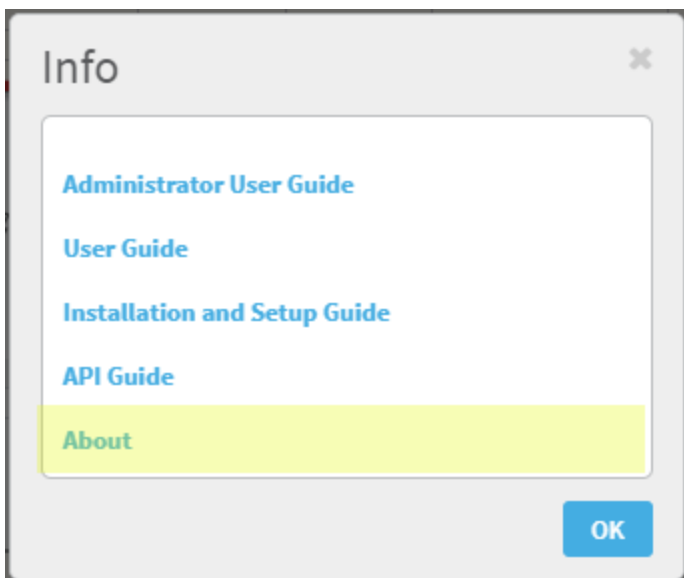
The **About** dialog appears, showing details about the product you have installed.

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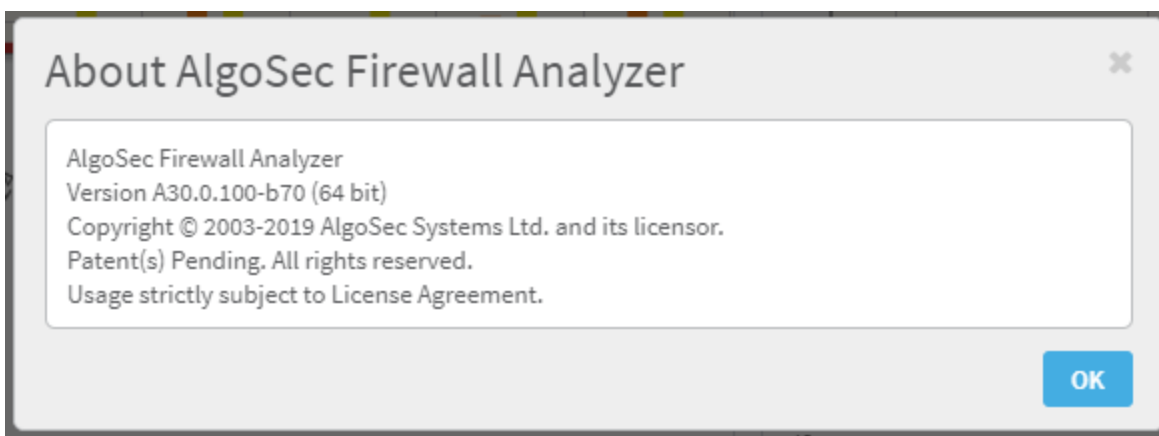
Note: If you are running the FIPS 140-2 compliant version of AFA, this information is indicated in the window.

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*.

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](#)

Configure user preferences

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

Access the Preferences page

To access your user preferences page, do the following:

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

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

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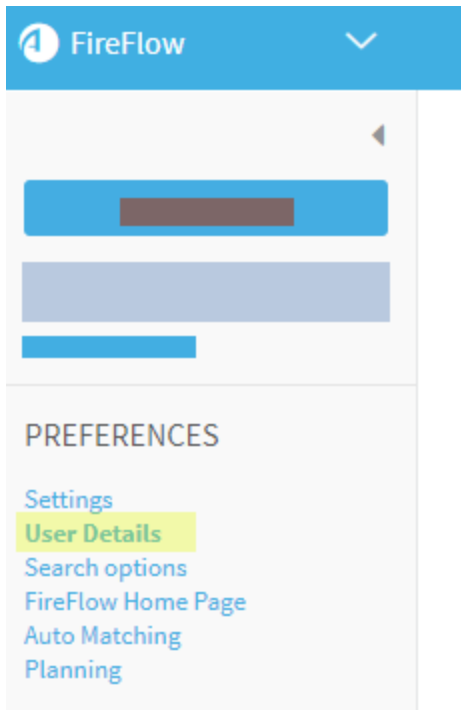
> **Note:** If the system is configured to import user information from an LDAP server upon each login, FireFlow reminds you that changes to these settings may be overridden then next time you log in.
>
> In such cases, you must make these changes in the LDAP server instead of FireFlow.

2. Modify the fields as needed. For details, see [User preferences fields](#).

3. Click **Save Preferences**.

User preferences fields

Enter details in the following fields as needed.

Identity fields

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

Location fields

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

Phone number fields

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

Additional information

This area displays any custom fields defined for your system.

Signature

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

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: • **Basic** • **Standard** • **Multi-Approval** • **Parallel-Approval** • **Automatic Traffic Change** 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. By default, related to the **Traffic Change Request (IPv6)** workflow. For details, see IPv6 traffic change workflow.
Multicast traffic change requests	Used to create multicast traffic change requests, for Cisco devices only. By default, related to the **Traffic Change Request (Multicast)** workflow. For details, see Multicast traffic change workflow.
Web filter change requests	Used to request changes in web filtering. By default, related to the **Web-Filter** workflow. For details, see Web filtering change workflow.
New device configuration change requests	Used to create requests for new device configurations. 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. By default related to the **Generic** workflow. 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. By default, related to the **Object Change** workflow. 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. By default, related to the **Object Change Multi Device** workflow. Supported only via API. For details, see [Multi-device object change workflow](#).
Rule Removal requests	Used to create change requests to remove a network policy rule. By default, related to the **Rule Removal** workflow. For details, see [Rule removal workflow](#).
Rule Modification requests	Used to create change requests to modify a network policy rule. By default, related to the **Rule Modification** workflow. For details, see [Rule modification workflow](#).
Recertification requests	Used to create requests to recertify Allow traffic added as the result of a traffic request. Available only to network operations users only. By default, related to the **Request-Recertification** workflow. 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.
	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.
	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.
	Default stages include: Request, Plan, Approve, Review, Implement, Validate, Resolved, and Audit.
IPv6-Traffic	Used for requests involving IPv6 traffic, for Cisco devices only.
	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.
	If the rule is no longer relevant, a Rule Removal change request is created to remove it.
	Default stages include: Request, Certify, Implement, Validate, Resolved, and Audit.
Multicast-Traffic	Used for requests for Multicast traffic changes, for Cisco devices only.
	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. 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. Default stages include: Request, Approve, Implement, validate, Resolved, and Audit.
Object-Change-Multi-Device	Used for requests to change device objects on multiple devices. Available only for change requests opened via API. Default stages include: Request, Plan, Approve, Implement, Validate, Resolved, and Audit.
Rule-Removal	Used for requests to remove or disable device rules. 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. Default stages include: Request, Approve, Implement, Validate, Match, Resolved, and Audit.
Bulk-Rules-Addition	Used for requests to add many rules to a device. 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. No device change planning or matching device changes to the request are required. 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. 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. For details, see Request changes.
Plan	Performed by network operators.
Approve	Performed by network operators or information security officers.
Review	Performed by controllers only.
Implement	Performed by network operators only.
Validate	Performed by network operators only.
Match	Performed by information security officers.
Resolved	Performed by network operators only.

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:

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.

   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. [Details ➡]
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.

Show All Risks

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

[Check All] [Clear All]   [Select additional users to notify]

   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:	Choose File No file chosen **Add More Files**

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 ⬈ Find out why

Recalculate   ✏ Edit

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.

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.
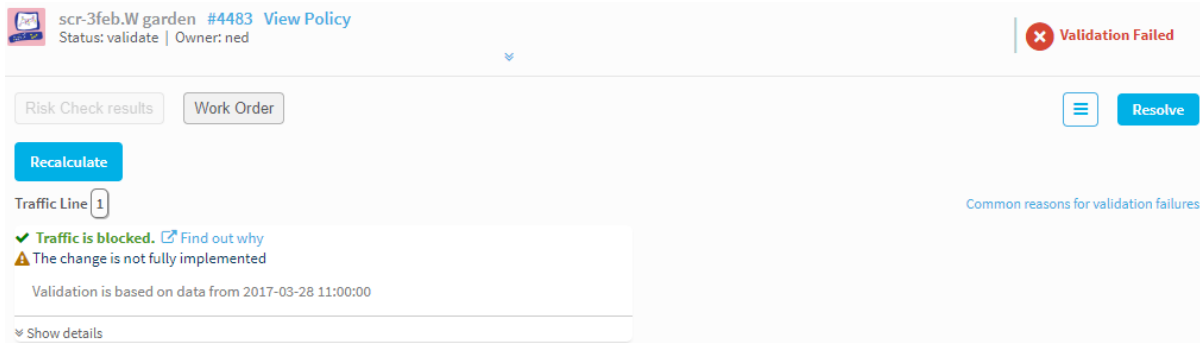
2. The validation process checks both that the requested traffic is not allowed or blocked, and also that the changes were done according to the work order.

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   Customize

   ▸ 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).
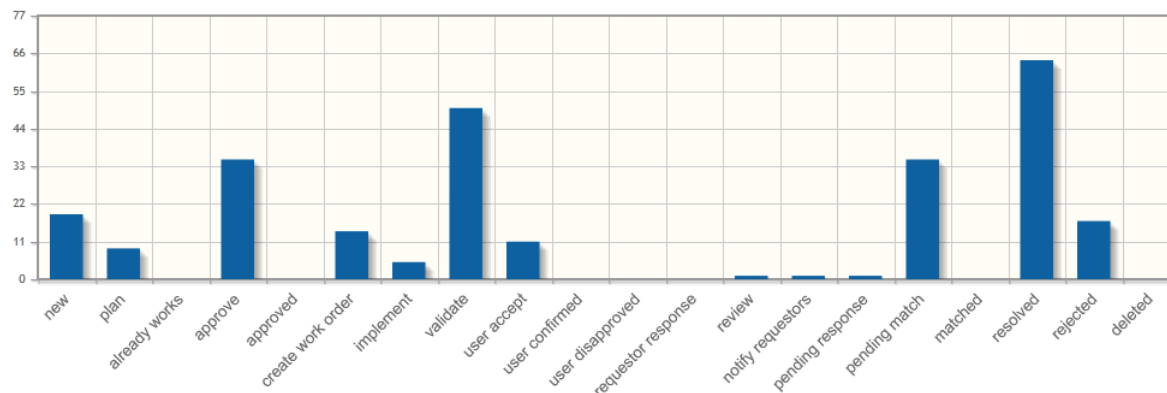
IPv6 traffic change workflow

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 ○ Drop

Show NAT

+ Add Traffic

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   Customize

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 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 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 GP_NW_SLI_LAN	NW_Garden_ICN_003	TCP https	accept	FireFlow #322: Added by Sally

Implementation Notes   Edit

Implementation   *(no value)*
Notes:

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:

> **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:

Rules that contain host group GP_Dthomson   Export:

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)			★ Any	tcp-1863-MSM-Messenger NetMeeting	✅ accept	FireFlow #344: MicroSoft Windows Update	0	N/A	0.000%	rose_checkpoint	
2	49 (Global)			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.

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:

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 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	

Check All   **Clear All**   **Select additional users to notify**

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.

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.

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:

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. [Details ➜]
   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.

   Show All Risks

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.


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.
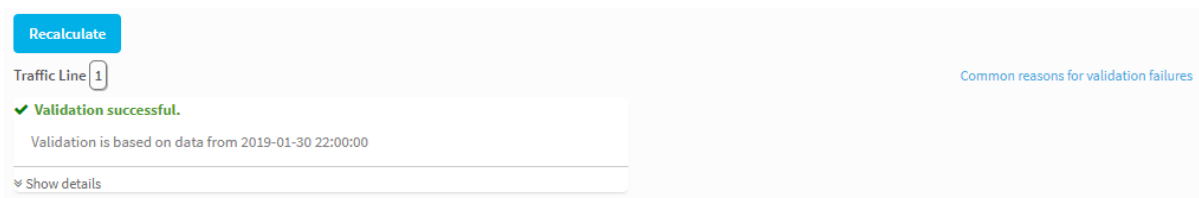
2. If validation indicates that the specified rule was not modified, then the network operations user re-initiates the Implement stage.

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	Customize
▸ 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:

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.

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.

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

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:	Choose File No file chosen Add More Files	

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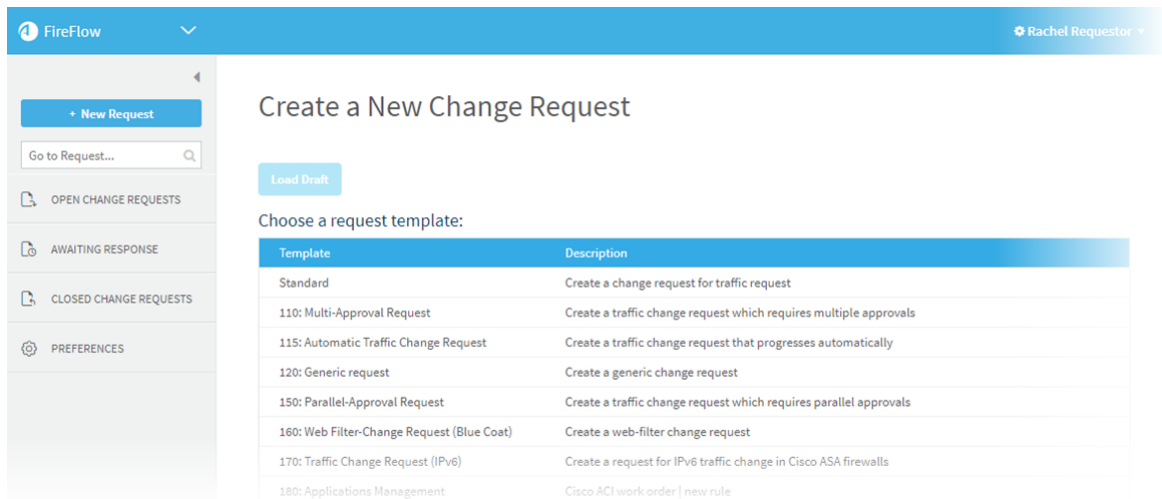
All FireFlow users can log in a submit a change request directly from FireFlow. The user interface will look different for FireFlow requestor users, displaying only the options available to them.

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:

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

Back   Save Draft   Next

*▼ General

Subject   Owner

Change request justification   Requestor*
                                                 rachel@mycorp.com

Due   Expires

Attachments   Device Name
+ Add files...

*▼ Traffic

Set traffic values   Import traffic from csv

1   Source ❓   Destination ❓   Service ❓   Action
     Type or select   Type or select   Type or select   Allow

     User ❓   Application ❓
     any ✕   any ✕

     ▸ NAT settings ❓

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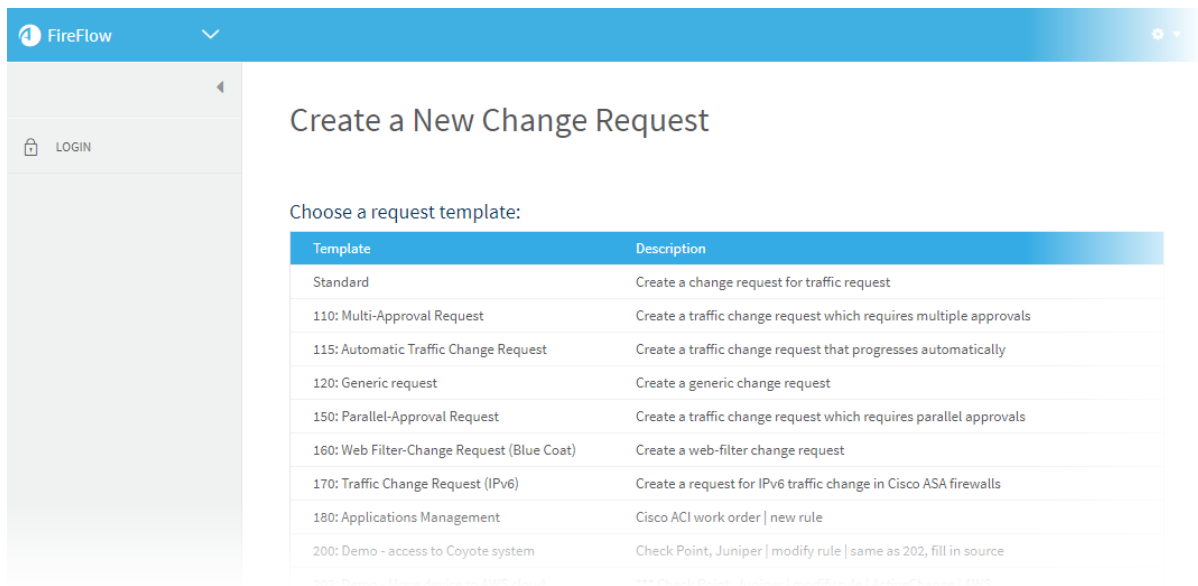
2. Click the name of the template you want to use. For more details, see [Request templates and workflows](#). If you have questions about custom templates or

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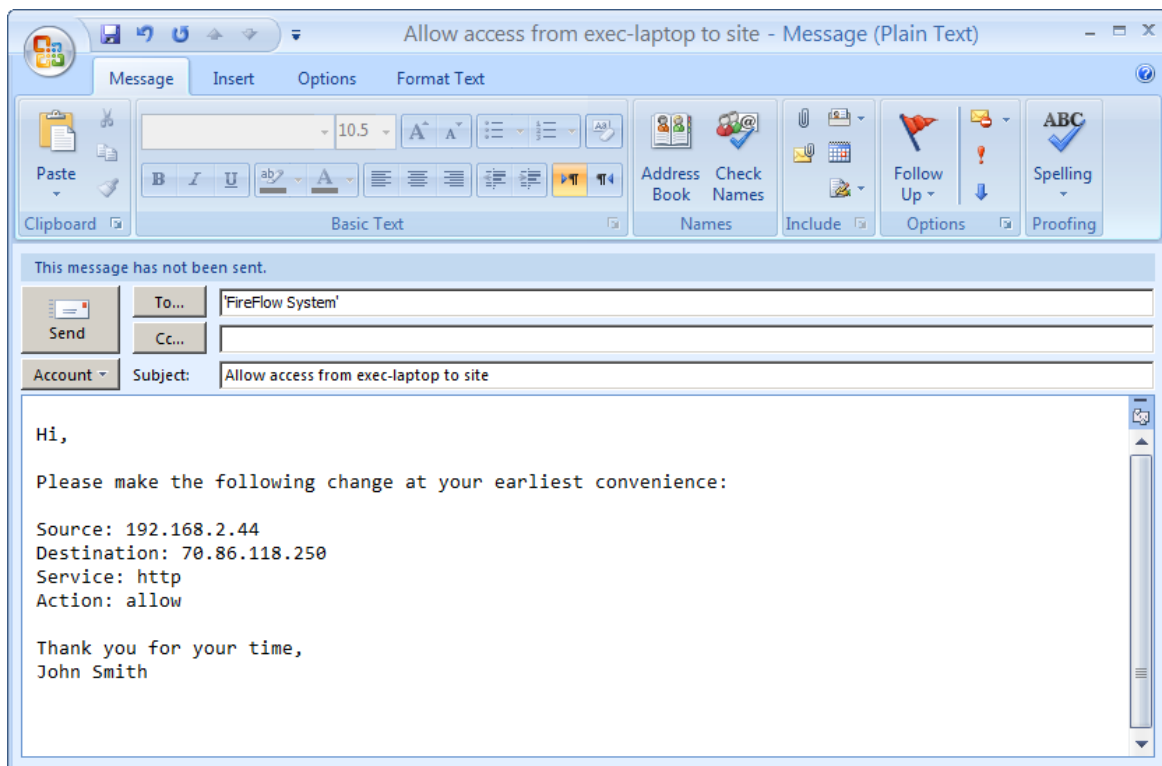
FireFlow creates your request and sends you an email confirmation. Your email text and any technical details specified is added to the change history.

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:

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. **Note:** This field is optional.
Due	Specify the date by which this change request should be resolved, by doing 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". **Note:** This field is optional.
Describe the issue	Type a free text description of the issue. 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. **Note:** This field is optional.

Name	Description
Attach File	To attach a file to your request, 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**. 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. • To add more files, click **Add More Files**. **Note:** This field is optional.
Requestor	In the Requestors Web Interface, this field displays your email address and is read-only. **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: • 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. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**. **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. The FireFlow change request generated for your request will be linked to the external system change request. **Note:** This field is optional.
Workflow	The change request's workflow. **Note:** This field is read-only.
From Template	The change request's template. **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. **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. **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: • 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. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**. **Note:** This field is optional.
Expires	Specify the date on which this change request will expire, by doing 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. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**. **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. **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**. This field is only relevant for Check Point and Palo Alto devices.
Destination	Specify the traffic destination(s). For details, see Change request wizards. 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. 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. 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. The default value is **Any**. 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: **Allow:** Allow the connection. **Drop:** Block the connection. **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. The **Source NAT**, **Destination NAT**, **Port Translation**, and **NAT Type** fields appear. Depending on system customizations, the **Source after NAT**, **Destination after NAT**, and **Port after Translation** fields may appear as well.
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. 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. 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. 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**). 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. 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. **Required Headers:** • Source • Destination • Service **Optional Headers:** • User. If this header is not present, the value defaults to "any". • Application. If this value is not present, the value defaults to "any". • Action. If this header is not present, the value defaults to "allow". Any other headers included in the CSV file are ignored. **Note:** All headers are not case sensitive. 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.
	The FireFlow change request generated for your request will be linked to the external system change request.
	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.
	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.
	Note: This field is optional.
Due	Specify the date by which this change request should be resolved, by doing 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. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**.
	Note: This field is optional.

Name	Description
Expires	Specify the date on which this change request will expire, by doing 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. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**. **Note:** This field is optional.
Request	Use this area to specify the traffic changes you would like. 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 🗑 . Due to system customizations, this area may differ in the following ways: • NAT fields may not appear. • The following additional NAT fields may appear: **Source after NAT**, **Destination after NAT**, **Port after Translation**. • The **Source**, **Destination**, and/or **Service** fields may be followed by a custom field. For information about these fields, consult with your FireFlow administrator. • 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: • Type the IP address, IP range, network, or device object. • Use the **Choose Source Wizard**. For details, see [Change request wizards](#). **Note:** Only IPv6 addresses are supported. You cannot mix IPv6 and IPv4 addresses in the same workflow.
Destination	Do one of the following: • Type the IP address, IP range, network, device object. • Use the **Choose Destination Wizard**. For details, see [Change request wizards](#). **Note:** Only IPv6 addresses are supported. You cannot mix IPv6 and IPv4 addresses in the same workflow.
Service	Do one of the following: • Type the device service or port for the connection (for example "http" or "tcp/123"). For more details, see [Traffic-based change request fields](#). For information on how to use non-TCP/UDP/ICMP protocols, [Supported layer 3 protocols](#). • 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: • **Allow:** Allow the connection. • **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. The **Source NAT**, **Destination NAT**, **Port Translation**, and **NAT Type** fields appear. 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. 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. 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. 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**). **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. **Note:** This field is read-only.
Workflow	The change request's workflow. **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. The FireFlow change request generated for your request will be linked to the external system change request. **Note:** This field is optional.
Describe the issue	Type a free text description of the issue. 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. This field is optional.

Name	Description
Attach file	To attach a file to your request, 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**. To add more files, click **Add More Files**. **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. 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. This field is optional.
Due	Specify the date by which this change request should be resolved, by doing 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. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**. This field is optional.

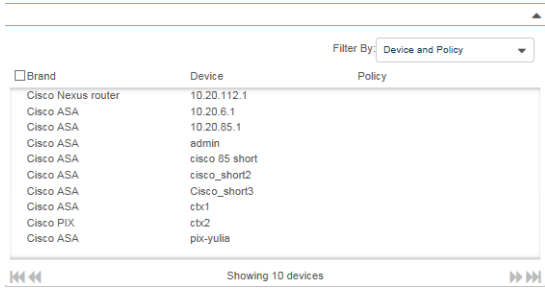| Name	Description
Expires	Specify the date on which this change request will expire, by doing one of the following: • Click ⊞, and select the desired date in the calendar that appears. To navigate to different months in the calendar, click **Prev** and **Next**. • Type the desired date in the field provided. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**. 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. 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 🗑 . Due to system customizations, this area may differ in the following ways: • NAT fields may not appear. • The following additional NAT fields may appear: **Source after NAT**, **Destination after NAT**, **Port after Translation**. • The **Source**, **Destination**, and/or **Service** fields may be followed by a custom field. For information about these fields, consult with your FireFlow administrator. • 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: • Type the IP address, IP range, network, device object, or DNS name of the connection source. • Use the **Choose Source Wizard**, as described in Using the Choose Source/Destination Wizard (see Change request wizards). To enter multiple values, press Enter. A new field appears for this source. Note: You cannot mix regular traffic and multicast in the same workflow. 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: `usergroup@host` Where: • *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. Note: LDAP user groups are only supported for devices configured to use OPSEC data collection. • *host* is the IP address, IP range, network, device object, or DNS name of the connection source. For example: **group1@1.2.3.4**, **group1@RNDNetwork**, or **group1@Any**. 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: • Type the IP address, IP range, network, device object, or DNS name of the connection destination. • Use the **Choose Destination Wizard**, as described in Using the Choose Source/Destination Wizard (see Change request wizards). To enter multiple values, press **Enter**. A new field appears for this destination. **Note:** You cannot mix regular traffic and multicast in the same workflow.
Service/Application	Do one of the following: • Type the device service or port for the connection (for example "http" or "tcp/123"). For details, see Supported layer 3 protocols. • Type the name of an application as defined in your Palo Alto or Check Point device. • Use the **Choose Service Wizard**. For details, see Change request wizards. To enter multiple values, press **Enter**. A new field appears for this service. **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: • **Allow:** Allow the connection. • **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. The **Source NAT**, **Destination NAT**, **Port Translation**, and **NAT Type** fields appear. Depending on system customizations, the **Source after NAT**, **Destination after NAT**, and **Port after Translation** fields may appear as well. Click NAT settings again to hide the settings.
Source NAT	Type the source NAT value, if the connection's source should be translated. Note: If the **Source after NAT** field appears below this field, then you must type the source NAT value *before* translation.
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. 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. 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**). **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. The FireFlow change request generated for your request will be linked to the external system change request. This field is optional.

Name	Description
Device Name	Click in the **Device Name** box. The device selection dialog box appears with a list of available Cisco devices.

To filter, in the **Filter By** list, select **Brand**, **Device**, **Policy**, **Device and Policy**, or **Selected**.

To select all devices for a brand, select the **Brand** check box.

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.

To move forward and backward in the device list, click the and icons.

Selected devices appear in the **Device Name** box.

Click the up arrow to close the dialog box.

Name	Description
Change request justification	Type a free text description of the issue. 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. This field is optional.
Attachments	To add attachments, click **Add files**. The **Choose File to Upload** dialog box opens. Browse to the desired file, and click Open. To select multiple files, press CTRL while selecting. This field is optional.

Web-filter change request fields

Name	Description
Requestor	In the Requestors Web Interface, this field displays your email address and is read-only. 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. This field is optional.
Due	Specify the date by which this change request should be resolved, by doing 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. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**. This field is optional.
Expires	Specify the date on which this change request will expire, by doing 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. FireFlow supports most relative and absolute formats, such as **yyyy-mm-dd**, **mm/dd/yyyy**, **Mon dd yyyy**, **next week**, or **now + 3 days**. 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: • Type the name of the user or user group that should be allowed/denied access to a URL. • 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: • Type URL's Web filtering category. • Use the **Choose Category Wizard.** For details, see Change request wizards. **Note:** When creating a change request via the Blue Coat **Blocked** page, this field is automatically filled in.
Action	Select the device action to perform for the connection. This can be any of the following: • **Allow:** Allow the connection. • **Block:** Block the connection.
Add More Web Filtering	To add more connections to the request, click this option and complete the fields.
🗑	To remove additional connections from the request, click this option next to the desired traffic.
From Template	The change request's template. This field is read-only.
Workflow	The change request's workflow. 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. The FireFlow change request generated for your request will be linked to the external system change request. This field is optional.
Describe the issue	Type a free text description of the issue. This description will be reviewed by the network operations and information security users who handle your change request. It will also be added to the change request history. This field is optional.
Attach file	To attach a file to your request, 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**. To add more files, click **Add More Files**. 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}	

Cancel Set Values

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:

2. Do one of the following:

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

3. Click **OK**.

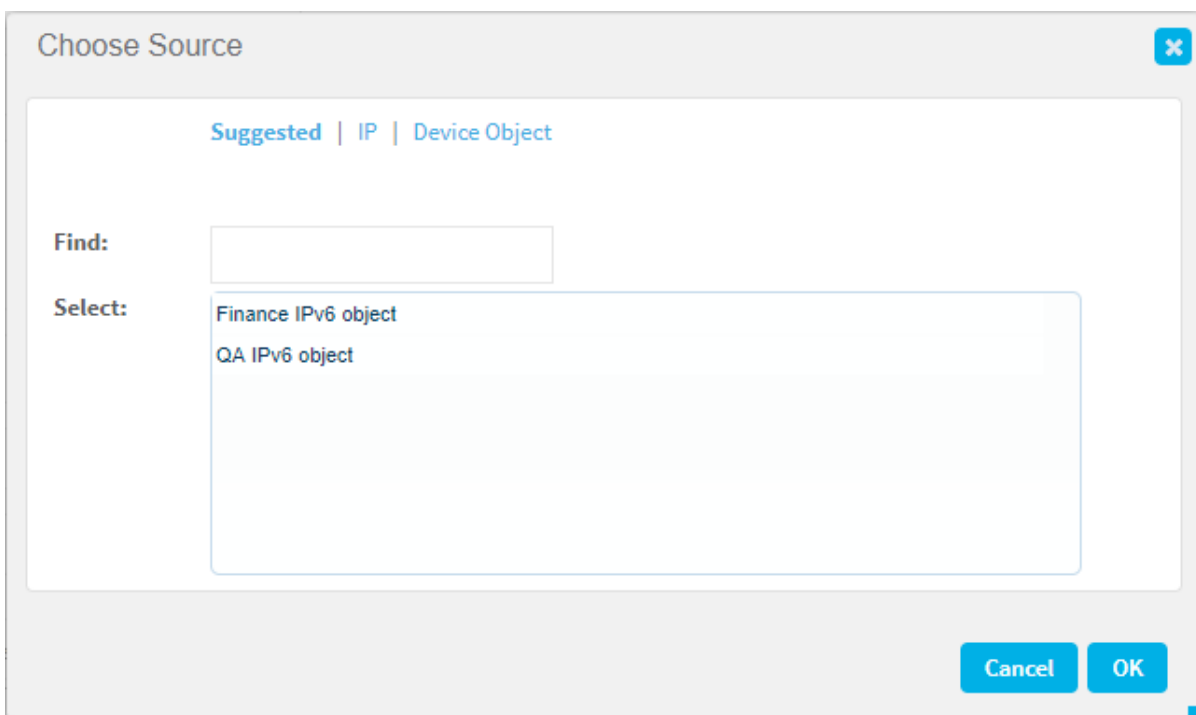If you entered a value in the **IP Address** tab, the wizard validates the entered value.

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.

2. Do one of the following:

Select from a list of device objects or suggestions	Do the following: - To search for a source/destination, in the **Find** field, enter any part of the source/destination's name (case-insensitive). - In the **Select** list, select the item you want to use as the source/destination.
Enter a specific value	Do the following: a. Click the **IP** tab. b. Do one of the following: **Specify an IP address**. Click **IP** and enter your IP address. **Specify an IP range.** Click **IP Range** and enter your IP range. **Specify a network**. Click **CIDR** and enter your network value. **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: a. Click the **Device Object** tab. b. To search for a device object, do the following: 　○ In the **Search** dropdown list, select the device in which the object is located. 　○ In the **For** field, enter any part of the object's name. The **Select** list displays all source/destinations containing the string you entered. To navigate between search result pages enter the page number you want to jump to in the **Page** field. 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.
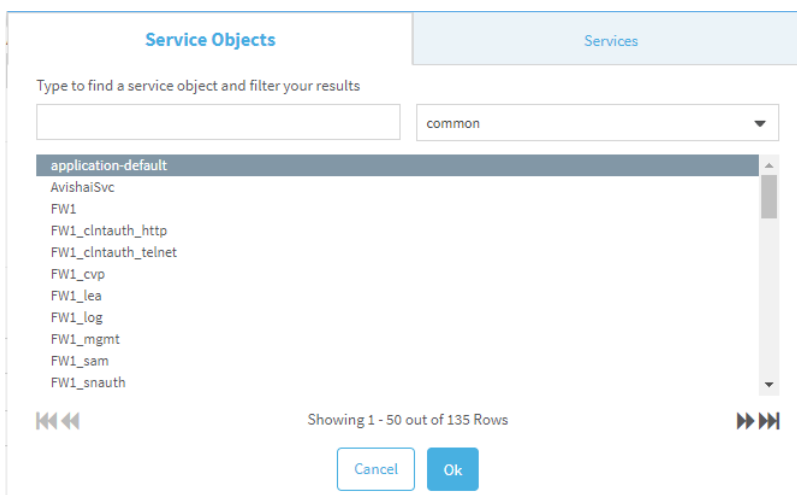
These wizards differ for IPv4 and IPv6 traffic, and may differ further, depending on your system configuration.

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.

2. Do one of the following:

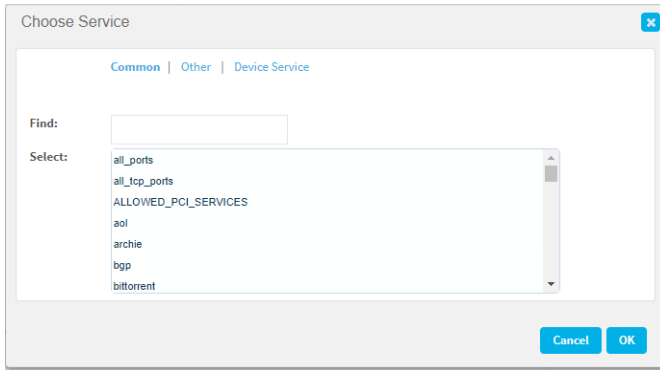| Select the service from a list of services	Do the following: a. In the dropdown menu, select the type of service you want to view. By default, only common service objects are displayed. b. To search for a service object, enter any part of the object's name in the search field (case insensitive). c. Select the service object you want to use from the list displayed.

Specify a custom service	Do the following:
	
	a. Click the **Services** tab.
	
	b. Enter the service in one of the following formats:
	
	    protocol/port, to indicate a single service.
	
	    protocol/*, to indicate any port for the specified protocol
	
	    protocol/port1-port2, to indicate a range of ports for a specific protocol
	
	    *, 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.

2. Do one of the following:

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

Select a service from a list of services defined on devices	Do the following: a. Click the **Device Service** tab. b. In the **Search** area, select a device from the dropdown list. 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**. d. In the **Select** list, select the desired service. **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.
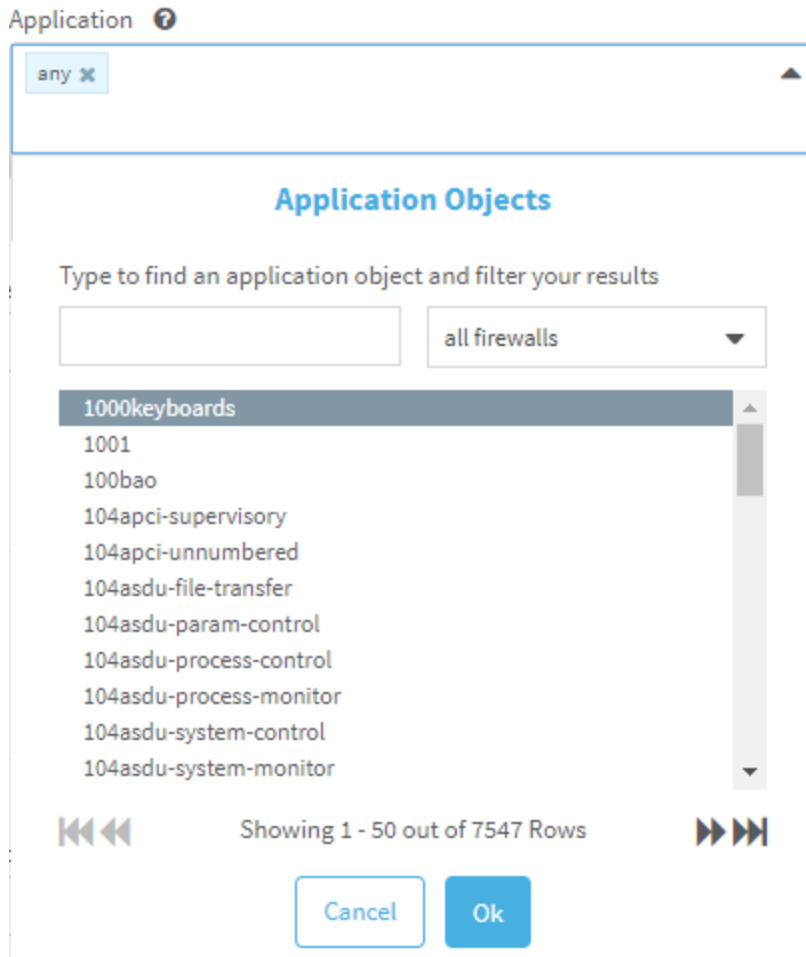
Choose Application wizard

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   ▶▶ ⏭

Cancel   Ok

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**.

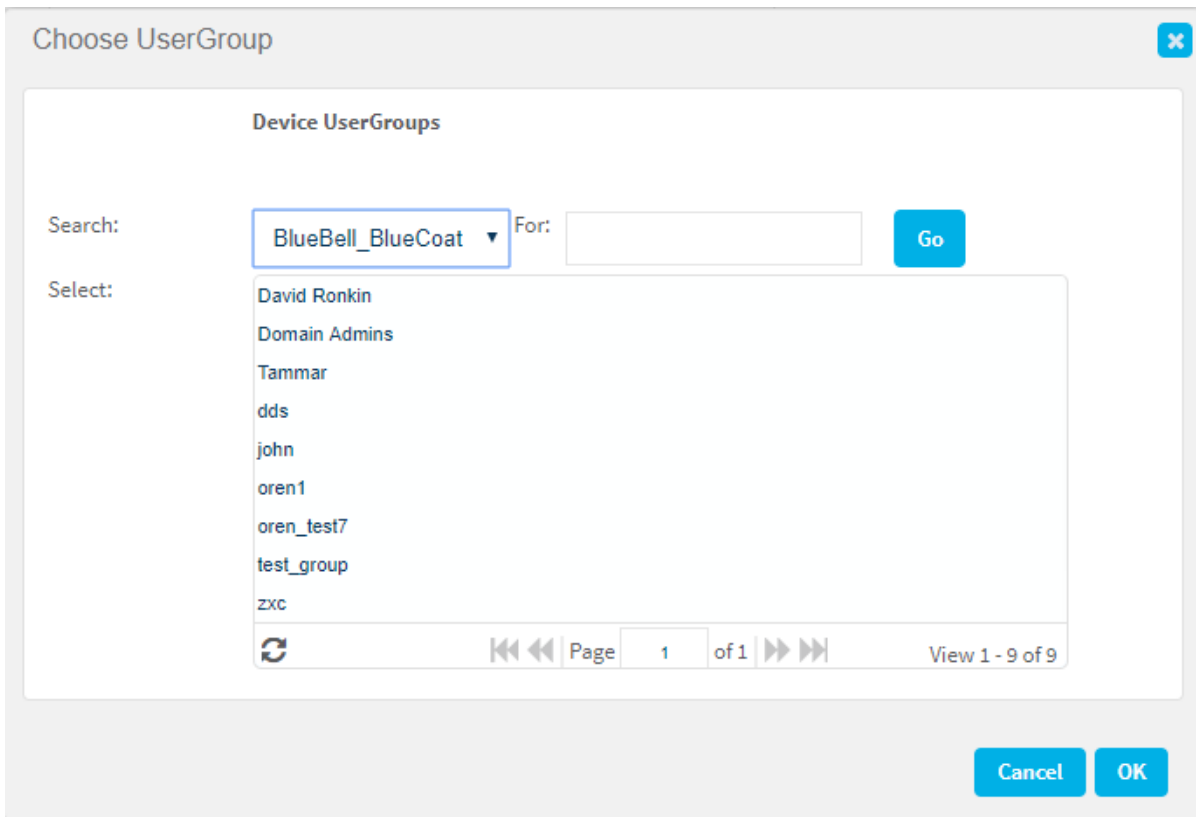The application appears in the **Application** field.

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.

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.
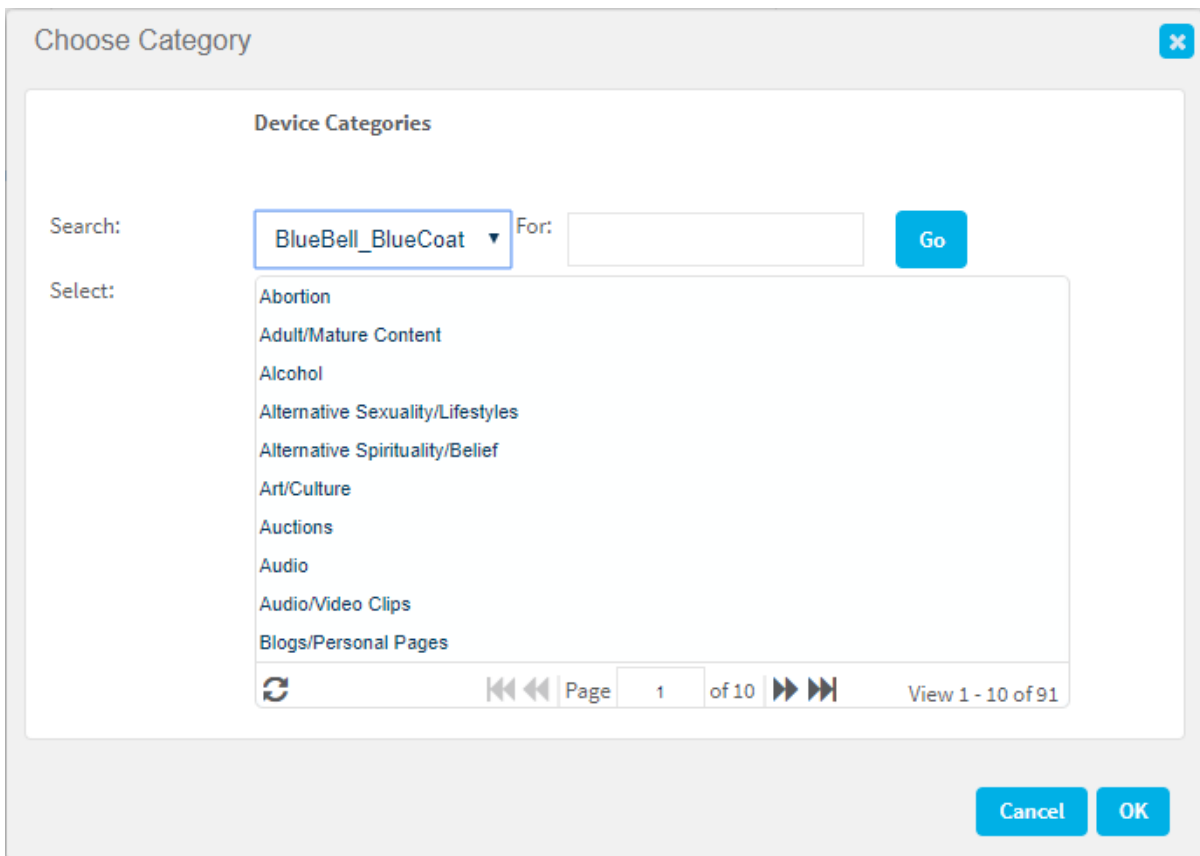
Choose Category wizard

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.

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.
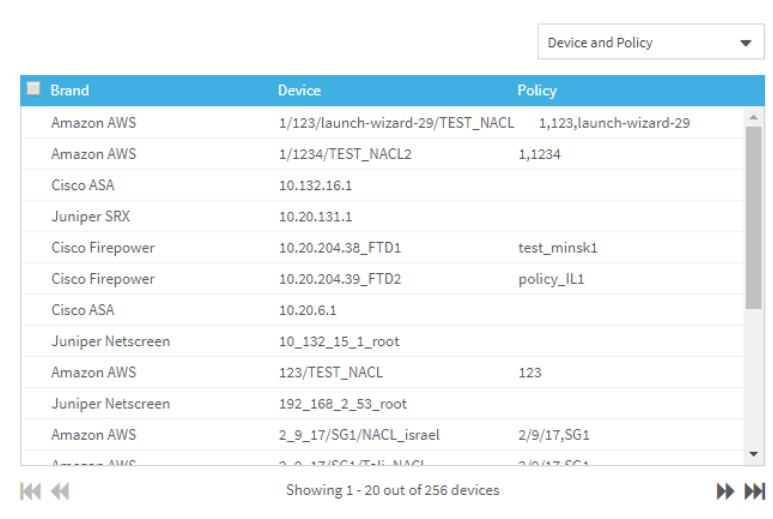
Select Devices wizard

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
		Device and 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/T-li_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.

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:
	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.
	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.
	3. When ready, the network operations user notifies the requestor that the changes were implemented.
	4. The requestor then verifies that the desired result was achieved.
	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: 1. A network operations user validates the implemented changes against the change request, to verify that the specified object change has been made. 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. 3. Next, the network operations user notifies the requestor that the changes were implemented. 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: 1. A network operations user validates the implemented changes against the change request, to verify that the work order recommendations have been implemented.
Rule modification change requests	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.
Recertification change requests	3. The network operations user then resolves the change request.

Multi-device object change requests	The following process occurs:
	1. The network operations user does not validate changes. Instead, the network operations user immediately notifies the requestor that the changes were implemented.
IPv6 traffic change requests	2. The requestor then verifies that the desired result was achieved.
Multicast traffic change requests	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.
Web filtering change requests	

For details, see:

- [Verify change request results](#)
- [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:

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.
	• 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.
	• 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.
	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.
	If the rule contains more traffic than recommended, FireFlow indicates this for you so that you can take any action, as required.
	For example:
	Traffic Line 1 ✔ **Traffic is allowed.** ⬀ Find out why ✖ The rule contains more traffic than recommended Validation is based on data from 2019-08-09 01:52:09
	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. - **"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. • **"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.

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.

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.

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.

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.

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](#).

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.

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.

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:

- [View change requests](#)
- [Search for change requests](#)
- [Verify change request results](#)
- [Respond to change 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.

> **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. 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:

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. 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.

> **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.
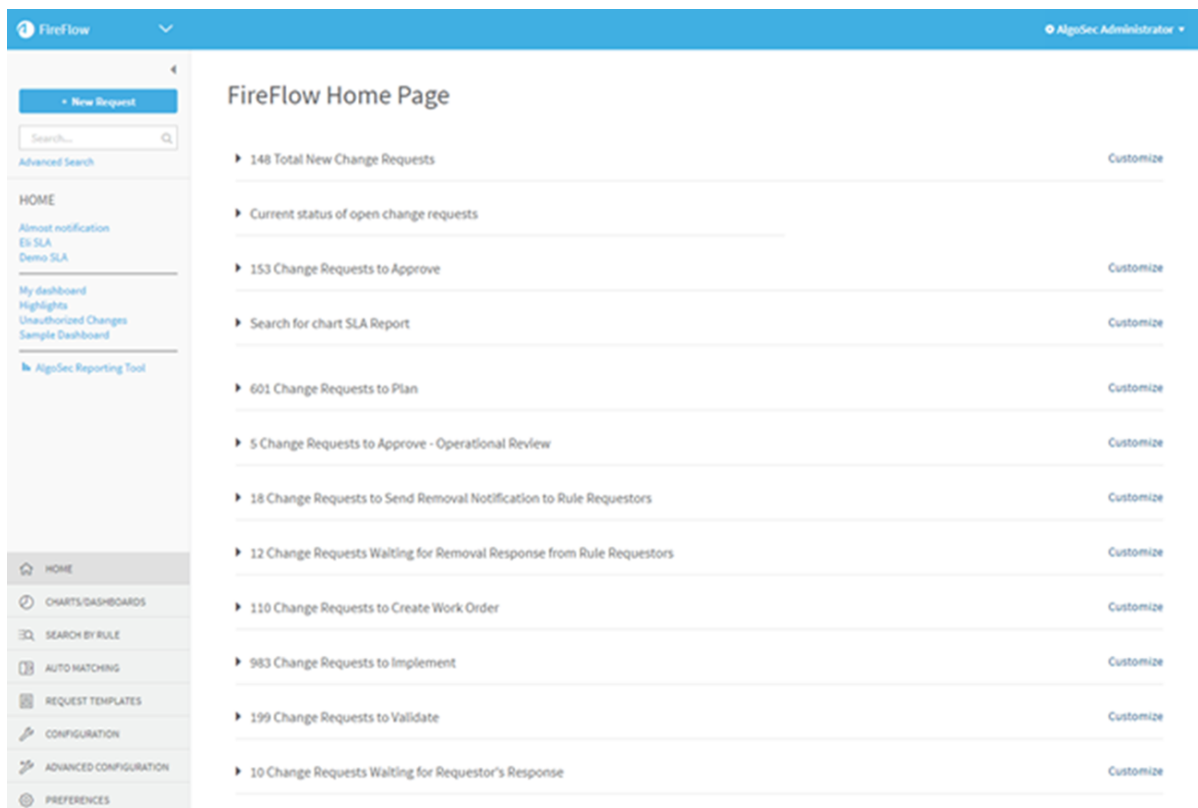
Note: By default, only lists that are relevant to your user role will appear in your **Home** page.

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.

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.
	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.
	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.
	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.
	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.
	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.
	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.
	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.
	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.
	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.
	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.
	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".
	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.
	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.

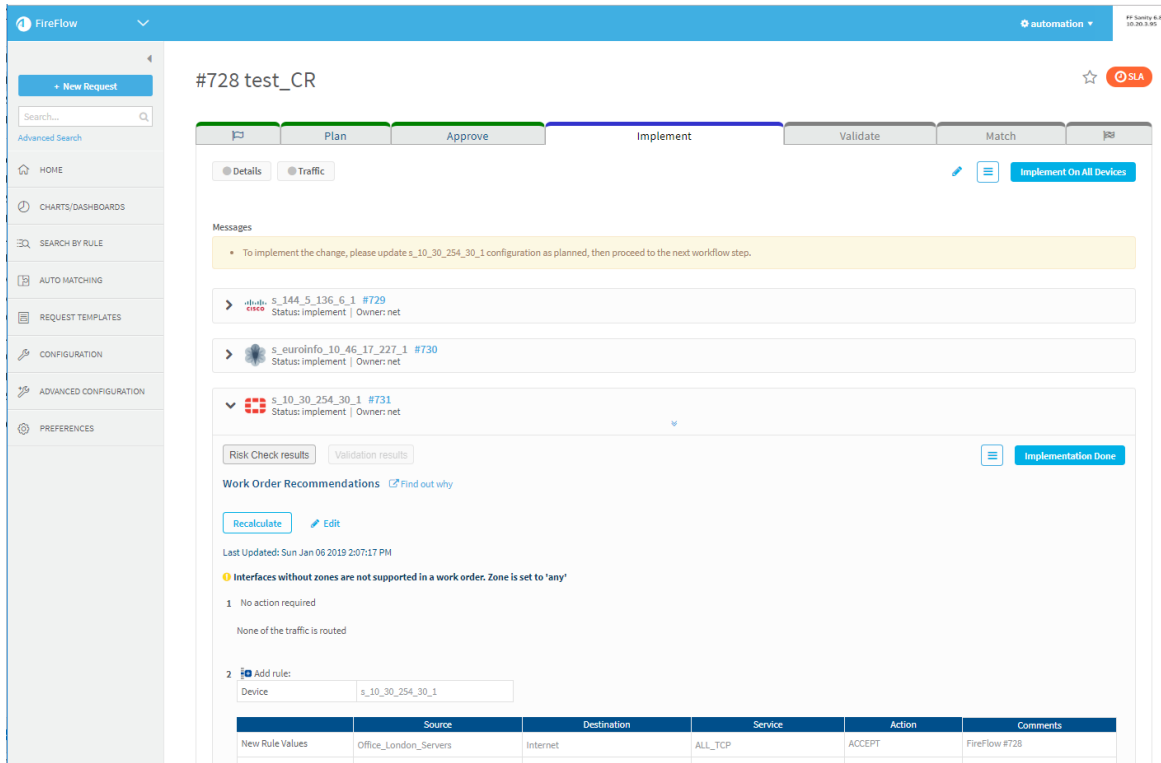| Change Requests to Expire in the Next 30 days	A list of change requests in the system that will expire between today and 30 days from today. This list only appears for users with network operations or administrator role.
Total New Change Requests	A list of all change requests in the system that are 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. 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.

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. The status bar maps the stages in the lifecylce from left to right. • The current stage appears in **blue**, completed stages appear in **green**, and future stages appear in **grey**. • **An empty flag** indicates that the request is new; **a checkered flag** indicates that the request is resolved. • Click a previous stage to display a read-only view of the request data for that stage. For more details, see Change request statuses.

Relevant device or policy	The device policy is displayed with the request's status, owner, and ID.
	For Palo Alto and Check Point policies, the **View Policy** link appears.
	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:
	• **IP**. The device's IP address.
	• **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.
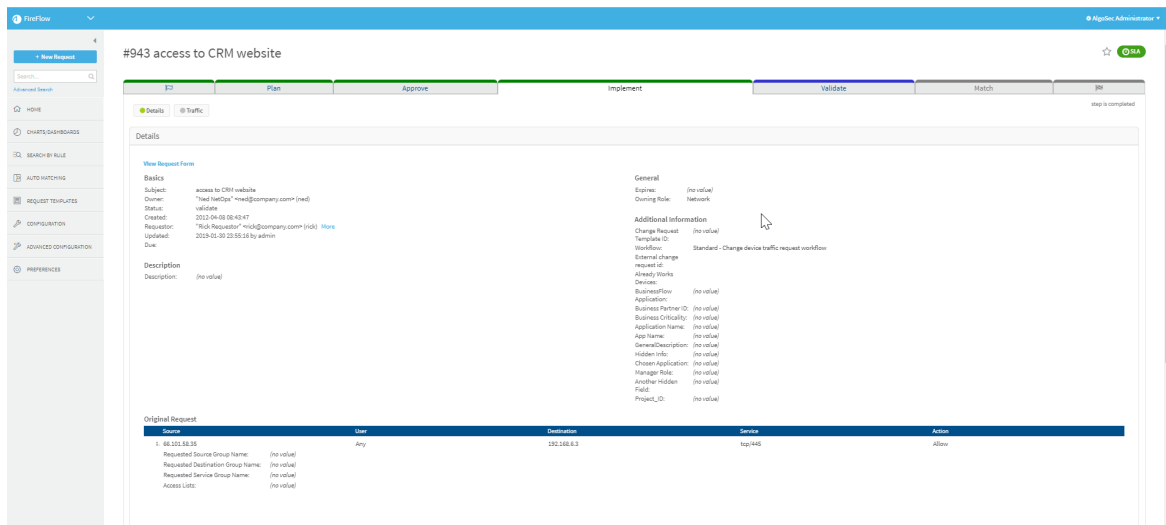
   For information about fields, see Details Fields (see [Details Fields](#)).

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.

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:
	a. Click ▶ next to the desired device to display the device's change request information.
	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**.
	If the information has not been calculated, the button will be disabled.
	b. Click the desired button.
	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:
	a. In the Change Request Lifecycle Status Bar, click **Plan**.
	The read-only view of the **Plan** tab appears.
	b. Click **Initial Plan results**.
	The initial plan PDF appears.
	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.
	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. **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>`.
	For example, "bobsnetops<bobsnetops@mycompany.com>".
	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>.
	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:
	• A date
	• **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. 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. 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. 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. 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. This field is optional.
Referred to by	The ID numbers of change requests that refer to the change request, separated by spaces. 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. 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. 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:
	• **Allow:** Allow the connection.
	• **Drop:** Block the connection.
Source NAT	The source NAT value to which the connection's source should be translated.
	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.
	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.
	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.
	Each change request is represented by its ID number, followed by its current status. For details, see Change request statuses.
	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. 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.

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.

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.
	For more details, see Request templates and workflows.
Device Name	The device for which this change request is relevant.
	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.
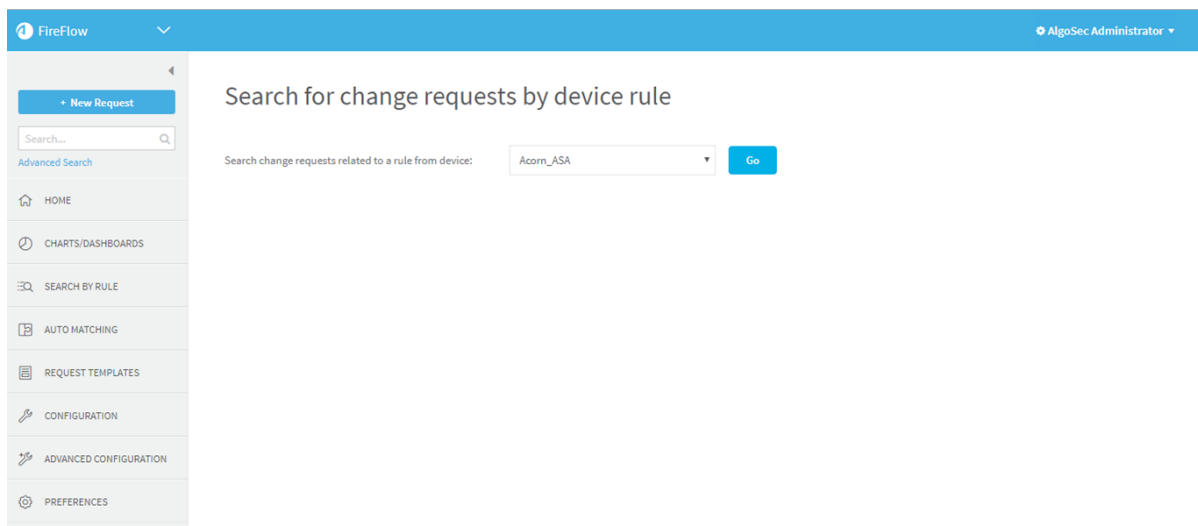
2. Select the desired device from the drop-down list and click **Go**.

    The **Search for change requests by device rule** page appears displaying all rules and objects for the device.

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.
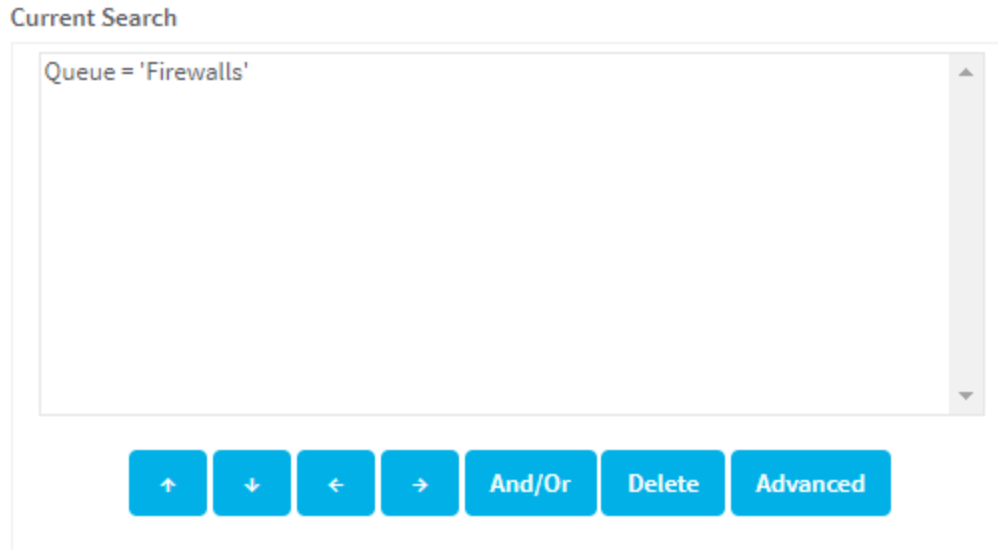
      For example: **Owner is johnS (John Smith)**

      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.

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.
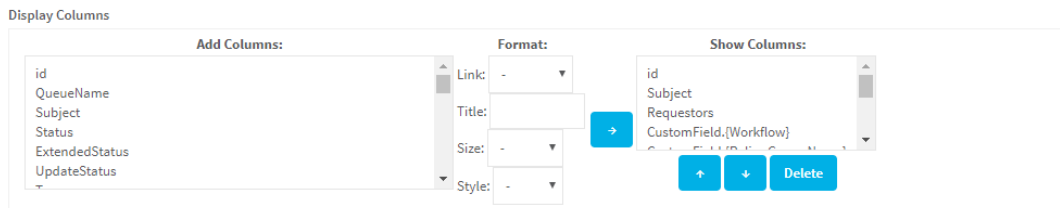
   b. For each column you want to appear in the search results, do the following:

i. In the **Add Columns** box, select a column you want to appear.

ii. Complete the fields in the **Format** area. For details, see <u>Advanced search column format fields</u>.

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.

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.

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: • 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".
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: • 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".

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: • Allow • Drop • 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: • A role name. • __USER_GROUPS__. All roles of which you are a member. 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: • A role name. • __USER_GROUPS__. All roles of which you are a member. 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. 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: • Unused Rule • Covered Rule • Special Case Rule 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: • **Stand by:** Standing by for the change requestors' responses. This status continues until the responses are received, or the due date passes. • **In process:** The change request is open. • **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. 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. 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. 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. 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. 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. 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. 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. 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. 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. 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. 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: • -. Items in the column are not linked. • **Take:** Clicking on an item in the column assigns you the relevant change request. • **Display:** Clicking on an item in the column displays the relevant change request.
Title	Type the name of the column.
Size	Specify the text size of items in the column, by selecting one of the following: • -. Items in the column appear in medium-sized text. • **Small:** Items in the column appear in small-sized text. • **Large:** Items in the column appear in large-sized text.
Style	Specify the font style of items in the column, by selecting one of the following: • -. Items in the column appear in normal font. • **Bold:** Items in the column appear in bold font. • **Italic:** Items in the column appear in italicized font.

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.

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" <ned ▾

- 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'
```

[↑] [↓] [←] [→] [And/Or] [Delete] [Advanced]

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.
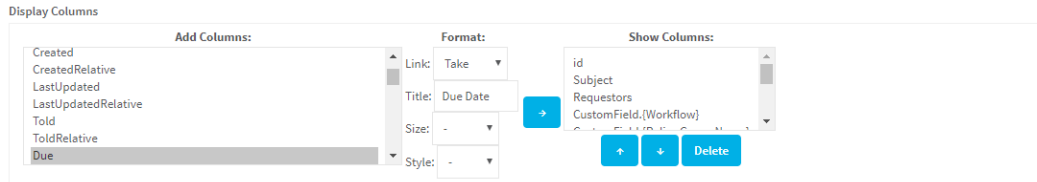
f. Ned clicks **Search** to start searching for Debbie's change request.

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:

   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. • 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. • 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. 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. If the rule contains more traffic than recommended, FireFlow indicates this for you so that you can take any action, as required. For example: Traffic Line 1 ✔ Traffic is allowed. ☑ Find out why ✘ The rule contains more traffic than recommended Validation is based on data from 2019-08-09 01:52:09 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. • **"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. • **"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.

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.

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.
	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:
	- 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. - 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:
	- 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. - If check boxes appear under the text box, select the desired email addresses.
Subject	Type the subject of the message.
	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:
	- Type the path to the file in the field provided. - Click **Browse**, browse to the desired file, and click **Open**.
	To add more attachments, click **Add More Files**.
	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.
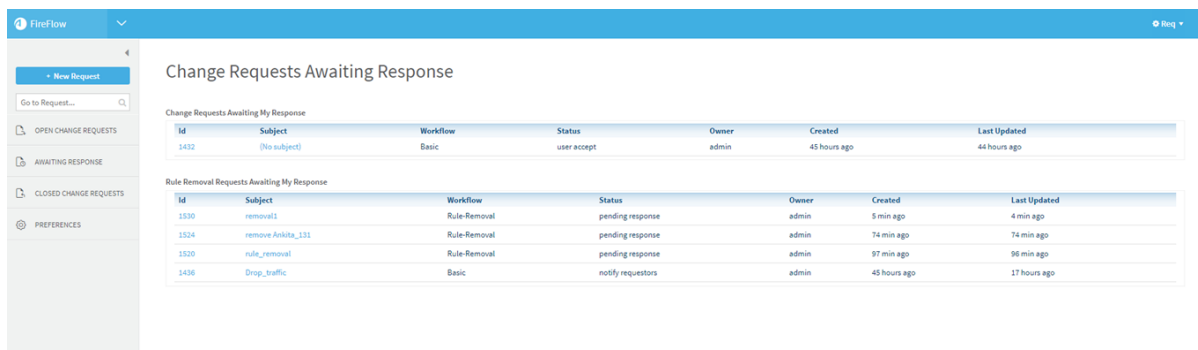
Do one of the following:

Respond to rule removal requests

Do the following:

1. In the main menu, click **Awaiting Response**.

    The **Change Requests Awaiting Response** page is displayed.

2. In the **Rule Removal Requests Awaiting My Response** list, click the change request.

    The **Rule Removal Request** page is displayed.

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.

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.

2. In the **Change Requests Awaiting My Response** list, click the change request.

   The **Traffic Removal Request** page is displayed.

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.

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.

Send us feedback

Let us know how we can improve your experience with the Requestor Guide.

Email us at: techdocs@algosec.com

> **Note:** For more details not included in this guide, see the online ASMS Tech Docs.