



AlgoSec AppViz

Software Version: A30.10

User Guide

View our most recent updates in our online [ASMS Tech Docs](#).

Document Release Date: 29 March, 2020 | **Software Release Date:** April 2020

Legal Notices

Copyright © 2003-2020 AlgoSec Systems Ltd. All rights reserved.

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

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

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

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

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

Specifications subject to change without notice.

Proprietary & Confidential Information

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

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

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

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

Contents

Welcome to AppViz	10
Access AppViz	10
AppViz main menu	11
Logins and other basics	13
Supported browsers	13
Log in to ASMS	13
View ASMS product details	16
Log out of ASMS	17
Business applications	19
View applications	19
Search for applications	20
Add applications	26
Application workflow	30
Application dashboard	30
Application DASHBOARD tab interface	31
Apply application drafts	37
Discard application drafts	39
Resolve active applications	40
Decommission applications	41
Export application content to PDF	43
Clone applications	44
Refresh application connectivity	45
View multiple versions of the same application	46
Edit general application information	47
Edit contact information	47
Application flows	48
Flow types	48
FLOWS tab interface	48
Flow connectivity status	50
Add flows to your application	51

Edit an application's flows	59
Remove flows from your application	60
Subscribe to another application's shared flows	61
Verify flow connectivity	63
Export an application's flows	64
Discover applications	65
Discover applications via AutoDiscovery or Cisco Tetration	65
Export flows directly from AFA	68
Application diagram	70
DIAGRAM tab interface	71
Modify the application diagram	73
Search the application diagram	75
Application change requests	78
CHANGE REQUESTS interface	79
View relevant FireFlow change requests	79
Application vulnerability	80
VULNERABILITY interface	80
Vulnerability assessment ratings	81
Scanned servers	81
Vulnerability scores	83
Application risks	84
Application activity log	85
ACTIVITY LOG interface	86
Filtering Activity Logs	86
Exporting Activity Logs	88
Analyze application impact	88
Application contacts	90
View application contacts	90
Add application contacts	91
Edit an application's contacts	93
Removing an application contact	93

Network objects	95
Manage network objects	95
Abstract objects	95
View a network object	96
Network object dashboard	98
DASHBOARD tab interface	99
Revision information area	99
Object change status	100
Network object actions	101
Object content and status information	102
General Information area	103
Vulnerability Assessment area	103
Add and edit network objects	103
Add a network object	104
Add a new network object to a group	106
Network objects applications	106
APPLICATIONS tab interface	106
View relevant applications	107
Network object change requests	108
Change Requests interface	108
View relevant FireFlow change requests	109
Network object activity logs	109
ACTIVITY LOG interface	109
Service objects	111
View a service object	111
Add a service object	112
Service object DASHBOARD	113
Service object applications	119
Service object change requests	120
Manage network / service objects	121
Edit a network or service object	121

Clone an object	125
Delete an object	126
Replace an abstract network object	127
Update an object's applications	133
Discard changes made to objects	134
Re-apply changes made to objects	136
Projects	138
Project types	138
View a project	139
Project dashboard	141
Manage projects	143
Project interface	143
Start a new project	146
Update a project's applications	151
Edit a project	155
Apply all application drafts	156
Discard a project	158
Close a project	158
Decommission retired servers	158
Export project content to PDF	159
Create an application migration project	159
Plan an application migration project	160
Save an incomplete plan	161
Select applications and network objects	161
Use the Add Applications wizard	168
Migrate network objects	169
Use the network object lookup wizard	171
Add a network object for migration	174
Create an application lifecycle project	174
AppViz administration	181
AppViz users, permissions, and roles	181

Roles and permissions	181
Create new unprivileged users	182
Manage permissions for applications	182
Manage permissions for users	185
Manage user roles	193
Custom fields	204
Add custom fields to flows	204
Custom Field Fields	207
Security zones	208
Define security zones	209
Configure the Internal zone	210
Critical processes	211
Critical Process scope	211
Supported label actions	211
Add a new critical process	212
Edit a critical process	215
Delete a critical process	216
Export all critical processes to CSV	217
Configure applications	217
Manage application expiration	217
Enable application expiration	218
Manage application labels	219
Add a label	221
Edit a label	223
Replace a label	224
Delete a label	226
Customize applications assigned to the PCI label	226
Manage application and user awareness	227
Enable validation for the user field	229
Manage vulnerability assessment scanners	229
Supported vulnerability assessment service providers	230

Vulnerability scanner configuration prerequisites	230
Define general vulnerability assessment settings	230
Add a vulnerability scanner	231
Delete a scanner	232
Run a vulnerability scan	233
Import vulnerability assessment information	234
Customize interactions with AFA and FireFlow	236
Manage application change requests	236
Manage object change requests	240
Logging and notifications	241
View all activity logs	242
Customize email notifications	243
Manage general email settings	245
Discovery settings	247
Configure an AutoDiscovery server	247
Configure a Cisco Tetration server	248
Configure advanced settings	249
AppViz maintenance	250
View AppViz product data	251
Download support data	251
AppViz troubleshooting permissions	252
Update all rule/application associations for AFA	253
Backup and restore AppViz from the CLI	253
Restart AppViz	253
Update or import AppViz data	254
Customize AppViz user interface text	254
Update data via CSV files	255
Supported import data	255
CSV file sources	255
Prepare a CSV file	256
Download a flows CSV example	263

Import CSV data into AppViz	263
Import network object CSV data into AppViz	265
Import CSV data into AppViz via CLI	269
Update objects from a CMDB	270
CMDB import support	270
Select specific custom fields to import	276
Reviewing the last object update	277
Configure advanced AppViz properties	280
Access and edit the user.properties file	280
Advanced AppViz property reference	280
Device objects	294
Manage device objects in AppViz	294
Edit device objects	295
Device editing process	295
Edit a device object from AppViz	296
Synchronize device object definitions	299
Delete a device object	300
Device object change statuses	302
Customize FireFlow object change requests	304
Manage groups with invalid members	306
Manage objects pending creation	307
Update all device objects	308
Update all device objects (GUI)	308
Update all device objects from (CLI)	312
Send us feedback	314

Welcome to AppViz

The AlgoSecAppViz add-on enables you to view your security network policies from the perspective of your business applications. Business applications are individual business needs that require special traffic flows to be allowed in network security policies.

The AppViz add-on is layered over AFA, and also has an optional AppChange component layered over FireFlow. Customers who have additional licenses for AppChange can manage FireFlow change requests from AppViz, from the business application perspective.

Access AppViz

AppViz and the additional AppChange component are add-ons layered over AFA and FireFlow, respectively.

Do the following:

- Access AppViz from the AFA or FireFlow left-side navigation menu.

Click  to open AppViz in a new browser tab.

- Once open, AppViz has its own left-side navigation menu and **Administration** area.

To access the Administration area, click your username at the top-right and select **Administration**.

For more details, see:

- [AppViz main menu](#)
- [AppViz administration](#)
- [AppViz maintenance](#)

Tip: At the top of each page in the workspace, click **AlgoSec Reporting Tool** to view

detailed reports on data across ASMS.

AppViz main menu

The main menu includes the following options:

HOME	<p>The default AppViz home page, which displays graphs and widgets about the configured applications.</p> <p>The HOME page also enables you to perform an Impact Analysis search. For details, see Analyze application impact.</p> <p>Note: The Applications by Lifecycle Phase widget is displayed only when vulnerability assessment is not configured. The Most Vulnerable Applications widget is displayed only when vulnerability assessment is configured.</p> <p>For more details, see Manage vulnerability assessment scanners.</p>
APPLICATIONS	<p>Enables you to view and manage the applications configured in AppViz.</p> <p>For details, see Business applications.</p>
NETWORK OBJECTS	<p>Enables you to view and manage network objects from AppViz.</p> <p>For details, see Network objects and Device objects.</p>
SERVICE OBJECTS	<p>Enables you to view and manage service objects from AppViz.</p> <p>For details, see Service objects and Device objects.</p>
PROJECTS	<p>Enables you to view and manage AppViz projects.</p> <p>For details, see Projects.</p>

DISCOVERY	<p>Enables you to discover new application data from device policies.</p> <p>For details, see Discover applications.</p> <p>Note: AutoDiscovery is an additional AlgoSec tool installed over AppViz, which enables you to automatically discover business applications and flows, and import them in to AppViz.</p>
------------------	--

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.

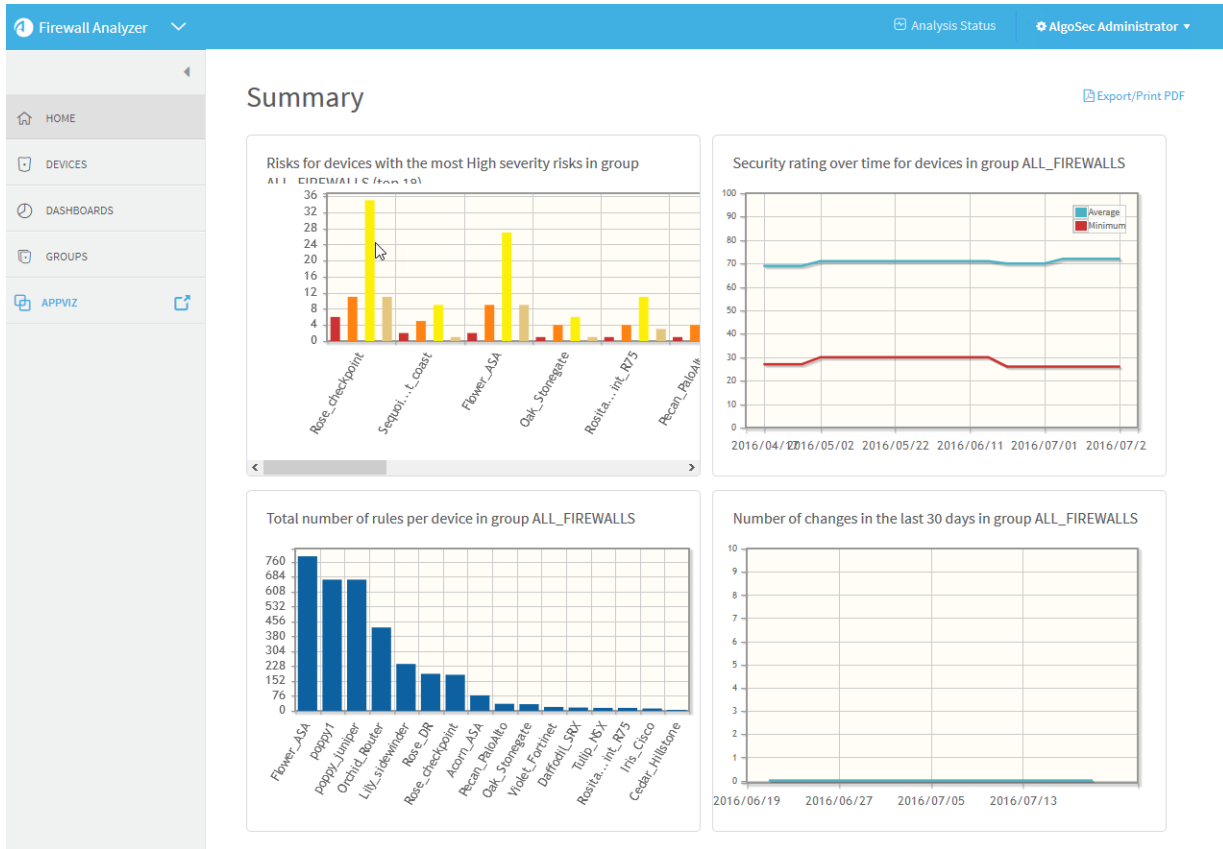


The screenshot shows the login interface for the algosec Security Management Suite. At the top right, there is a link labeled "About". The logo for "algosec" is prominently displayed in the center, with the "a" in a blue circle. Below the logo, the text "Security Management Suite" is centered. There are two input fields: "User Name" and "Password". Below these fields is a blue "Login" button.

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

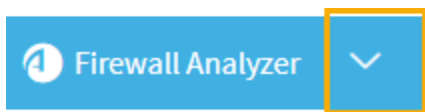
You are logged in, and ASMS displays AFA by default.

For example:

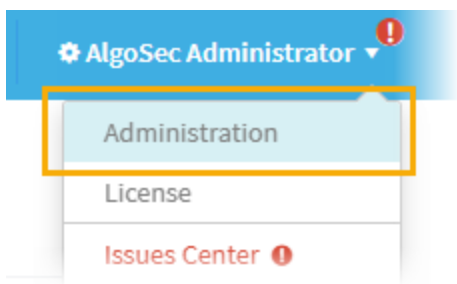


Switch ASMS products

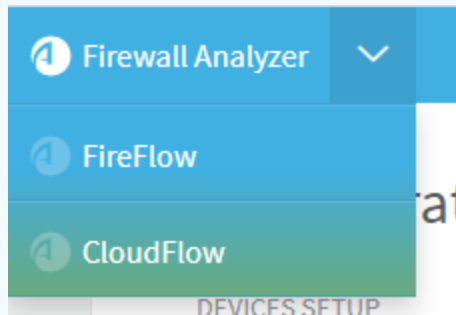
If you are a user in multiple ASMS products, such as AFA, FireFlow, and AppViz, switch between products using the dropdown at the top-left, above the main menu.



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.

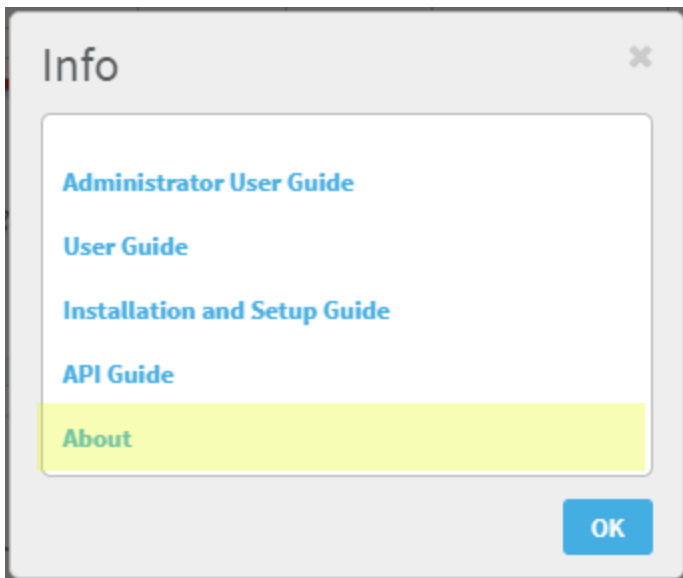
- **To adjust the size of the main menu**, hover between the menu and the workspace and drag the border left or right.
- **To collapse the menu entirely**, click  at the top. When collapsed, click  to expand it again.

View ASMS product details

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

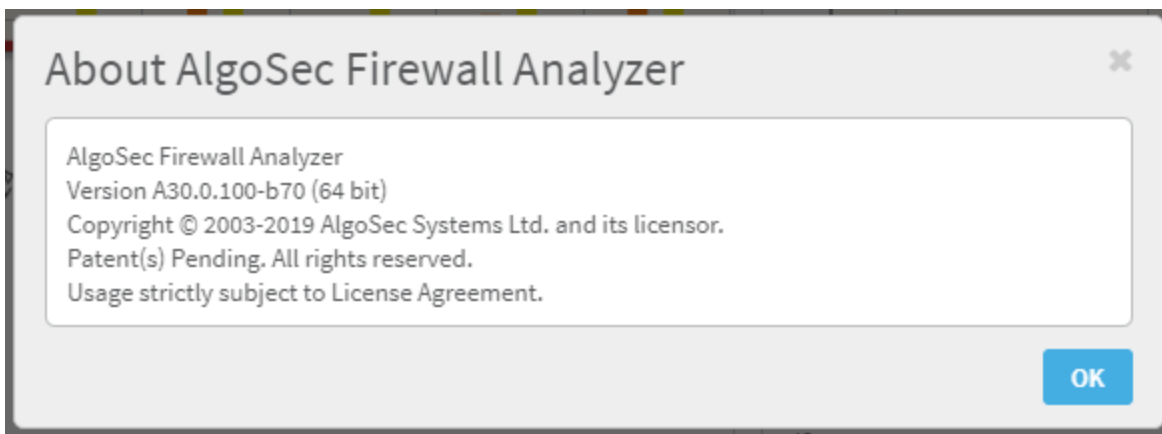
Do the following:

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*.

Business applications

In AppViz, an application is a business need that may require specific traffic flows to be allowed in your network security policy. Typically, an application is associated with the various user communities that use its services and manage the application.


View applications

From the AppViz main menu, click **APPLICATIONS** to search for and view the applications configured in AppViz.


Recent applications are displayed by default under the search bar. Click an application name to view its details in the workspace.



- **The colored square** next to each application name represents its current status, which is based on the connectivity status of the application's flows.

Colors include:


 **Allowed.** The network security policy is configured to allow all of the application's connectivity requirements. Every flow in the application is allowed.

 **Blocked.** One or more of the application's flows are blocked or partially blocked.

 No connectivity information, or applications with a status of **Decommissioned** or **Pending Decommission**.


- **Images** such as  or  indicate an application's revision status. Click the icon to select the revision you want to view.

Enter text in the search bar to search for an application name. For more details, see [Search for applications](#).

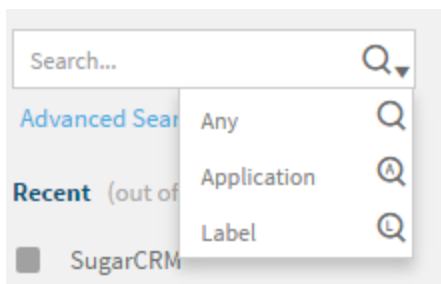
Tip: To return to the other areas available from the main menu, click the hamburger menu  at the top left, and select the page you want to navigate to.

Search for applications

At the top left of the AppViz Applications area, enter text in the search bar at the top left to search for application names or labels.

To search for application names or labels only, click  and select an option from the dropdown menu:

Note: This search only returns current versions of your applications, and cannot access historical data.



Perform an advanced search



Under the **Applications** search bar, click **Advanced Search** to perform an advanced search for applications.



In the **Advanced Search** dialog, enter text in any of the fields to find matching applications.

- Start typing to select from a list of auto-complete options.
- Click lookup links to use wizards to help you find your data. For details, see:
 - [Network object lookup wizard](#)
 - [Service lookup wizard](#)
 - [Users lookup wizard](#)
 - [Network application lookup wizard](#)
 - [Advanced search wizard auto search](#)
- At the top-right, click **Clear all filters** to clear your search criteria.

Click **Search** to perform your search.

Advanced search fields include:

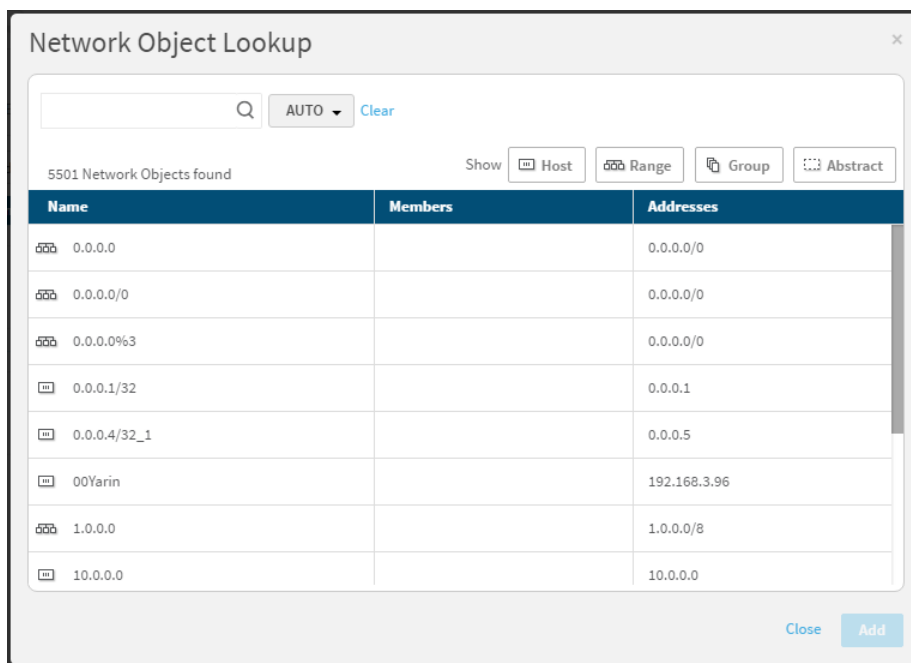
Field	Description
By Traffic	<p>Enter details in any of the following fields:</p> <ul style="list-style-type: none"> • Source. A server name or IP address for the traffic source you want to search for. • User. The user name for the user of the traffic you want to search for. • Destination. A server name or IP address for the traffic destination you want to search for. • Network Application. A network application name for the traffic source you want to search for. • Service. A service name or definition of the service of the traffic you want to search for. • Click  to add another traffic line to your search criteria. • Click  to delete a traffic line. <p>Note: The User and Network Application fields appear only when user or application awareness is configured.</p>
By Network Objects	Enter the name of a network object.
By Devices	Enter the name of a device.
By Risk	Enter a risk code or title.
By Vulnerability	Enter a CVE identifier or vulnerability description.
By Connectivity	<p>Select one or more connectivity statuses for the application's flows.</p> <p>Note: This search parameter is related to flow connectivity, <i>not</i> application connectivity. The results will include all applications with at least one flow with the specified connectivity.</p>

Field	Description
By Status	Select one or more revision statuses.
By Label	Enter a label name.
By Projects	Enter a project name.
By Custom Field	Enter a custom field name and value. <ul style="list-style-type: none"> Click  to add another custom field line. Click  to delete a custom field line.
By Expiration Date	Enter a range of application expiration dates.

Network object lookup wizard

1. Click **Network object lookup** below the desired field.

The **Network Object Lookup** wizard appears.



Note: If device objects with the same name (but different content) appear, the device on which the object is defined is indicated.

2. To search for network objects, use the Auto-Search. For details, see [Advanced search wizard auto search](#).
3. To filter the results by object type, click one or more of the **Show** buttons.
 - The first **Show** button you click causes all other buttons to become disabled (and consequently not appear in the results).
 - Clicking additional buttons causes the object type you click to toggle: if it was enabled it will become disabled and vice versa.
 - By default, all **Show** buttons are enabled (all objects appear in the results).
4. Select one or more network objects from the list.

The number of network objects selected appears above the list.
5. Click **Add**.


The selections are added to the field.

Users lookup wizard

Note: If user field validation is not enabled, the only users that appear in this lookup are users that were previously created in AppViz. Administrators can enable user field validation as needed. For details, see [Enable validation for the user field](#).

To select a user using the Users Lookup wizard:

1. Click **User lookup** below the **Users** field.

The **Users Lookup** wizard appears.
2. To search for users, type the search criteria into the search box, and click .
3. Select one or more users from the list.

4. Click **Add**.

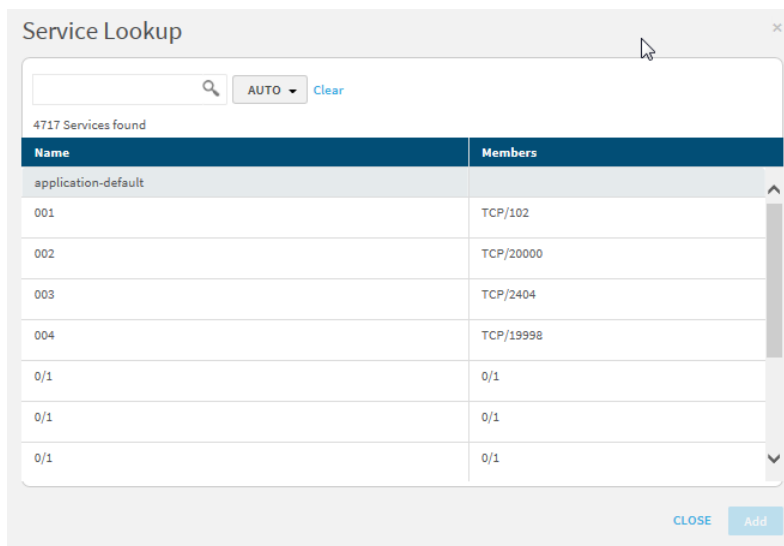
The selections are added to the field.

Service lookup wizard

To select a service using the Service Lookup wizard:

1. Click the link below the desired field.

The **Service Lookup** wizard appears.



2. To search for services, use the Auto-Search. For details, see [Advanced search wizard auto search](#).

3. Select one or more services from the list.

The number of services selected appears above the list.

4. Click **Add**.

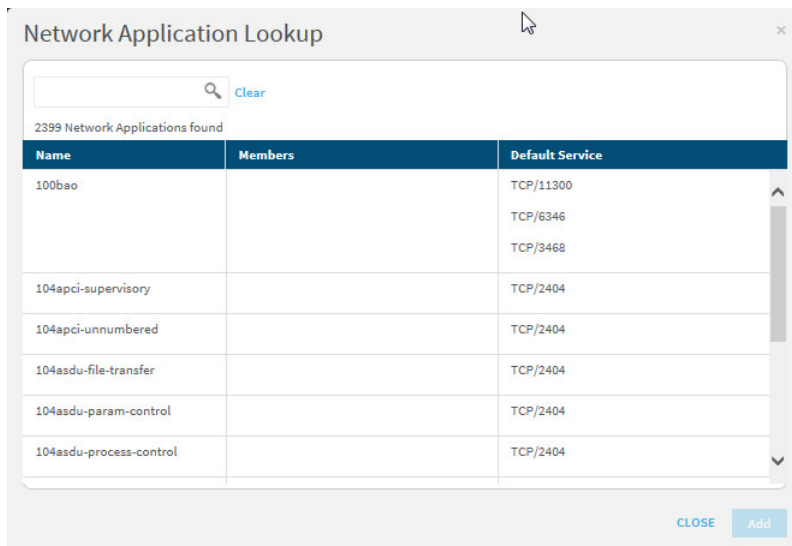
The selections are added to the field.

Network application lookup wizard

To select an application using the Network Application Lookup wizard:

1. Click **+ Network Application Lookup**.

The **Network Application Lookup** wizard appears.



2. To search for network applications, type all or part of an application name in the search box, and press enter.

3. Select one or more applications from the list.

The number of network applications selected appears above the list.

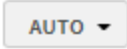
To clear all your selections, click **Clear**.

4. Click **Add**.


The selections are added to the field.

Advanced search wizard auto search

To use the Auto Search:

1. In the  drop-down menu, select one of the following options:

Search parameter	A search will return...
Containing the range	All objects that contain the searched content.
Contained within the range	All objects that are entirely contained in the searched content.
Exact address/service match	All objects that are an exact match of the searched content.
Intersection	All objects that have any overlap with the searched content.
Match as object name	All objects whose name contains the searched phrase.
Auto	All objects whose names contain the searched phrase. If an IP address/range or service definition is entered, then all servers/services which intersect with the given content.

2. Type the search criteria into the search box, and click .
3. Select one or more objects from the list below the search box.

Note: You may select multiple objects, but if you perform a search after making a selection, the original selection will not stay selected.

Add applications

This procedure describes how to add a new application to AppViz manually.

Do the following:

In the AppViz Applications area, click **+ New Application** at the bottom-left.

1. Go to the **Applications** area. For details, see [Welcome to AppViz](#).
2. Click **+ New Application**.

The **New Application** form appears in the workspace.

3. To clone an existing application:
4. Click the **Based on existing** tab.
5. In the **Base Application** box, type the name of the application to clone. Or, click **Application lookup** to search for the base application or select from the **Application Name list**.
6. Complete or modify the fields as needed. For details, see [Application fields](#).
7. To associate contacts with the application, do the following in the **Contacts** area:
8. Click **Add contact**.
The **Add contact** wizard appears.
9. Use the wizard to select the contact. For details, see [Use the Add Contact wizard](#).
10. To add a label to the application, see [Add a label](#).

Note: This area only supports adding user-defined labels, not system labels

such as the labels associated with Critical Processes. System labels, by definition, are only added to applications as the result of a system function.

11. To add an attachment to the application, click **Attach files** and follow the instructions.
12. Click **Save Changes**.

The application is added.


Application fields

In this field...	Do this...
Name	Type the name of the application.
Expiration Date	Click the calendar icon to select an expiration date. Note: Expiration date may be modified in edit mode.
Business Unit	Type the name of the business unit.
Business Unit Location	Type the name of the business unit location.
Line Of Business	Type the line of business.
Business Criticality	Type the criticality of the business.
Business Partner ID	Type the ID of the business partner.

Use the Add Contact wizard

To add contacts:

1. Do one of the following:
 - Select a contact from the **Contacts** list below the search box.
 - Search for a contact, by doing the following:
2. Type any part of the contact name in the search box.


3. Click .
4. Select the contact's role from the **Roles** list.
5. Click **Save Changes**.

The contact is added to the application.

Add a label

Note: You can only add user-defined labels, not system labels. By definition, system labels are automatically added to applications because of a system configuration.

To add a label to an application:

1. If you are working from the application's **Dashboard** tab, click  **Edit**. Otherwise, continue to the next step.

The **Labels** field appears in an editable format.

2. Start typing the label name in the field.

A drop-down list appears with auto-completed options.

If the user has permission to create new labels, the list additionally includes an option to create a new label with the name you specified and add it to the application.

3. Select the desired label in the drop-down list.

The label appears in the field.

4. To de-select a label, click **x**.

Note: You can only de-select user-defined labels, not system labels.

5. If desired, repeat the procedure to add additional labels.

6. If you are working from the application's **Dashboard** tab, click **Save Changes**.
Otherwise, continue with the relevant procedure.

Application workflow

Use AppViz to manage your applications using the following steps:

1. Add, edit, or remove flows from an application. The application revision status changes to **Draft**.
2. Apply the draft revision to the network security policy, or remove it. AppViz opens a FireFlow change request to block traffic flows that are no longer in use.

For details, see:

- [Application dashboard](#)
- [Application flows](#)
- [Application diagram](#)
- [Application change requests](#)
- [Application vulnerability](#)
- [Application risks](#)
- [Application activity log](#)
- [Analyze application impact](#)
- [Application contacts](#)

➔ See also:

- [Creating and Discovering Applications](#)
- [Working with Applications](#)

Application dashboard

The application's **DASHBOARD** tab provides the ability to:

- Quickly and easily view a summary of an application's status and history.
- Verify an application's connectivity.
- Apply or discard changes to an application.
- Resolve an application's blocked flows.
- Decommission an application.
- Edit application information.
- Export application information.
- Create a cloned of the application.

Application DASHBOARD tab interface

The screenshot shows the AppViz application dashboard for an application named 'eCommerce'. The interface is divided into several sections:

- Header:** 'Firewall Analyzer' and 'APPVIZ' are visible on the left, and 'AlgoSec Administrator' is on the right.
- Left Sidebar:** Contains 'Applications' with a search bar set to 'Production'. Below the search bar, there are search results for 'LDAP', 'DNS', and 'eCommerce' (which is selected).
- Main Content Area:**
 - Application Name:** 'eCommerce' with a red status indicator and a '1 BLOCKED' notification.
 - Navigation Tabs:** 'DASHBOARD' (selected), 'FLOWS', 'DIAGRAM', 'CHANGE REQUESTS', 'VULNERABILITY', 'RISKS', and 'ACTIVITY LOG'.
 - Revision 7 Summary:**
 - Revision Status: Active
 - Revision Creation Date: 17/06/2015 08:20
 - Number of flows: 4
 - Risk Score: 100%
 - Vulnerability Score: 34
 - Action Buttons:** 'Resolve', 'Decommission', 'Export', 'Clone', and 'Refresh Connectivity'.
 - Application Diagram:** A visual representation of the application's flow, showing a sequence of components connected by lines.
 - General Information:**
 - Created on: 20/11/2014 04:28
 - Expiration Date: 29/11/2016
 - Application lifecycle: Testing
 - Business Criticality: High
 - Business Partner ID: RVX-1287TY
 - Labels:** 'BOS-DC', 'Critical', 'Finance', and 'Production'.

Dashboard Tab Areas

Revision Information

This area displays the following information about the revision of the application you are viewing:

- **Revision.** The current revision's number, counting from the application's creation.

For more details, see [View multiple versions of the same application](#).

- **Revision Status.** One of the following:

Status	Description
Active	The revision of the application currently in use. This revision's traffic flow needs are currently incorporated in the network security policy.
Draft	A revision of the application that has changes that have not been incorporated in the network security policy.
Pending Implementation	An application that has been updated, but the change request is still being processed in FireFlow. If the change request is rejected, the revision status will revert to being active.
Rejected	A revision of the application whose FireFlow change request was rejected.
History	A revision of the application that was once in use. The application has been revised, and the changes have been incorporated in the network security policy.
Pending Decommission	An application that has been decommissioned, but the FireFlow change request that is blocking the traffic has not yet been resolved. If the change request is rejected, the revision status will become rejected.
Decommissioned	An application that is no longer in use. The application's flows have been removed from the network security policy.

By default, revision status changes from **Pending Implementation** to **Active** once the FireFlow change request reaches the reconcile, pending match, or resolved statuses. For more details, see [Configure advanced AppViz properties](#)

- **Revision Creation Date.** The date the revision was created.
- **Number of flows.** The total number of traffic flows.

Note: The number of blocked traffic flows appears on the Flows tab. Blocked flows are resolved using the **Resolve** action.

- The number of FireFlow change requests submitted for the application. Clicking **View** takes you to the **Change Requests** tab.
- **Risk Score.** The application's risk score.
- **Vulnerability Score.** The application's vulnerability score.

Application Diagram

This area displays one of the following graphs:

- **Application Diagram.** For details, see [Application diagram](#).
- **Change Requests Over Time**
- **Application Security Rating Over Time**

Click the side arrows to switch between graphs.

Actions

Action	Description
Apply Draft	This is an optional action for draft revisions and rejected revisions. Applying a draft updates an application according to the changes specified in the revision. For details, see Apply application drafts .
Discard Draft	This is an optional action for draft revisions and rejected revisions. Discarding a revision deletes all changes made to the application. For details, see Discard application drafts .

Action	Description
Resolve	This is an optional action for active revisions with blocked flows. Resolving an application opens blocked flows that are required by the application. For details, see Resolve active applications .
Decommission	This is an optional action for active revisions. Decommissioning an application disables the application. For details, see Decommission applications .
Export	This is an optional action for all revisions. You select which information to export. For details, see Export application content to PDF
Clone	This is an optional action for all revisions. Cloning allows you to create a duplicate of an application (with a different name). For details, see Clone applications .
Refresh Connectivity	This is an optional action for all revisions except decommission. Refreshing connectivity updates AppViz's connectivity information for the application. For details, see Refresh application connectivity .

Note: You can never perform an action that initiates change requests for applications that are **Pending Implementation** or **Pending Decommission**.

Note: When a FireFlow change request is created as the result of an application action, the subject of the change request signifies the application. For details, see [Customize interactions with AFA and FireFlow](#).

General Information

This area displays the following information about the application:

Info	Description
Created on	Date the application was created.
Expiration Date	<p>Date application is set to expire.</p> <ul style="list-style-type: none"> • If an application has expired, APPLICATION EXPIRED appears in the upper right corner. • If an application is nearing expiration, Expires in <i>n</i> days appears in the upper right corner. <p>See Manage application expiration .</p> <ul style="list-style-type: none"> • Testing. The application is undergoing tests before use. • Staging. The application is undergoing limited use before it is put into production. • Production. The application is currently being used. • Decommission. The application is no longer being used.
Lifecycle phase	<p>By default, one of the following:</p> <div style="background-color: #e6f2e6; padding: 10px; border: 1px solid #ccc;"> <p>Tip: The lifecycle phase is not tightly coupled with the network security policy, and only signifies the application's state from the business perspective.</p> <p>You can optionally customize the names and number of lifecycle phases. For details, see Custom fields.</p> </div>

Additionally, any of the following that is relevant for the application will be displayed in this area:

- **Business Unit**
- **Business Unit Location**
- **Line of Business**
- **Business Criticality**
- **Business Partner ID**

- **Attachments**
- **Any custom fields that you have added**

To edit an application's general information, see [Edit general application information](#).

Labels

This area displays all labels associated with the application and allows you to add new user-defined labels.

There are two different types of labels in AppViz:

User-defined labels	Basic labels that can be created and added to any application as a way of organizing applications in groups. These labels appear in blue.
System labels	<p>Labels that are automatically assigned to an application as the result of a system function. Applications with system labels include:</p> <ul style="list-style-type: none"> • Critical Process Applications. All applications that are part of a critical process are marked with its label. The label will be the name of the critical process and will appear in maroon. For more details, see Critical processes. • PCI Applications. All applications that contain a network object that intersects the PCI zone in their active revision are marked with the PCI label. The label appears in teal.

For more details, see [Business applications](#).

Contacts

This area displays contact information for all contacts associated with the application.

To edit an application's contacts, see [Edit contact information](#).


Apply application drafts

Applying an application draft activates changes to the application that you have made in the draft revision. You can apply all of the changes in a draft or only some of the changes. A FireFlow change request is created to apply the specified changes to the network security policy.

- When you apply all the changes in a draft revision, the draft enters the **Pending Implementation** status.
- When you apply some of the changes in a draft revision, a new application revision with only the selected changes is created and enters the **Pending Implementation** status. The original draft revision remains intact (as a draft revision) with both the changes that were and were not applied.

Note: When applying a draft where some of the changes in the draft have already been applied, only the changes that have not yet been applied will appear as options to be applied with the FireFlow change request.

To apply an application draft:

1. View the application for which you want to apply a draft. For details, see [Business applications](#).
2. In the **Actions** area of the **Application Dashboard** tab, click .

The **Apply Flows Changes** window appears, describing the FireFlow change request that will be created to add or remove traffic flows for the application in the network security policy.

Apply Flows Changes: For resolve

Change Request Summary AppViz Change Request for For resolve Show legend

Changes in Flows
Will be included in the change request

<input checked="" type="checkbox"/>	Name	Source	User	Destination	Service
<input checked="" type="checkbox"/>	1	<input type="checkbox"/> 199.244.255.130 <input type="checkbox"/> a_10.10.75.100 <input type="checkbox"/> Host10.10.75.90	<input type="text" value="Any"/>	<input type="text" value="Host10.30.75.5"/>	<input type="text" value="ssh"/>
Changes details					
<input checked="" type="checkbox"/>	2	<input type="text" value="146.28.33.0/24"/>	<input type="text" value="Any"/>	<input type="checkbox"/> 144.5.130.21 <input type="checkbox"/> Host10.20.75.101	<input type="text" value="admin_http"/>
Changes details					

Cancel Apply

- Flows to be added to the application and objects to be added to a flow appear highlighted in .
- Flows to be removed from the application and objects to be removed from a flow appear highlighted in .
- Flows to be edited in the application and objects to be edited in a flow appear highlighted in .

Note: If traffic flows have been removed from the application, but the traffic intersects the needs of another application, a FireFlow change request will not be created to remove the traffic.

Note: If the draft that is being applied includes changes that have already been applied, only the changes that have not yet been applied will appear in the **Apply Flows Changes** window.

3. Clear the check boxes next to the flows that you do not want to apply.

Apply Flows Changes: For resolve

Change Request Summary * AppViz Change Request for For resolve Show legend ▾

Changes in Flows
Will be included in the change request

<input type="checkbox"/>	Name	Source	User	Destination	Service
<input checked="" type="checkbox"/>	1	<input type="text" value="199.244.255.130"/> <input type="text" value="a_10.10.75.100"/> <input type="text" value="Host10.10.75.90"/>	<input type="text" value="Any"/>	<input type="text" value="Host10.30.75.5"/>	<input type="text" value="ssh"/>
Changes details					
<input type="checkbox"/>	2	<input type="text" value="146.28.33.0/24"/>	<input type="text" value="Any"/>	<input type="text" value="144.5.130.21"/> <input type="text" value="Host10.20.75.101"/>	<input type="text" value="admin_http"/>
Changes details					

Note, only changes in the selected flows will be part of the change request Cancel

Note: Only the selected changes will be included in the FireFlow change request.

- (Optional) Edit the **Change Request Summary** field.

The contents of this field will be the subject of the FireFlow change request(s).

- Click **Apply**.

The draft is applied. This may take a few minutes.

The relevant change request is created. The FireFlow change request will include a link to the application, the application's diagram, and details of the changes to the application's flows.

Note: The application information in FireFlow will only be visible to users with the required AppViz / AppChange permissions.


When the change request is resolved in FireFlow, the new revision of the application will be **Active**.

Discard application drafts

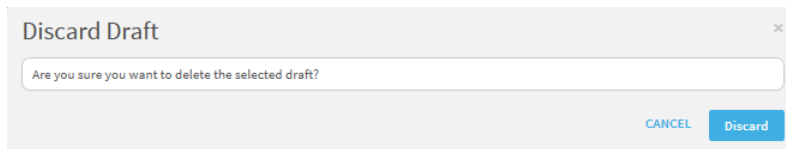
Discarding an application draft deletes all changes to the application you have made in the draft revision. No record of changes you have made to the draft revision is kept, as

the changes were never active.

To discard an application draft:

1. View the application for which you want to remove an application revision. For details, see [Business applications](#).
2. In the **Actions** area of the **Application Dashboard** tab, click .

The **Discard Draft** window appears.



3. Click **OK**.

The draft is discarded.

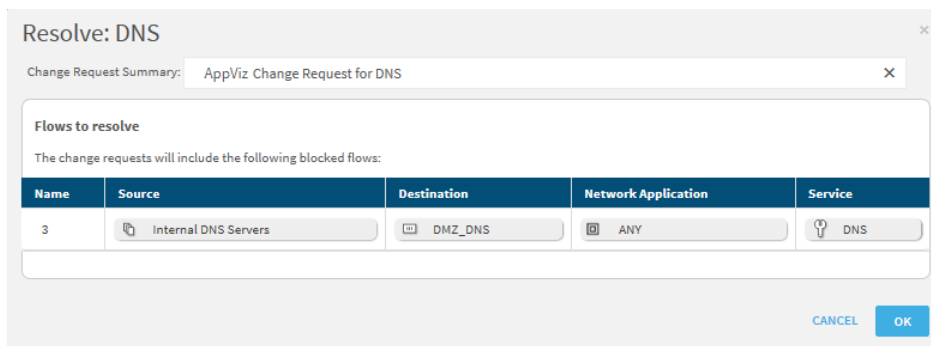
Resolve active applications

When some or all of an active application revision's flows are blocked, you have the option to resolve the application. This action issues a change request to open blocked flows.

To resolve active applications:

1. View the application you want to resolve. For details, see [Business applications](#).
2. In the **Actions** area of the **Application Dashboard** tab, click the  icon.

The **Resolve** window appears, describing the FireFlow change request that will be created.



3. Click **OK**.

The relevant change request is created. The FireFlow change request will include a link to the application, the application's diagram, and details of the changes to the application's flows.

Note: The application information in FireFlow will only be visible to users with the required AppViz / AppChange permissions.

Decommission applications

Decommissioning an application deactivates the application. A FireFlow change request is created to block traffic that was allowed for the sake of the application, and the application enters the **Pending Decommission** revision status.

When an application enters the **Pending Decommission** revision status, the following occurs:


- A change request opens in FireFlow to close any relevant traffic.
- No actions that initiate change requests can be performed on the application.
- The application will appear grayed out in the **Applications** tab of any network or service objects associated with the application.
- If the application is currently used in a critical process, project or discovery search, the application will appear grayed out. You will no longer be able to use the application in any of these processes.

If the change request is resolved in FireFlow, the application enters the **Decommissioned** revision status, and the following occurs:

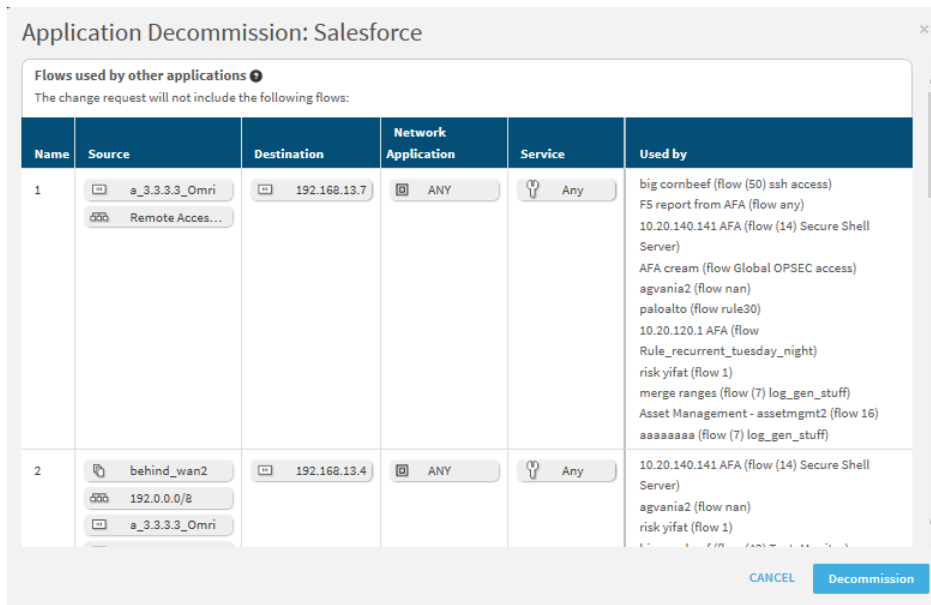
- The network and service objects that were associated with the application lose the association. The objects will still appear in the application's **Flows** tab, but the application will not appear as an affected application for its objects in the **Application** tab or for a search or impact analysis.
- If the application is used in a critical process, project or discovery search, the application will be removed.
- The application's history will still be visible in the activity logs in the administration area. For details, see [Application activity log](#).
- Any rules in AFA that were associated with the application will lose their associations.

If the decommissioning change request is rejected, the application will revert to its previously active revision.

To decommission an application:

1. View the application you want to decommission. For details, see [Business applications](#).
2. In the **Actions** area of the **Application Dashboard** tab, click the  icon.

The **Application Decommission** window appears, describing the FireFlow change request that will be created to block traffic in the network security policy. If the traffic slated to be blocked intersects the needs of another application, a FireFlow change request will not be created to remove the traffic.




3. Click **Decommission**.

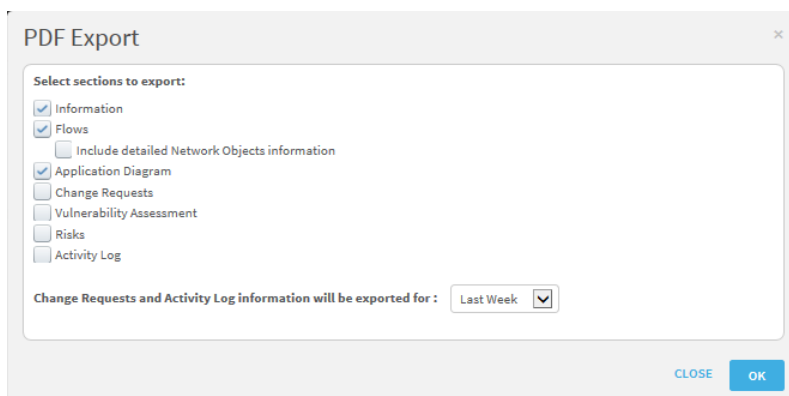
The relevant change request is created and the application enters the **Pending Decommission** revision status.

Export application content to PDF

To export application content:

1. View the application you want to export. For details, see [Business applications](#).
2. In the **Actions** area, click .

The **PDF Export** window appears.



3. Select the information to export, and click **OK**.

You can choose specific tabs and/or all Change Request and Activity Log information for the last week, month, or quarter.

Your browser will prompt you to save or open the PDF file.

Clone applications

To facilitate the creation of a new application that is similar to an existing one, you can clone the application and edit it to meet the new requirements.

There are two options for cloning an application:

- From the **New Application** page
- From the **Actions** area of the application's **Dashboard** tab

Note: When you clone an application, any user-defined labels will be cloned, but the system labels will not be cloned. For example, if an application has one user-defined label and one label indicating it is part of a Critical Process, only the user-defined label will be created with the clone.


To clone an application from the New Application page:

1. In the Applications panel, click **+New Application**.

The New Application area appears.

2. Click the **Based on existing** tab.
3. In the **Base Application** box, type the name of the application to clone. Or, click **Application lookup** to search for the base application or select from the **Application Name** list.
4. Modify data fields as needed. For details, see [Business applications](#).

To clone an application from the Applications Dashboard:


1. View the application that you want to clone. For details, see [Business applications](#).
2. In the **Actions** area of the application's **Dashboard** tab, click .
The Edit Name window appears.
3. Type the name for the cloned application and click **OK**.
4. Modify data fields as needed. For details, see [Business applications](#).

Refresh application connectivity

Refreshing application connectivity checks whether the network security policy allows all the traffic flows that an application requires and updates all the connectivity information AppViz has for the application. To verify the application connectivity per traffic flow, see [Application flows](#).

Note: You must have permission to refresh connectivity to perform this procedure.

To refresh application connectivity:

1. View the application for which you want to verify the connectivity. For details, see [Business applications](#).
2. In the **Dashboard** tab, click .

AppViz checks whether the network security policy allows all the application's required traffic flows. This may take a few minutes.

The color of the icon next to the application's name is updated to reflect the current connectivity of the application. For more details, see [Business applications](#).

View multiple versions of the same application

When you are viewing an application with more than one revision, you can navigate between the different revisions. You can identify applications with more than one revision because the icon to the left of the application's name appears with an arrow:



To view different revisions of the same application:

1. View the application. For more details, see [Business applications](#).
2. Click the icon to the left of the application's name.
A drop-down menu appears.
3. Select the icon that represents the revision you want to view.


This icon...	Indicates this revision...
	Active or Decommissioned
	Pending implementation or Pending decommission
	Draft

Note: The color of the icon indicates the connectivity status, not the revision status. For more details, see [Business applications](#).

The revision you selected appears.

Edit general application information

To edit general information:

1. View the application for which you want to edit the general information. For more details, see [Business applications](#).
2. In the **General Information** area of the **Application Dashboard** tab, click  **Edit**.
3. Edit the desired fields as needed. For more details, see [Business applications](#).

Other fields may appear, depending on your custom field configuration.


Note: Renaming an application is disabled when a connectivity check is running for the application.

4. To edit or delete an existing attachment, click the **Attachment** link.
5. To add an attachment, click **Attach files** and follow the instructions.
6. Click **Save Changes**.

The edits are saved.

Edit contact information

To edit contact information:

1. View the application for which you want to edit the contact information. For more details, see [Business applications](#).
2. In the **Contacts** area of the **Application Dashboard** tab, click  **Edit**.
3. To associate a new contact with the application, do the following:
 - a. Click **Add contact**.
The **Add contact** wizard appears.
 - b. Use the wizard to select the contact. For more details, see [Business applications](#).

4. To remove a contact from the application, click the **X** next to the contact.
5. Click **Save Changes**.

The edits are saved.

Application flows

The application's **FLOWS** tab enables you to manage an application's traffic flows.

Flows describe traffic to and from servers, which are represented by network objects, via a specific service. Flows may also specify a user or network application, and include other fields, such as comments.

Flow types

AppViz applications include the following types:

Application flows	Flows that are custom-built for a specific application.
Shared flows	<p>A semi-custom flow that can be relevant for many applications. Shared flows are templates with empty source and destination values, which are provided by a subscribing application.</p> <p>Note: For shared flows when user awareness is enabled, the User field will be treated the same way as the Source field. When the source is the place holder, the user will also be a place holder.</p>
Subscribed flows	An instance of a shared flow that's customized for a specific application, with its source and destination fields provided by the application.

FLOWS tab interface

The **FLOWS** tab displays all of your application's flows and details in a series of tables.

The screenshot shows the 'Enterprise Backup' application configuration in the Firewall Analyzer. The interface is divided into a sidebar and a main content area. The sidebar contains a search bar and a list of search results. The main content area displays a table of flows categorized into Application Flows, Shared Flows, and Subscribed Flows. Each flow entry includes columns for Name, Source, User, Destination, Network Application, Service, and Comments.

Name	Source	User	Destination	Network Application	Service	Comments
2	Mgmt_Net	Any	Backup Servers	Any	HTTPS	
3	Backup Servers	Any	GRP-NTP-SERVERS	Any	NTP	Time Sync
Shared Flows						
Name	Source	User	Destination	Network Application	Service	Comments
1	Placeholder	Placeholder	Backup Servers	Any	backup, HTTPS	Publish Backup Application
Subscribed Flows						
Name	Source	User	Destination	Network Application	Service	Comments
DNS (4)	Backup Servers	Any	Internal DNS Servers	Any	DNS	Publish DNS se application

Do any of the following:

- Click a column heading to sort the table by that column, and click it again to reverse the sort order.
- Hover over a network object or service to display its contents.
- Click a network object to display further details, including its name, type, origin, and addresses.

For more details, see:

- [Flow connectivity status](#)
- [Add flows to your application](#)
- [Edit an application's flows](#)
- [Remove flows from your application](#)
- [Export an application's flows](#)
- [Subscribe to another application's shared flows](#)
- [Verify flow connectivity](#)

Note: Adding, removing, or editing an application's flows changes the application's

revision to **draft**. The flow is not updated in the related network security policy until the draft revision is returned to **active**. For more details, see [Application dashboard](#).

Tip: AppViz also enables you to import flows from a discovery server or a CSV file. Importing flows also matches, or updates matching details, with AppViz applications. For more details, see [Discover applications](#).

Flow connectivity status

Every flow has a connectivity status. The traffic each flow represents may be allowed or blocked by the current network security policy. The flows tab indicates the connectivity status of each flow with colored strips on each side of the flow. Additionally, hovering over the strip reveals a tool tip with the connectivity status for the flow.


Note: The connectivity status of each flow contributes to the connectivity status of the application. For more details, see [Business applications](#).

Name	Source	User	Destination	Network Application	Service	Comments	CONNECTIVITY
1	cats_support Dogs_New_LAX dogs_support mice.home	Any	FortiManagerZebra_https	Any	HTTPS	Original Rule Number = 15,from devices: violet_fortinet fasdfda	CONNECTIVITY
2	jalapeno.net	Any	RedPepper-Replacement (abs...	Any	HTTP	Original Rule Number = 18,Comment was: FireFlow #412,from devices: violet_fortinet	Cannot run connectivity check for abstract flow
3	jalapeno.net	Any	red.pepper RedPepper-Replacement (abs...	Any	HTTPS	Original Rule Number = 19,Comment was: FireFlow #412,from devices: violet_fortinet	CONNECTIVITY
4	debbly_int	Any	violet_int_10-8 violet_int_old	Any	HTTP ICMP_ANY	Original Rule Number = 4,from devices: violet_fortinet	CONNECTIVITY
5	violet_grp_Forti-Management	Any	all	Any	DNS HTTPS SSH	Original Rule Number = 5,from devices: violet_fortinet	CONNECTIVITY



Allowed

If AppViz is configured to differentiate between unprotected traffic and traffic that is explicitly allowed, the green strips for unprotected traffic are striped. For more details, see [Configure advanced AppViz properties](#)

	<p>Blocked or Partially blocked.</p> <p>Note: You can determine whether the flow is blocked or only partially blocked by hovering over the strip. The tool tip which appears is specific.</p>
No strip	<p>No connectivity information</p>

Note: Abstract flows are indicated with pale blue stripes, but this is not a connectivity status for the flow. An abstract flow is a flow that does not represent any real traffic. Therefore, connectivity information is not relevant. For details, see [View a network object](#).

Add flows to your application

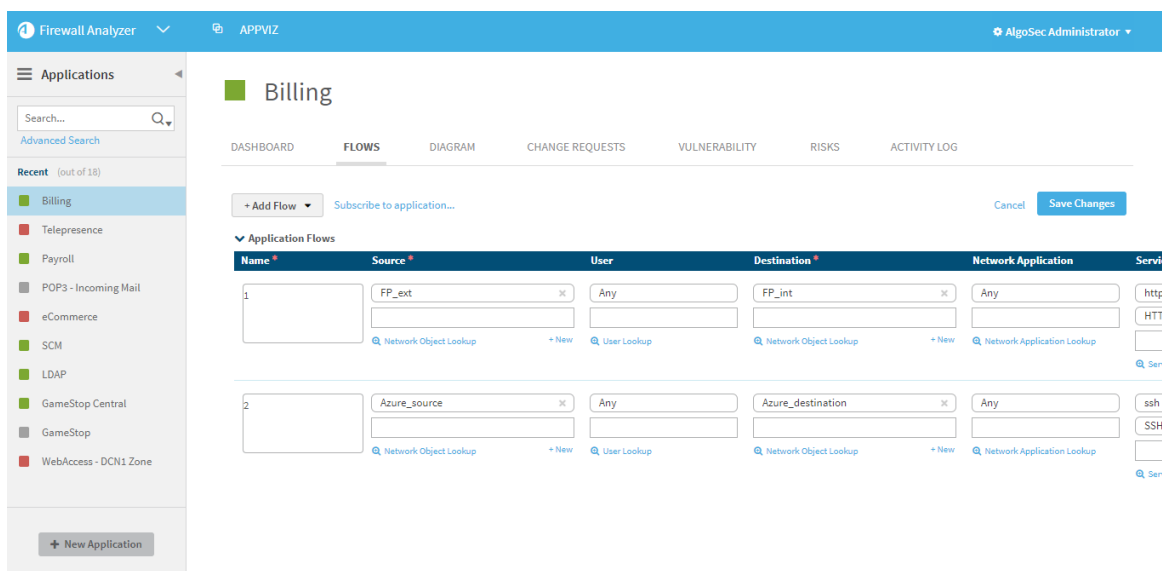
This procedure describes how to add an application or shared flow to your application.

Tip: Alternately, subscribe to another application's shared flows. For more details, see [Subscribe to another application's shared flows](#).

Do the following:

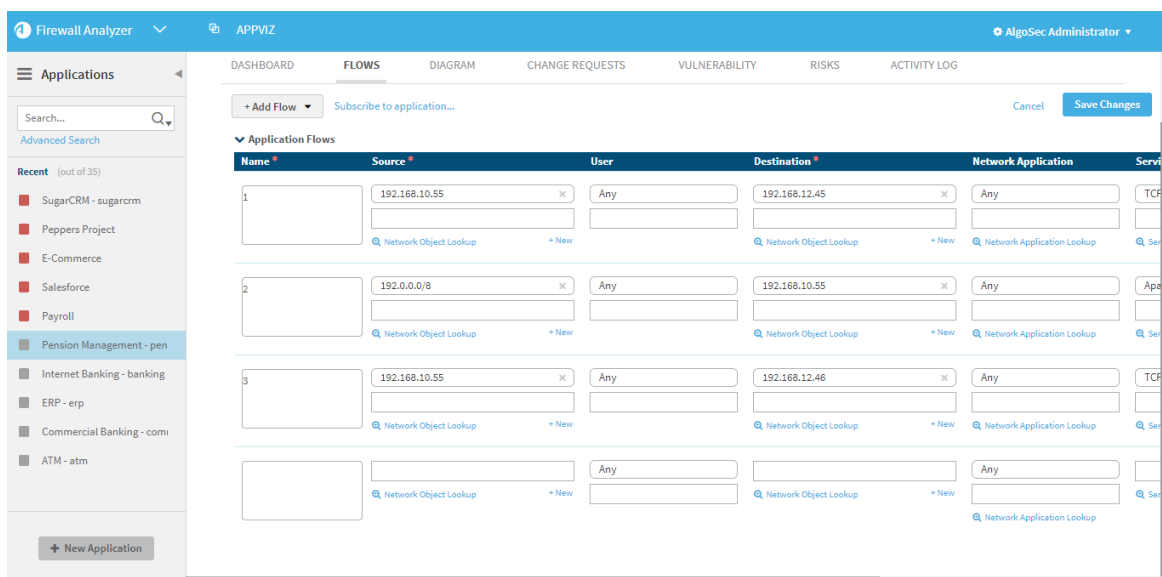
1. View the application for which you want to add a flow.
2. Click the **FLOWS** tab, and then click **Edit Flows**.

All the flows for the application appear in an editable format.



3. In the **+Add Flow** drop-down menu, select the flow type.

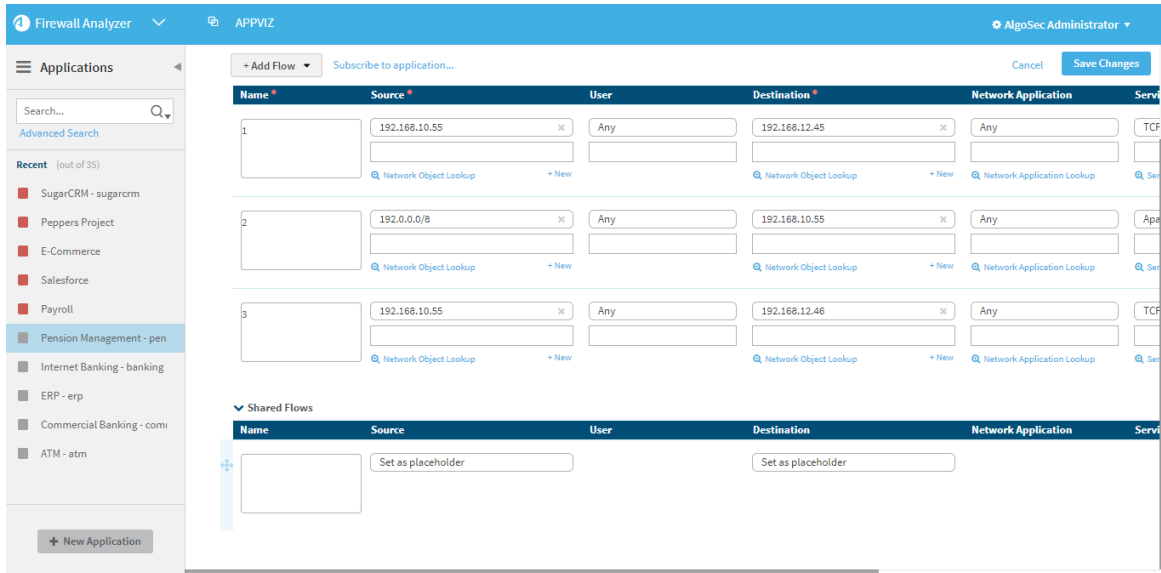
An empty flow appears at the bottom of the relevant list for the selected flow type.



4. To re-order flows, drag and drop the desired flows up or down.

5. For a shared flow, select the placeholder.

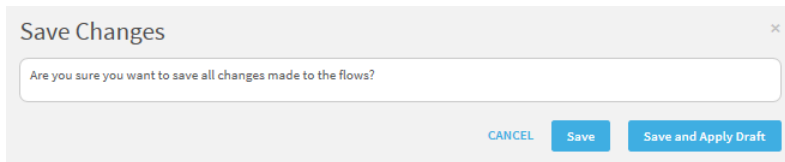
The placeholder is the field that is customizable for any application subscribing to it.



Note: When user awareness is enabled, the **User** field will be treated the same way as the **Source** field. When the source is the placeholder, the user will also be a placeholder.

6. Complete the fields as needed. For details, see [Flow fields](#).
7. Click **Save Changes**.

The **Save Changes** window appears.



- To save changes, click **Save Changes**.

The flow is updated, and this version of the application is saved as a draft revision.

- To save changes and apply the draft, do the following:
 - a. Click **Save and Apply Draft**.

The **Apply Draft** dialog box appears, describing the FireFlow change request that will be created to add or remove traffic flows for the application in the network security policy. If traffic flows have been removed from the application, but the traffic intersects the needs of another application, a FireFlow change request will not be created to remove the traffic.

- b. Click **OK**.

The flows are updated and the draft is applied. This may take a few minutes.


Note: The **Save and Apply Draft** option is disabled when the application has a revision pending implementation.

Flow fields

Field	Name
Name	Type the name of the flow.
Source	<p>Type the flow's source, or utilize the following features to aid you in selecting a source:</p> <ul style="list-style-type: none"> • Click the field to view recent objects, and then select the source from the list. • Start typing, and then select the source from the list of auto-completed options. • Use the Network object lookup wizard. For details, see Business applications. • Create a new object. For details, see Add a new network object.

Field	Name
User	<p>Type the flow's user, or utilize the following features to aid you in selecting a user:</p> <ul style="list-style-type: none">• Click the field to view recent users, and then select the user from the list.• Start typing, and then select the user from the list of auto-completed options. <p>Note: "Any" is the default value in the User field.</p> <p>This field only appears when user awareness is enabled. For more details, see Configure applications.</p>
Destination	<p>Type the flow's destination, or utilize the following features to aid you in selecting a destination:</p> <ul style="list-style-type: none">• Click the field to view recent objects, and then select the destination from the list.• Start typing, and then select the destination from the list of auto-completed options.• Use the Network object lookup wizard. For details, see Business applications.• Create a new object and add it to the flow. For details, see Add a new network object.

Field	Name
Service	<p>Type the flow's service, or utilize the following features to aid you in selecting a service:</p> <ul style="list-style-type: none"> • Click the field to view recent objects, and then select the service from the list. • Start typing, and then select the service from the list of auto-completed options. • Use the Service Lookup wizard. For details, see Business applications. • Create a new object and add it to the flow. For details, see Add a new service. <p>Note: Additional services cannot be added to a flow that already has the application-default service (this service represents the default service behind selected network applications). You can click x in the Service column to remove this service.</p>
Network Application	<p>Type the flow's network application, or utilize the following features to aid you in selecting a network application:</p> <ul style="list-style-type: none"> • Click the field to view recent network applications, and then select the network application from the list. • Start typing, and then select the network application from the list of auto-completed options. • Use the Network application lookup wizard. For details, see Business applications. <p>Note: "Any" is the default value in the Network Application field.</p> <p>This field only appears when application awareness is enabled. For more details, see Configure applications.</p>
Comments	Type a comment for the flow. This field is optional.
Any custom field	There may be other flow fields if custom fields have been added. For more details, see Custom fields .

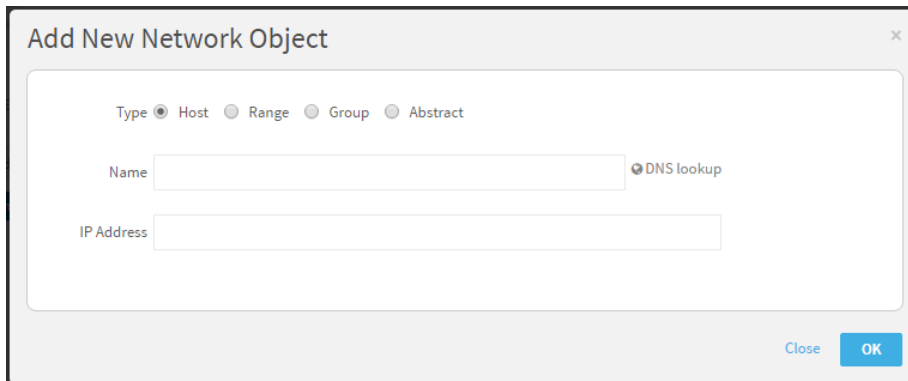
Field	Name
	To re-order the flows in the application, drag and drop a flow by this icon. The icon appears to the left of a flow when you hover over it.

Add a new network object

To add a new network object:

1. Click **+New**.

The **Add New Network Object** window appears.



2. Select the **Type** of network object: **Host**, **Range**, **Group** or **Abstract**. For more details, see [Network objects](#).
3. In the designated fields, type the following information for the new network object:
 - Name
 - **IP Address**, **IP Addresses**, or **Members**. Abstract objects do not have an address until conversion.)
4. Click **OK**.

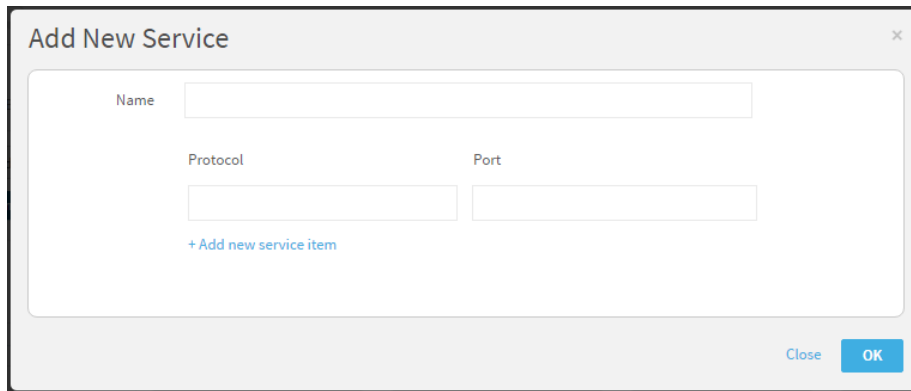
The new network object is added to the field.

Add a new service

To add a service to a flow:

1. Click **Add New Service**.

The **Add New Service** window appears.



The screenshot shows a dialog box titled "Add New Service" with a close button (X) in the top right corner. The dialog contains three input fields: "Name", "Protocol", and "Port". Below the "Protocol" field, there is a blue link that says "+ Add new service item". At the bottom right of the dialog, there are two buttons: "Close" and "OK".

2. In the designated fields, type the following information for the new service:


- Name
- Protocol
- Port

Note: If you've defined the **Protocol** as **ICMP**, use the **Port** field to define the ICMP type.

3. To add additional services to the service object, do the following:

- a. Click **Add new service**.

Additional **Protocol** and **Port** fields appear.

- b. Complete the fields.
- c. To remove a service, click  .

4. Click **OK**.

The new service object is added to the field.

Edit an application's flows

To edit a flow:

1. View the application for which you want to edit a flow. For more details, see [Business applications](#).

2. Click the **Flows** tab.

The **Flows** tab appears.

3. Click **Edit Flows**.

All the flows for the application appear in an editable format.

The screenshot shows the 'Billing' application configuration page in the Firewall Analyzer. The 'Flows' tab is active, displaying a table of application flows. The table has the following columns: Name, Source, User, Destination, Network Application, and Service. Two flows are listed:

Name	Source	User	Destination	Network Application	Service
1	FP_ext	Any	FP_int	Any	http
2	Azure_source	Any	Azure_destination	Any	ssh

4. To re-order flows, drag and drop the desired flows up or down.
5. Complete the fields as needed. For details, see [Flow fields](#).
6. Click **Save Changes**.

The **Save Changes** Dialog box appears.

- To save changes, click **Save Changes**.

The flow is updated, and this version of the application is saved as a draft revision.

- To save changes and apply the draft, do the following:

Note: The **Save and Apply Draft** option is disabled when the application has a revision pending implementation.

- a. Click **Save and Apply Draft**.

The **Apply Draft** dialog box appears, describing the FireFlow change request that will be created to add or remove traffic flows for the application in the network security policy. If traffic flows have been removed from the application, but the traffic intersects the needs of another application, a FireFlow change request will not be created to remove the traffic.


For more details, see [Business applications](#).

- b. Click **OK**.

The flows are updated and the draft is applied. This may take a few minutes.

Remove flows from your application

To remove a flow:

1. View the application for which you want to remove a flow. For more details, see [Business applications](#).
2. Click the **Flows** tab.
The **Flows** tab appears.
3. Click **Edit Flows**.
All the flows for the application appear in an editable format.
4. Click  on the row of the flow you want to remove.
5. Click **Save Changes**.

The **Save Changes** Dialog box appears.

- To save changes, click **Save Changes**.

The flow is updated, and this version of the application is saved as a draft revision.

- To save changes and apply the draft, do the following:

Note: The **Save and Apply Draft** option is disabled when the application has a revision pending implementation.

- a. Click **Save and Apply Draft**.

The **Apply Draft** dialog box appears, describing the FireFlow change request that will be created to add or remove traffic flows for the application in the network security policy. If traffic flows have been removed from the application, but the traffic intersects the needs of another application, a FireFlow change request will not be created to remove the traffic.

For more details, see [Business applications](#).

- b. Click **OK**.

The flows are updated and the draft is applied. This may take a few minutes.

Subscribe to another application's shared flows

Applications can subscribe to another application's shared flows. The subscribing application specifies a custom value for the shared flow's placeholder/missing field. For more details, see [Add flows to your application](#).

By default, the application containing the shared flow is responsible for all of the shared flow's subscriptions. If desired, you can configure AppViz to treat the applications subscribed to the shared flow as responsible for the traffic. For more details, see [Configure advanced AppViz properties](#)

To subscribe to an application:

1. View the application for which you want to add subscribed flows (the "subscriber" application). For more details, see [Business applications](#).

2. Click the **Flows** tab.

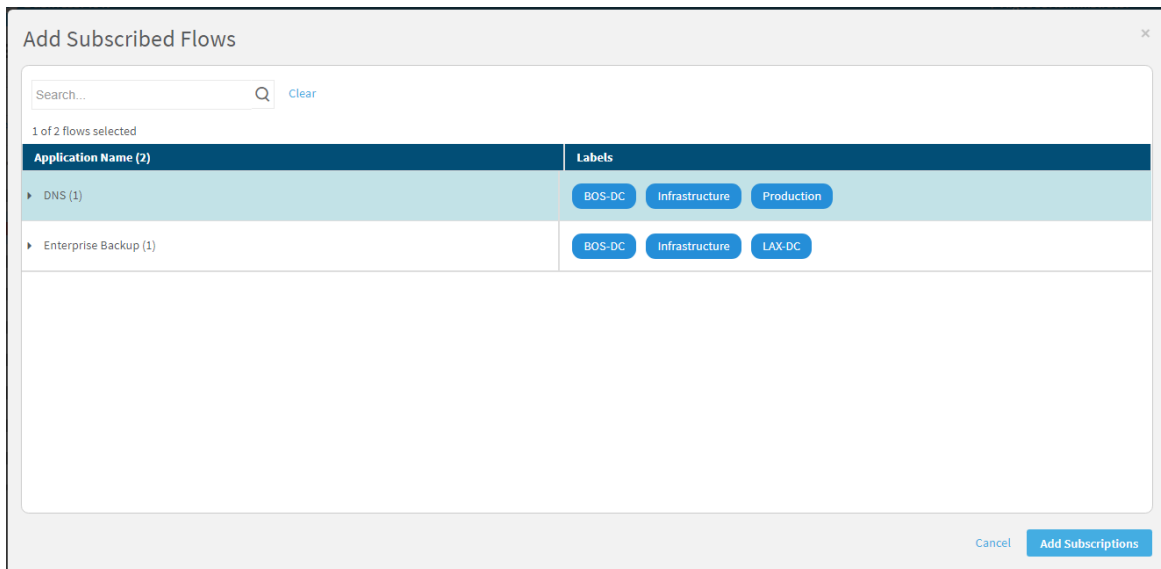
The **Flows** tab appears.

3. Click **Edit Flows**.

All the flows for the application appear in an editable format.

4. Next to the **Add Flow** button, click the **Subscribe to application...** link.

The **Add Subscribed Flows** window appears.



5. To subscribe to an entire application (all of its shared flows), select the desired applications.

6. To subscribe to individual flows, do the following:

- a. Next to the desired application, click  .

The applications flows appear.

- b. Select the desired flows.

7. Click **Add Subscriptions**.

The subscribed flows appear in the application's **Flows** tab.

The screenshot shows the 'Enterprise Backup' application page in the AppViz interface. The 'Flows' tab is active, displaying a table of flows. The table is organized into three sections: Application Flows, Shared Flows, and Subscribed Flows.

Name	Source	User	Destination	Network Application	Service	Comments
Application Flows						
2	Mgmt_Net	Any	Backup Servers	Any	HTTPS	
3	Backup Servers	Any	GRP-NTP-SERVERS	Any	NTP	Time Sync
Shared Flows						
1	Placeholder	Placeholder	Backup Servers	Any	backup, HTTPS	Publish Backup Application
Subscribed Flows						
DNS (4)	Backup Servers	Any	Internal DNS Servers	Any	DNS	Publish DNS se application

8. Complete the required fields as needed. For details, see [Add a new network object](#).

9. Click **Save Changes**.

A confirmation message appears.

10. Click **Save**.

Verify flow connectivity

Verifying flow connectivity checks whether the network security policy allows the traffic that the flow specifies.

To verify flow connectivity:

1. View the application which contains the flow for which you want to verify flow connectivity. For more details, see [Business applications](#).
2. Click the **Flows** tab.

The **Flows** tab appears.

3. Click  next to the flow.

AppViz checks whether the network security policy allows the traffic flow. This may take a few minutes, depending on the complexity of the flow and network policy.

If the flow is blocked, red stripes appear around the flow.

4. To view details regarding the flow's connectivity, click the **Connectivity** link.

A new window opens with details of the traffic simulation query from AlgoSec Firewall Analyzer.

Note: If the **Connectivity** link is not enabled for a flow, the last connectivity check failed or has expired. If you run a new check, the link will be re-enabled.

Export an application's flows

You can export an application's flows to a CSV file.

Note: If desired, you can configure all flow exports to include connectivity information. For more details, see [Configure advanced AppViz properties](#)

To export an application's flows:

1. View the application for which you want to add a flow. For more details, see [Business applications](#).

2. Click the **Flows** tab.

The **Flows** tab appears.

3. Click  **Export to CSV**.

The CSV file is exported.

Your browser will prompt you to open or save the file.

Discover applications

This topic describes how to discover business applications and import them and their flows into AppViz.

Discover applications via AutoDiscovery or Cisco Tetration




This procedure describes how to discover applications automatically, either via AlgoSec AutoDiscovery or Cisco Tetration.

Note: In order to discover applications automatically, you must configure an AutoDiscovery or Tetration server in the AppViz **Administration** area.

For more details, see [Discovery settings](#).

Do the following:

1. In AppViz, click **DISCOVERY** from the navigation menu on the left, and then click:

 AutoDiscovery	Discover applications and flows using a configured AlgoSec AutoDiscovery server.
 Cisco Tetration	Discover applications and flows using a configured Cisco Tetration server.
 Import Flows from File	<p>Import flows from a prepared CSV file. This is especially helpful when exporting flows from AFA, where you can use the policy as stored in AFA to create the CSV file.</p> <p>Do the following:</p> <p>Click Select File to browse and select the file to import.</p> <ul style="list-style-type: none"> • Download a sample file if needed. For more details, see Update data via CSV files. • If you are working in AFA, export flows directly from the AFAPolicy tab. For details, see Export flows directly from AFA. <p>AppViz displays a summary of the applications and flows found. If AppViz failed to import many lines, you may have a small + at the end of the line. Click the small + to expand the list fully.</p> <p>To continue with your import, click Next.</p>



2. AppViz starts pulling discovered applications from the selected source. When complete, results are displayed in a table with the following columns:

Discovered applications	The name of the business application discovered via AutoDiscovery or Tetration.
# of connections	The number of connections found for the discovered application.

AppViz applications	<p>The AppViz application mapped to the discovered application. The default AppViz application name is the name of the discovered application.</p> <ul style="list-style-type: none"> • If an AppViz application already exists with the same name, any newly discovered flows are added to the existing AppViz application. • If no AppViz application is found with the same name, a new AppViz application is created.
----------------------------	---

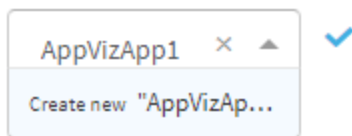
Edit the mapped AppViz application name


To edit the name assigned to the AppViz application by default, do the following:

- Click  next to the AppViz application name.
- Either select another existing application from the dropdown list, or click  to clear the current value and enter a new name.



If you enter a new name, click **Create new** under the text box to confirm the name.

For example:



- Click the  to save your changes.
- Click **Next** to continue.

AppViz displays a summary of the applications and flows that AppViz will import or create.

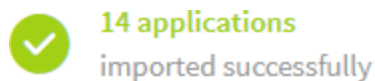
A list of flows is collapsed under each relevant AppViz application. Click the arrows ( and ) to expand or collapse the flows.

Note: If your system is configured to optimize traffic flows, the flows are displayed after optimization. This means you'll have a lower count of flows than what AppViz originally detected. For more details, see [Configure advanced settings](#).

Tip: By default, all AppViz applications and flows are selected for import. Clear the checkbox next to each application or flow that you do not want AppViz to create at this time.

4. Click **Import**. AppViz starts importing the selected applications and flows.

When complete, AppViz displays the results of any applications imported successfully, partially, or if any applications failed. For example:




5. Click **Finish** to return to the main **Discovery** page.

The new applications are listed in the **APPLICATIONS** area in AppViz, and will be synchronized with AFA as configured.

Export flows directly from AFA

This procedure describes how AFA users can export business application flows directly from the AFA **Policy** tab into AppViz.

 [Export Policy Rules from AFA](#): Watch to learn about exporting flows from AFA.

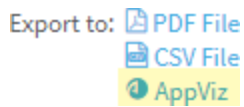
Do the following:

1. In AFA, view the device, group, or matrix you want to export flows from.
2. Click the **Policy** tab to display the associated rules, and select the rules you want

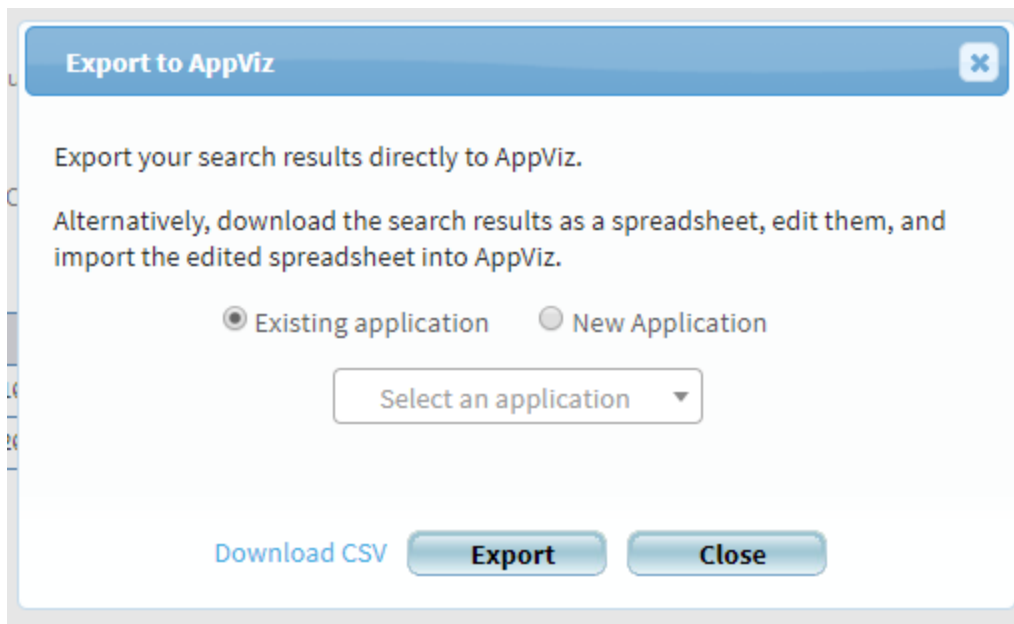
to export into AppViz flows.

- Use the filter to modify the rules displayed.
- Selecting the checkbox in the header row selects all the rules on the page you are viewing only, and not all of the flows on all pages.

3. At the top right, above the table, click **Export to: AppViz**.



The **Export to AppViz** dialog box appears.



4. In the **Export to AppViz** dialog, do the following:

<p>Define your application</p>	<p>Select whether to export the selected rules to an existing application, or to a new application.</p> <ul style="list-style-type: none"> • If you select Existing Application, select the application from the dropdown list. • If you select New Application, enter the application name in the text box that appears.
---------------------------------------	---

<p>Export or download the flows</p>	<p>Do one of the following:</p> <ul style="list-style-type: none"> • Click Export to export the selected rules directly to AppViz as business flows. <p>The flows are transferred to the specified application in AppViz, and a success message appears.</p> <p>To view the updated application, click Open application, and then click OK.</p> <p>For more details, see Rules that are not imported automatically.</p> <ul style="list-style-type: none"> • Alternately, click Download CSV to download a file with the flow definitions. <p>When you're ready, import these into AppViz. For details, see Discover applications via AutoDiscovery or Cisco Tetration</p>
--	--

Rules that are not imported automatically

The following types of rules are not imported automatically:

- Disabled rules
- Deny rules
- Rules with drop actions
- Rules that already exist in AppViz

If some of your selected rules cannot be imported, AFA provides a CSV to download containing the rule details.

Edit the CSV file if needed, and then use it to import the rules into AppViz manually. For details, see [Update data via CSV files](#).

Application diagram

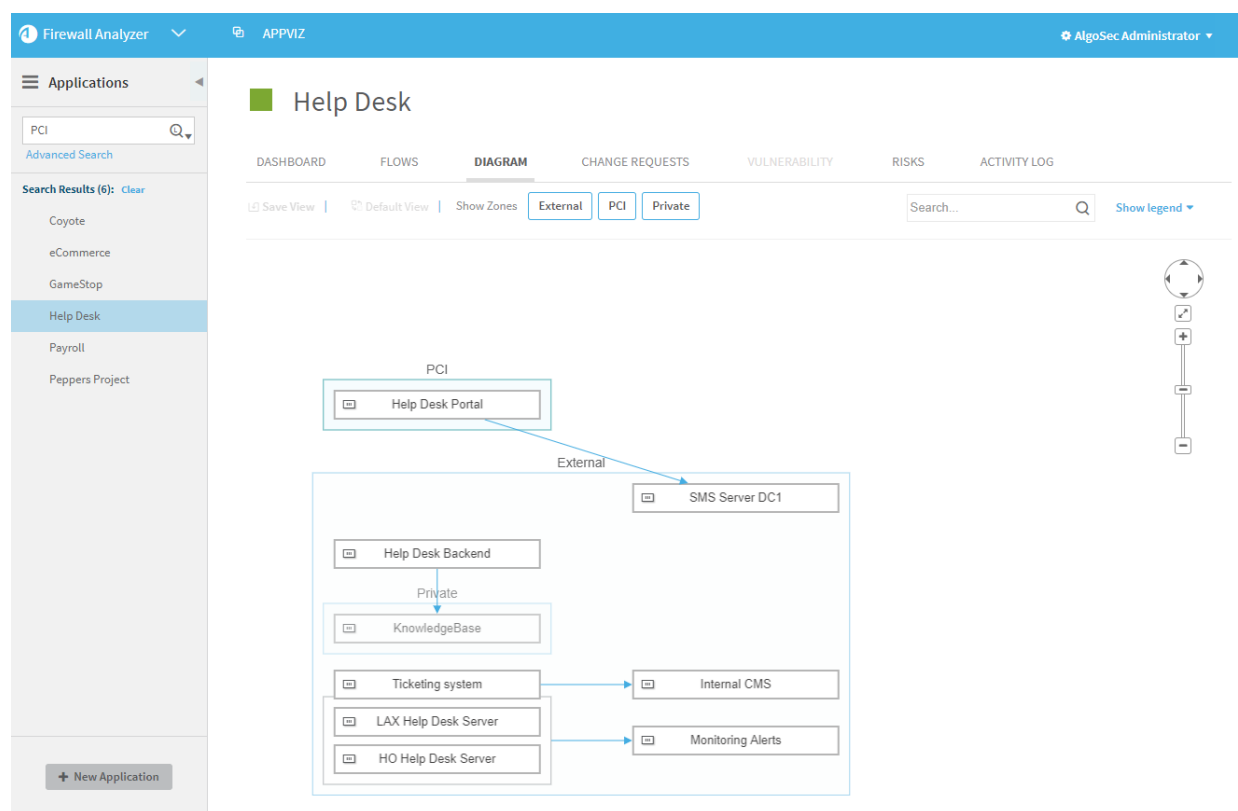
This topic describes the application's DIAGRAM tab, which represents all of the application's flows visually.

DIAGRAM tab interface

The traffic flows from left to right, and every object appears exactly once. Subscribed flows as well as application flows appear in the diagram.

To modify the diagram, see [Modify the application diagram](#).

To search the diagram, see [Search the application diagram](#).



Nodes

Each node represents a network object.

- Hovering over an object displays a tooltip with its contents.



- Clicking on an object opens a window displaying object details and a link to the object's AppViz page.

- When vulnerability assessment is configured, the color of the border around an object indicates the object's vulnerability score. For more details, see [Application vulnerability](#).

Arrows

Each arrow represents a flow (and specifically, the flow's service).

- Red arrows indicate the flow is blocked. All other arrows are blue.
- Hovering over an arrow displays a tooltip with the flow's name (as a link) and its service.



Clicking on the link in the tooltip brings you to the flows tab and the specific flow appears highlighted in pink.

Pension Management - pensionmgmt (Draft)

DASHBOARD **1 Blocked** FLOWS DIAGRAM CHANGE REQUESTS VULNERABILITY RISKS ACTIVITY LOG

[Export to CSV](#) [Edit Flows](#)

▼ Application Flows


Name	Source	User	Destination	Network Application	Service
1	192.168.10.55	Any	192.168.12.45	Any	TCP
2	192.0.0.0/8	Any	192.168.10.55	Any	Ap
3	192.168.10.55	Any	192.168.12.46	Any	TCP

Zones

Objects appear grouped by zones.

- The icon indicates that the object spans zones. In the diagram, the object will appear in its most relevant zone, defined as follows:

1. PCI
2. Defined in risk profile spreadsheet
3. Internal
4. External

Note: Objects in the internal zone in addition to another zone are not marked with the  icon.

- To specify objects should not be grouped by a specific zone, see [Modify the application diagram](#).
- To customize zone definitions and how they appear in the diagram, see [Security zones](#).

Modify the application diagram

Note: All saved modifications will appear wherever the application diagram appears (including in FireFlow).

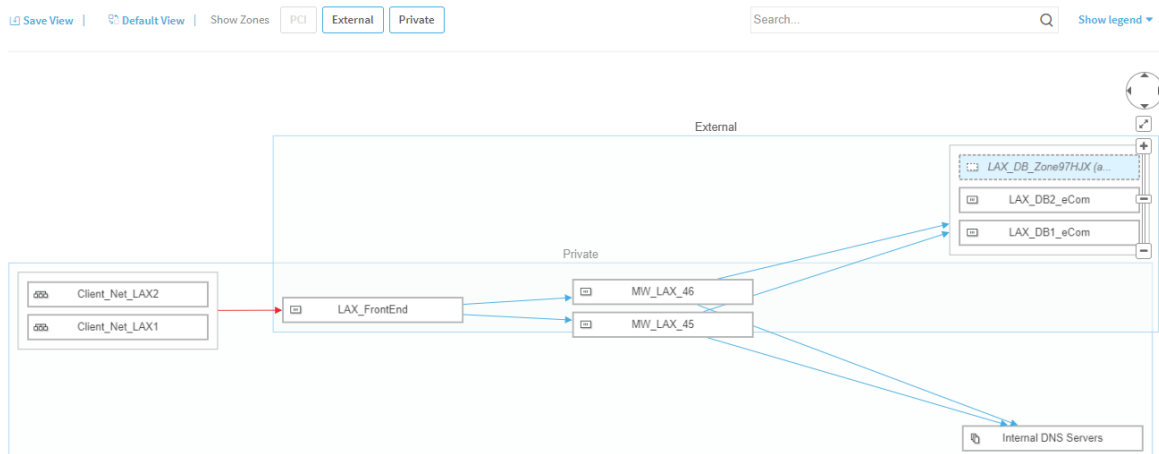
To modify the application diagram:


1. View the application. For details, see [Business applications](#).
2. Click the **Diagram** tab.

The **Diagram** tab appears.

3. To specify objects should not be grouped by a specific zone, select the zone's button in the **Show Zones** area.


The zone button appears disabled. The objects in the zone still appear in the diagram, but they are no longer grouped by the zone.





Note: Objects which span zones (and are marked with ) will not appear in their other zones when their most relevant zone is disabled. Conversely, objects in the internal zone as well as another zone will move to the internal zone when their most relevant zone is disabled.

4. To move the entire diagram, do one of the following:

- Drag and drop the diagram (by clicking an empty space).

- Click the directional arrows: .

5. To change the size of the diagram, do one of the following:

- To zoom in or out, use the zoom slider: .
- To revert to the default zoom, click .

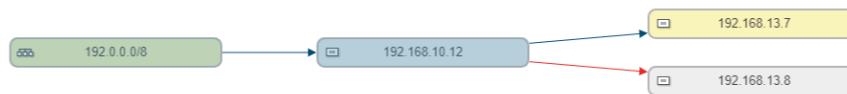
6. To move objects, do one of the following:

- To move a single object, drag and drop the node.
- To move multiple objects, do the following:

7. Select multiple nodes by doing one of the following:

- While holding CTRL or SHIFT, select the desired nodes individually.
- While holding CTRL or SHIFT, drag a selection area around the desired nodes.

The selected nodes are highlighted in blue. Nodes that were already highlighted in yellow (because they are search results) are highlighted in green.



The blue and green objects are selected and ready to be moved.

The yellow and green objects are search results. For information about searching the diagram, see [Search the application diagram](#).

8. Drag and drop the group of nodes.

Note: You cannot move member objects within their group, only the entire group as a single node.

9. To revert to the diagram's default layout, click **Default View**.

Reverting to the default layout discards all manual changes that have ever been made to the diagram.

10. To save the changes you made to the diagram, click **Save View**.

The diagram's modifications are saved.

Search the application diagram

You can search the diagram for any text or IP address. The search results will be network object nodes and/or service object arrows.

To search the application diagram:

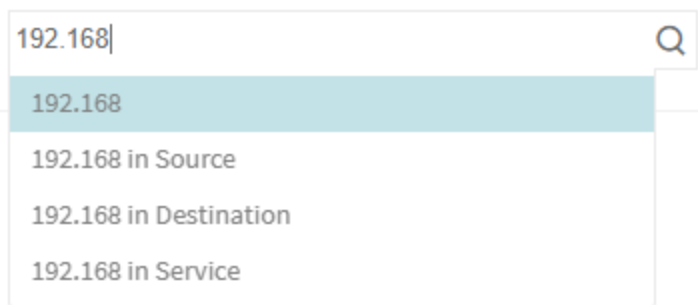
1. View the application. For details, see [Business applications](#).

2. Click the **Diagram** tab.

The **Diagram** tab appears.

3. In the search field, type the text or IP address to search.

A drop-down menu appears, allowing you to specify whether to search all fields or a specific field.



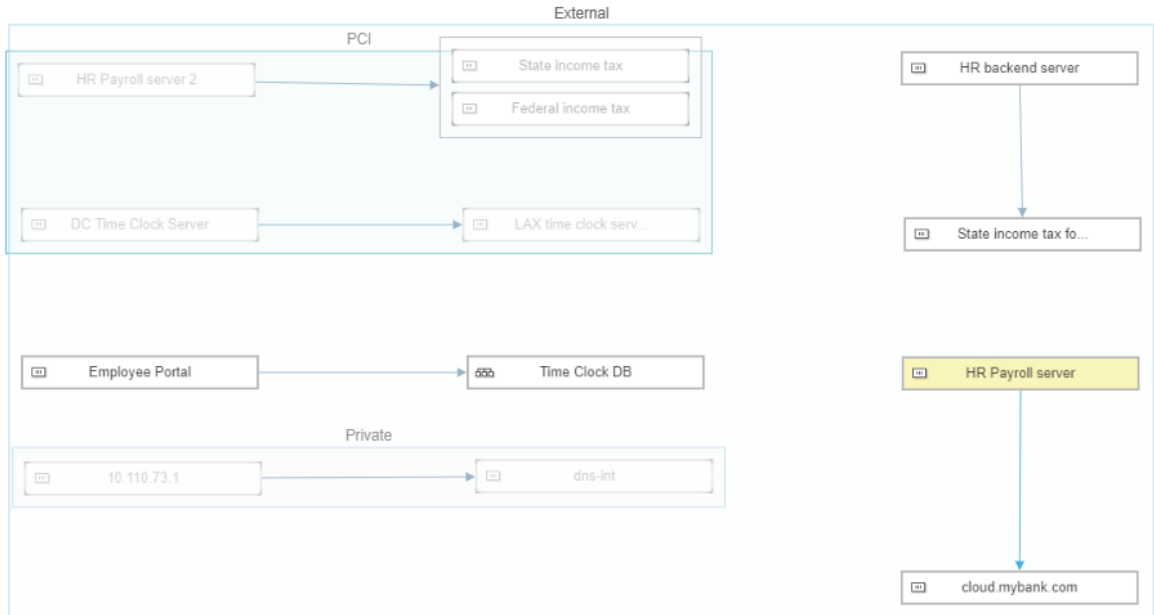
4. Select the desired option in the drop-down menu.

The search parameter you specified appears in the search box.



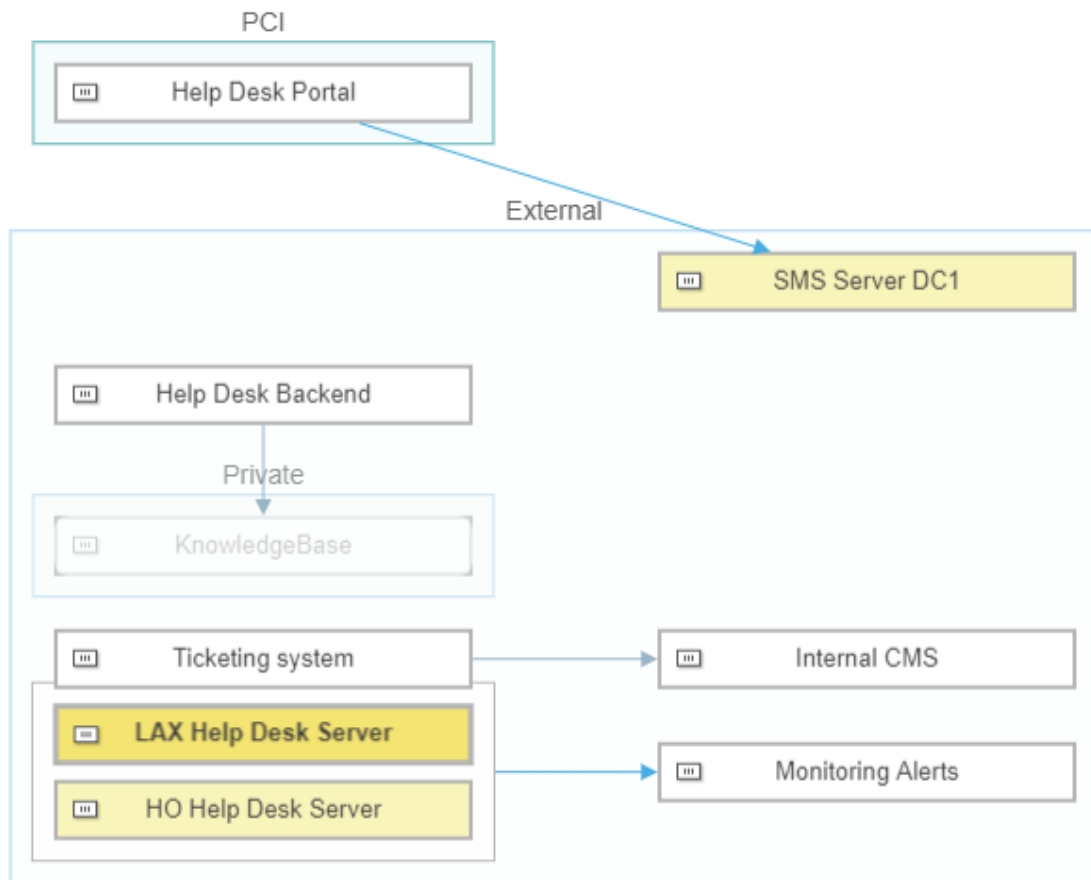
If desired, specify additional parameters.

The search results appear in yellow and become the focus of the map.



5. To view the list of search results, click **Results**.
6. To find on a specific result, select it in the **Results** list.

The map focuses on the specific result and its associated elements in the relevant flow. The result becomes highlighted in a deeper yellow color.



7. To clear the search, click the **Clear** link.

Application change requests

This topic describes the application's **CHANGE REQUESTS** tab, which displays details for all FireFlow change requests that have been created for the application or objects being used by the application.

CHANGE REQUESTS interface

The screenshot shows the FireWall Analyzer interface for the SugarCRM application. The 'CHANGE REQUESTS' tab is active, displaying a table of change requests. The table is divided into two sections: 'Application traffic changes (1)' and 'Object changes (1)'. The 'Application traffic changes' section contains one entry with ID 4015, Status 'Implement', and a summary 'BusinessFlow Change Request for SugarCRM'. The 'Object changes' section contains one entry with ID 4023, Status 'Rejected', and a summary 'BusinessFlow Change Request for Apache httpd 2.2.25'. The table columns are ID, Status, Change Request Summary, Issue Date, Issued By, and Revision.

ID	Status	Change Request Summary	Issue Date	Issued By	Revision
4015	Implement	BusinessFlow Change Request for SugarCRM	15/08/2016 14:57	AlgoSec Administrator	1
4023	Rejected	BusinessFlow Change Request for Apache httpd 2.2.25	15/08/2016 15:03	AlgoSec Administrator	

View relevant FireFlow change requests

To view relevant FireFlow change requests:

1. View the application, network object, or service object for which you want to view a relevant change request.

For details, see [Business applications](#), [Network objects](#), and [Service objects](#).

2. Click the **Change Requests** tab.

The **Change Requests** tab appears.

3. To change the sort order of the list, click the desired column heading. To reverse the sort order, click the heading again. The sort direction is indicated by the white triangle in the location of the sort icon (▾).

4. Click the change request you wish to view.

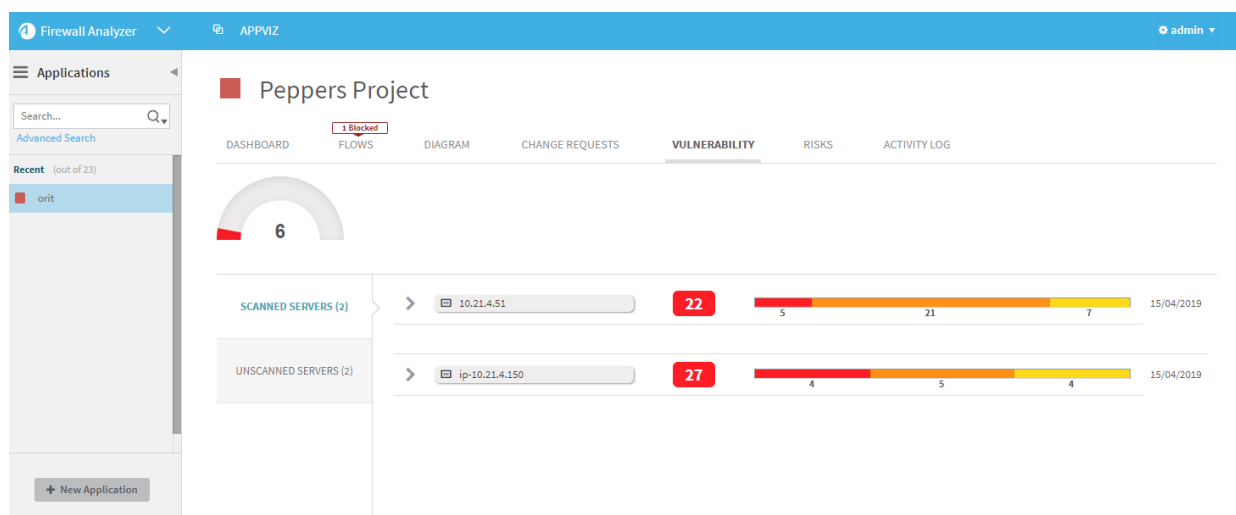
A new window opens, displaying the change request in FireFlow.

Application vulnerability

This topic describes the application's **VULNERABILITY** tab, which lists the vulnerabilities associated with the servers used by the application.

This tab is enabled when vulnerability assessment is configured. For more details, see [Manage vulnerability assessment scanners](#).

VULNERABILITY interface



Note: This tab is shown only when AppViz has at least one vulnerability scanner configured and scan results to display. For details, see [Manage vulnerability assessment scanners](#).

The application's vulnerability score is displayed in gauge at the top of the page, from **0** (many vulnerabilities, shown in red) to **100** (no vulnerabilities, shown in green). The gauge also shows the percentage of servers that are being scanned.

Below, the servers associated with the application are listed either on the **SCANNED SERVERS** or **UNSCANNED SERVERS** tabs. Unscanned servers are those servers for which AppViz has no vulnerability data.

Vulnerability assessment ratings

AppViz calculates security ratings for servers and applications. Ratings range from 0-100, where 100 is the best score, with no vulnerabilities.

Security ratings are color-coded to indicate severity as follows:

- Scores between **85-100**: Green
- Scores **80-85**: Yellow
- Scores **0-50**: Red

AppViz assigns each vulnerability found with a CVSS score, and then uses all of the CVSS scores for a specific server to calculate that server's security rating. The server security rating is calculated using the following formula:

$$100 * [1 - (\text{Min}(\text{Tv}_h, 50) + \text{Min}(\text{Th}, 20) + \text{Min}(\text{T}_m, 10) + \text{Min}(\text{TI}, 5)) / (50 + 20 + 10 + 5)]$$

Where:

- **T_{vh}** = Sum of all CVSS scores with **10 > score > 6.9**
- **Th** = Sum of all CVSS scores with **6.9 > score > 3.9**
- **T_m** = Sum of all CVSS scores with **3.9 > score > 1.9**
- **TI** = Sum of all CVSS scores with **1.9 > score > 0**

Application severity is the average of security ratings for its half lowest scored servers.

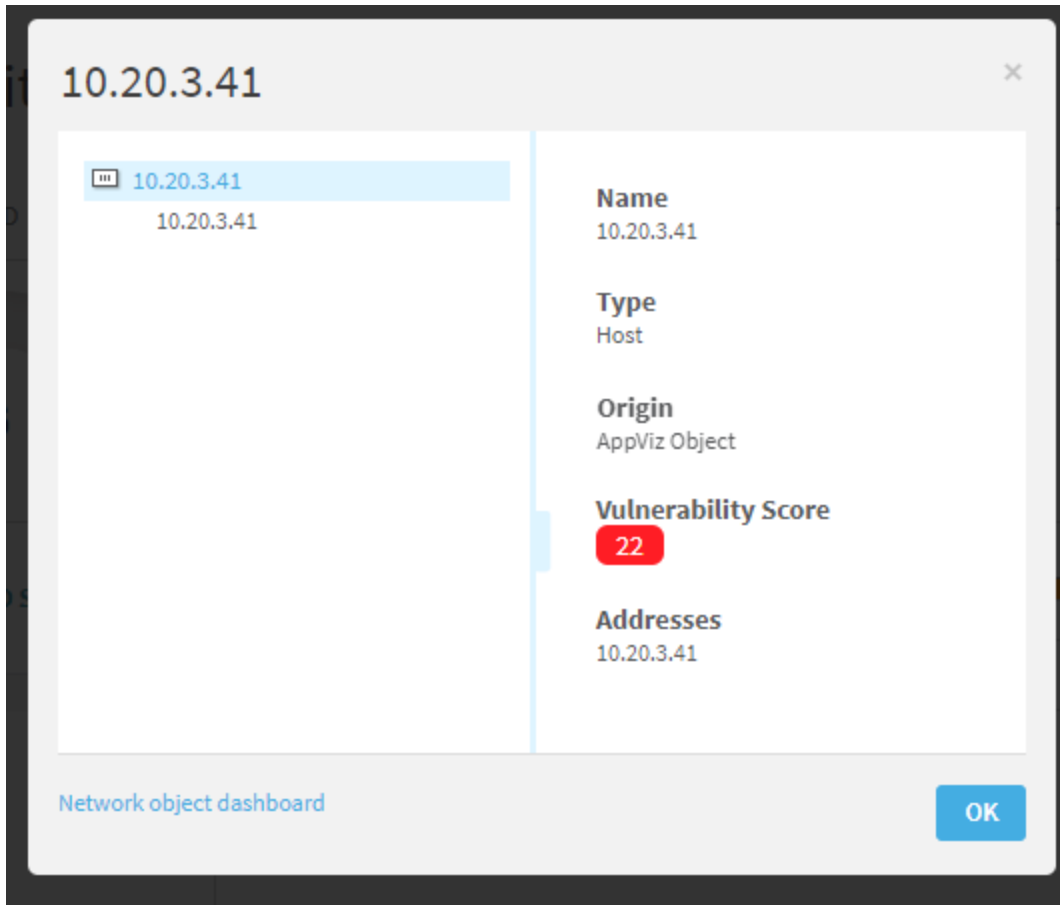
Scanned servers

For each server scanned, AppViz shows the relevant network object, vulnerability score, summary color strip, and the date of the last scan. For network objects that represent multiple IP addresses, the vulnerabilities for all relevant IP addresses are included.

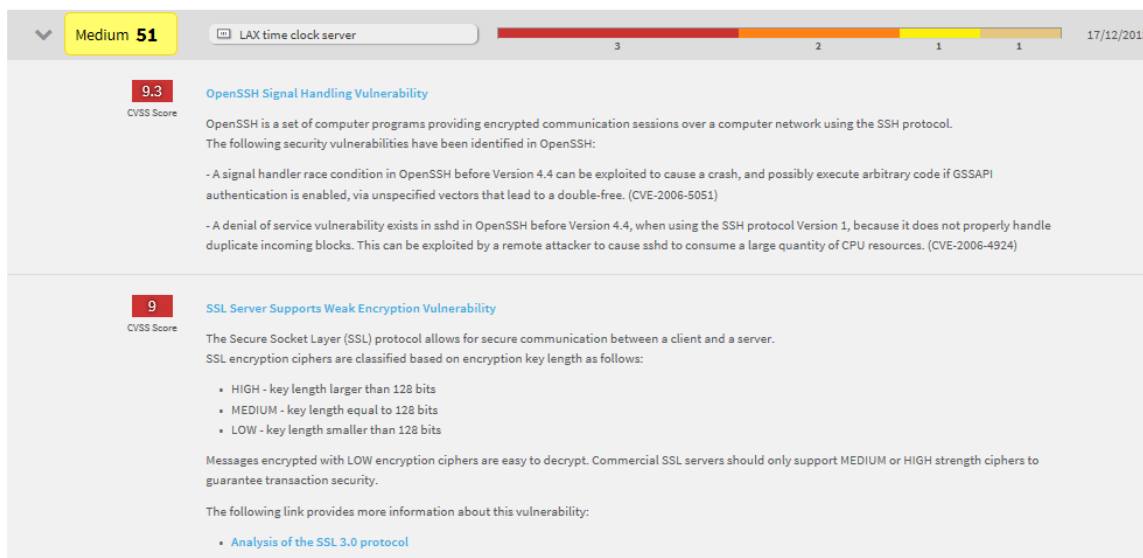
Do one of the following:

- Click the network object name to display details about the network object in a popup. From there, click **Network object dashboard** to jump to the network object

details page.



- Click the arrow > for each server to expand the details of each vulnerability found.
For example:



From there, click a vulnerability name to drill down for more details from the scanner’s system.

Vulnerability scores

AppViz provides a security rating between 0-100 for each network object, as well as for each application.

The higher the security rating, the more secure the application or network object is. The colors indicate the security rating as follows:

	Low (0-30)
	Medium (31-60)
	High (61-90)
	Very high (91-99)
	No vulnerabilities found (100)
	No scan data found

Score calculation

Scores are calculated using the Common Vulnerability Scoring System (CVSS). Each vulnerability found is assigned a CVSS score. AppViz uses all CVSS scores for a

specific server to calculate that server's security rating.

AppViz uses the following formula to calculate the security rating for each server:

$$\text{Server severity score} = 100 * [1 - (\text{Min}(\text{Tvh}, 50) + \text{Min}(\text{Th}, 20) + \text{Min}(\text{Tm}, 10) + \text{Min}(\text{TI}, 5)) / (50 + 20 + 10 + 5)]$$

where :

- **Tvh** = Sum of all CVSS scores with **10 > score > 6.9**
- **Th** = Sum of all CVSS scores with **6.9 > score > 3.9**
- **Tm** = Sum of all CVSS scores with **3.9 > score > 1.9**
- **TI** = Sum of all CVSS scores with **1.9 > score > 0**

An application's severity is the average of all security ratings for its half lowest scored servers.

Application risks

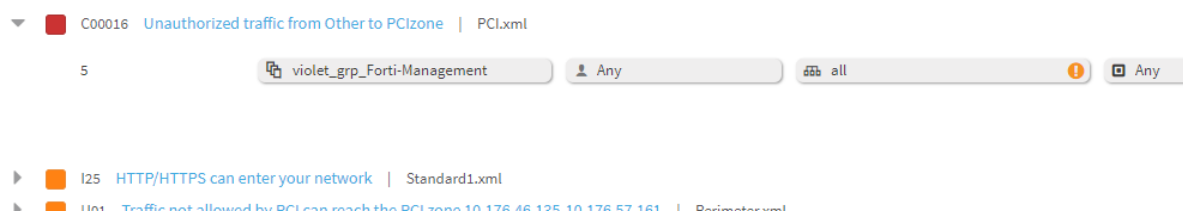
This topic describes the application's RISKS tab, which describes the risks associated with the application.

The screenshot displays the AppViz interface for the 'Peppers Project' application. The top navigation bar shows 'Firewall Analyzer' and 'APPVIZ'. The left sidebar lists various applications, with 'Peppers Project' selected. The main content area shows the 'RISKS' tab, featuring a green gauge indicating a 97% risk score, updated on 09/11/2015 08:58. Below the gauge are two view options: 'VIEW BY FLOWS' and 'VIEW BY RISKS', with the latter selected. A 'Sort by:' dropdown is set to 'High to low'. The risk list includes:

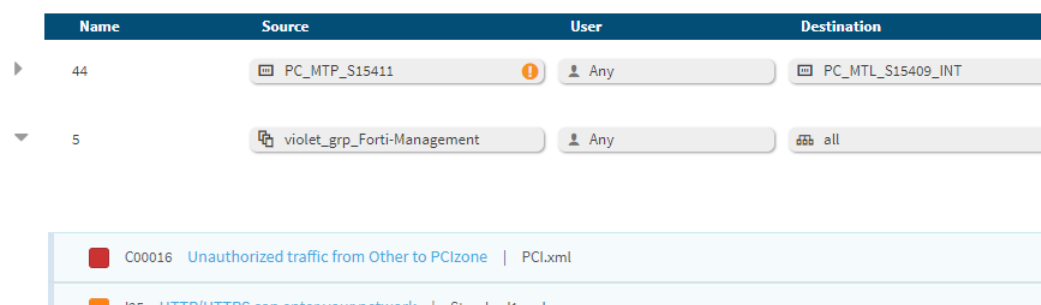
- C00016 Unauthorized traffic from Other to PCIzone | PCI.xml
- I25 HTTP/HTTPS can enter your network | Standard1.xml
- U01 Traffic not allowed by PCI can reach the PCI zone 10.176.46.135-10.176.57.161 | Perimeter.xml
- C00017 Unauthorized traffic from Other to Net1,Net2,PartnerNet | PCI.xml
- C00018 Unauthorized service from Other to Net3 | PCI.xml
- D04 Risky Microsoft services between internal networks | PCI.xml
- R09 "Any destination" rules | PCI.xml

The AlgoSec Firewall Analyzer provided **Risk Score** and the date of the last risk update appear at the top of the page.



The **VIEW BY RISKS** tab provides a list of all the risks associated with the application. You can sort the risks using the **Sort by** drop-down menu. To view the flows associated with a risk, click ▶.



The **VIEW BY FLOWS** tab provides a list of all the applications flows. You can sort the flows using the **Sort by** drop-down menu. To view the risks associated with a flow, click ▶.



To view the details of a risk in AFA, click the name of the risk.

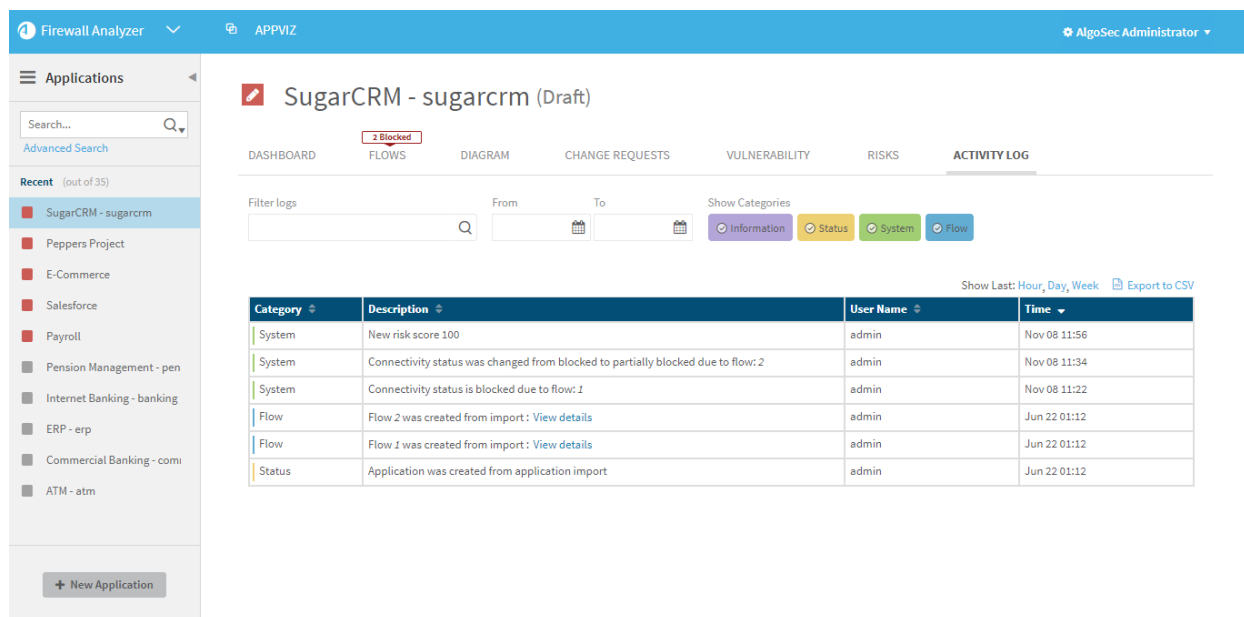
To manually refresh an application's risk information, click . If a change has been made to an application revision since the last risk update, the risk information may be outdated or no longer relevant. In this case,  appears next the the **Risks** tab.

To export the risk information for the application to a CSV file, click  [Export to CSV](#).

Application activity log

This topic describes the application's **ACTIVITY LOG** tab, which displays a log of all actions that affected the application.

ACTIVITY LOG interface



Column	Description
Category	The activity's category: Flow, Information, Status, or System.
Description	Description of the activity.
User Name	Name of user who performed the activity.
Time	Date and Time the activity occurred.


Filtering Activity Logs

To filter and sort activity logs:

- To filter the logs by a textual search, do the following:
 1. Type your search text into the search box.

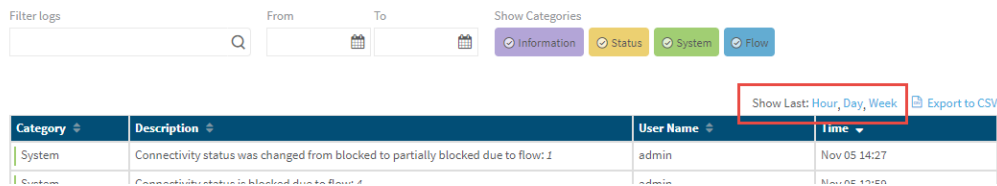
A drop-down menu appears, allowing you to specify whether to search all fields or a specific field.
 2. Select the desired option in the drop-down menu.

The search parameter you specified appears in the search box.

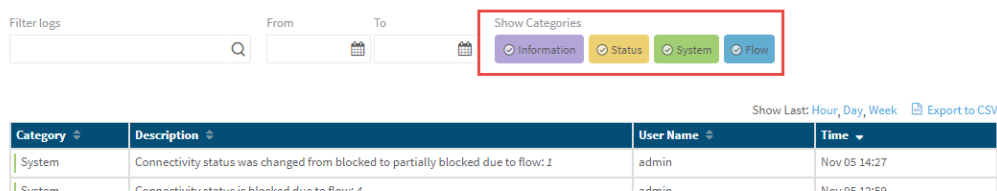
3. If desired, specify additional parameters.
4. Click  .

The logs which do not satisfy the search parameter(s) you specified are removed from the log list.

- To filter the logs by **Time**, do one of the following:
- To filter out all logs before a date, click on the calendar icon in the **From** field, and select the date.
- To filter out all logs after a date, click on the calendar icon in the **To** field, and select the date.
- To filter out all logs outside a range of dates, select dates for both the **From** and **To** fields.
- To filter out all logs that did not occur within the last hour, day or week, click the desired link in the **Show Last** field.



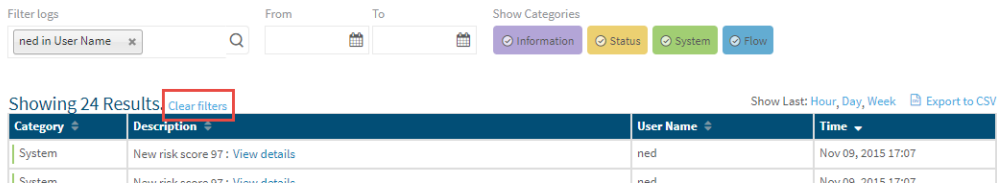
- To filter the logs by **Category**, click one or more of the **Show Categories** buttons.



All logs which do not have one of the specified categories are removed from the log list.


- To sort the logs by a specific column, click the desired column header.
- To reverse the sort order, click the heading again.

- To clear all filters, click the **Clear filters** link.



Exporting Activity Logs

To export activity logs to a CSV file:

1. View the **Activity Log** tab.
2. Click  **Export to CSV**.

Your browser will prompt you open or save the file.

Analyze application impact

This topic describes how to perform an **application impact analysis**, which searches for applications by servers or devices.

Sort search results by name, date modified, or connectivity, and view any application flows relevant to the search.

Note: This search feature only returns active, pending, and draft revisions. It does not search history or rejected revisions.

Do the following:

1. From the AppViz HOME page, in the **Impact Analysis** area, complete the fields as follows:

Servers	Type a server name or IP address for the server you want to search for, or click Network object lookup to select a server using the Server Lookup wizard. For details, see Business applications .
----------------	--

Devices	Type a device name.
Vulnerabilities	Type the CVE identifier or vulnerability description. Note: Relevant only when vulnerability assessment is configured.

2. Click **Search**.

The **Search Results** appear in the workspace.


The screenshot shows the 'Search Results' page in the AppViz interface. The page title is 'Search Results' and it indicates 'Found 20 revisions'. A 'Sort by:' dropdown menu is set to 'Name'. On the right, there is an 'Export to CSV' button. The main content area displays a table of search results with the following columns: Application Name, Date, Lifecycle Phase, and Status.


Application Name	Date	Lifecycle Phase	Status
Coyote	18/11/2014	Planning	Active
Coyote	18/11/2014	Planning	Pending Implementation
DNS	20/10/2015	Planning	Active
Domino Server / Lotus Notes	14/02/2013	Pre Production	Active
eCommerce	20/10/2015	Planning	Active
Email	18/11/2014	Planning	Pending Implementation
Email	03/11/2014	Planning	Active
Email	24/10/2015	Planning	Draft
Enterprise Backup	20/10/2015	Planning	Draft
Enterprise Backup	23/02/2015	Planning	Active
Help Desk	23/11/2014	Production	Active
LDAP	20/10/2015	Planning	Active
Local Backup	26/10/2015	Planning	Pending Implementation
Payroll	28/10/2015	Production	Active
Pappers Project	01/12/2014	Production	Active
POP3 - Incoming Mail	11/02/2013	Production	Active
Telepresence	23/11/2014	Pre Production	Pending Implementation
WebAccess - rose checkpoint	18/11/2014	Planning	Pending Implementation
WebAccess - rose checkpoint	01/12/2014	Planning	Active

Each application appears with the following information:

- date the application was last modified
- lifecycle phase
- revision status

Do any of the following:

- **Sort the applications shown.** Select an option from the **Sort by** field at the top of the page.
- **View the flows** for a specific application that are relevant to your search. Click the  to the left of the application.

- **Export search result data.** Click  [Export to CSV](#). Exported data includes application, sources, destinations, services, comment, and name.

Application contacts

This topic describes how to view, add, remove and edit application contacts.

The directory of contacts is used to inform relevant people of application changes.

Contacts from the directory are associated with specific applications; each application contact is assigned a specific role. All contact information for an application is displayed in the **Contacts** area of the application DASHBOARD tab.

For more details, see [Application dashboard](#).

View application contacts

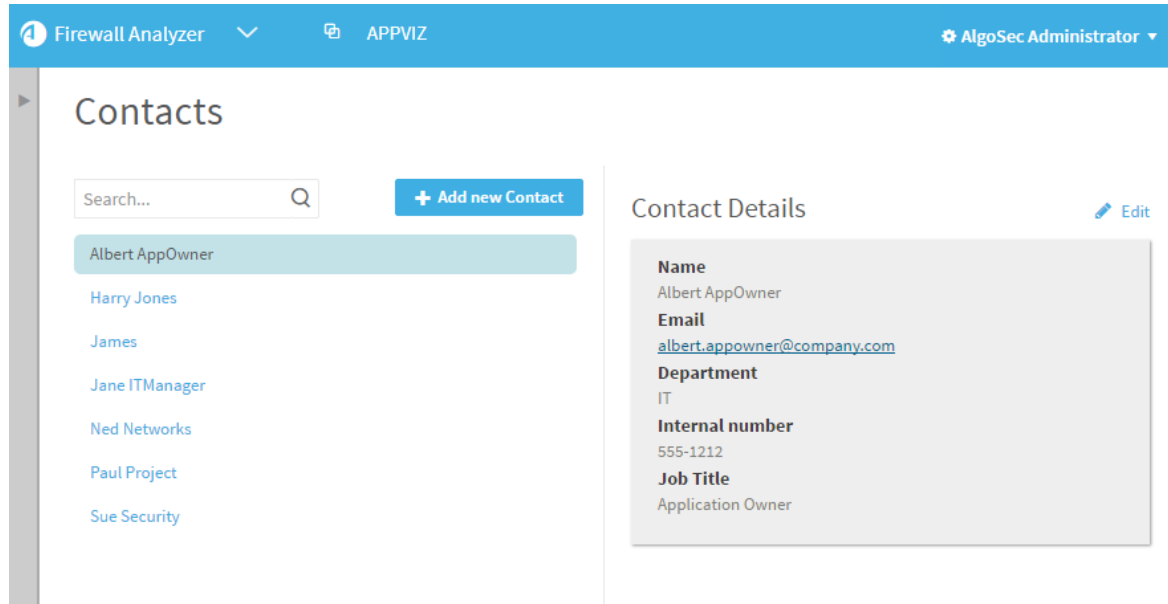
To view a contact:


1. In the toolbar, click your username.

A drop-down menu appears.

2. Click **Contacts**.

The **Contacts** area appears in the workspace.



3. To search for a contact, type any part of the contact's name in the search field, and click .

All contacts containing the string you entered are displayed.

4. Click the desired contact's name in the list below the search field.

The contact's details are displayed in the workspace.

Add application contacts

To add a contact:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Click **Contacts**.

The **Contacts** area appears in the workspace.

3. Click **+Add new Contact**.

The **Add new contact** area appears in the workspace.

The screenshot shows a web interface for adding a new contact. The title is 'Add new contact'. Below the title are seven input fields, each with a label to its left: 'First name', 'Middle name', 'Last name', 'Email', 'Department', 'Internal number', and 'Job Title'. At the bottom left of the form area are two buttons: 'Cancel' and 'Save Changes'.

4. Complete the fields as needed.

Contact fields

In this field...	Do this...
First name (mandatory)	Type the contact's first name.
Middle name	Type the contact's middle name.
Last name (mandatory)	Type the contact's last name.
Email (mandatory)	Type the email address.
Department	Type the department name.
Internal number	Type the contact's internal telephone number.
Job Title	Type the job title.


Note: Custom contact fields may appear. For more details, see [AppViz maintenance](#).

5. Click **Save Changes**.

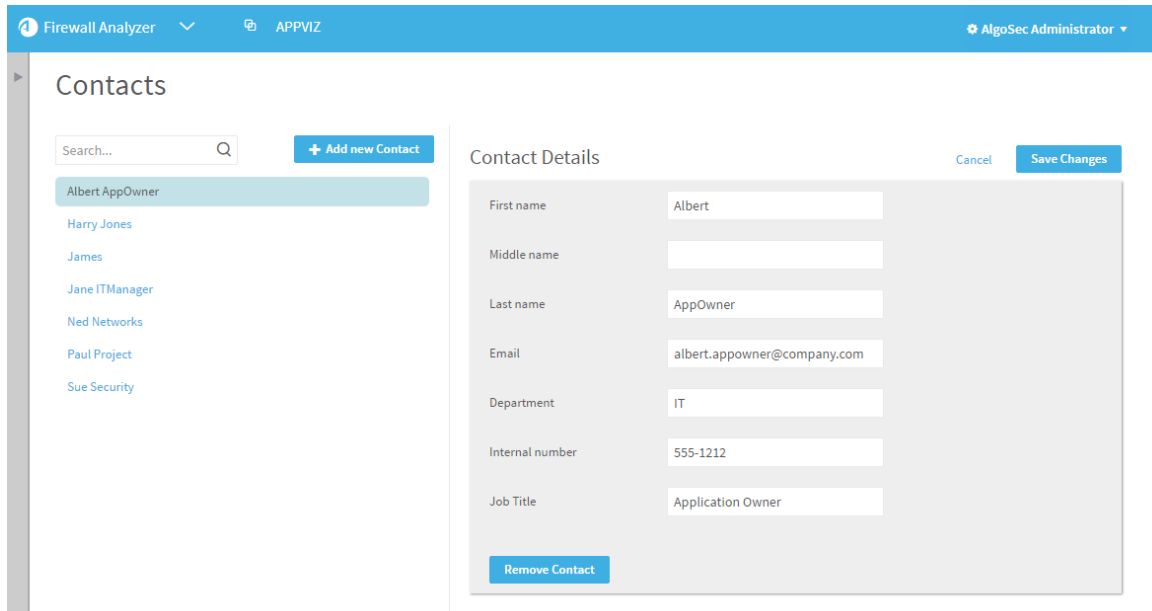
The contact is added.

Edit an application's contacts

To edit a contact:

1. View the contact you want to edit. For details, see [View application contacts](#).
2. Click .

The contact's information appears in editable fields.



The screenshot shows the 'Contacts' management interface. On the left, a list of contacts is displayed with 'Albert AppOwner' selected. On the right, the 'Contact Details' form is open, showing the following information:


First name	Albert
Middle name	
Last name	AppOwner
Email	albert.appowner@company.com
Department	IT
Internal number	555-1212
Job Title	Application Owner

3. Update the fields as needed. For details, see [Contact fields](#).
4. Click **Save Changes**.

The contact's new information is saved.

Removing an application contact

To remove a contact:

1. View the contact you want to remove. For details, see [View application contacts](#).
2. Click .

The contact's information appears in editable fields.

3. Click **Remove Contact**.

The **Remove Contact** dialog box appears.



4. Click **OK**.

The contact is removed.

Network objects


This section describes how to manage network objects in AppViz.

Manage network objects

Do any of the following:

- View an overview of all network objects and edit, clone, or delete them. For details, see [Network object dashboard](#).
- View an overview of each network object. For details, see [View a network object](#).
- Create new network objects. For details, see [Add and edit network objects](#).
- View the applications that include a specific network object. For details, see [Network objects applications](#).
- View the change requests that involve the network object. For details, see [Network object change requests](#).
- View activity logs for a specific network object. For details, see [Network object activity logs](#).

Note: If two device objects with the same name have different content, the device on which the objects were defined will be indicated throughout the Web Interface.

Tip: To return to the other areas available from the main menu, click the hamburger menu  at the top left, and select the page you want to navigate to.

Abstract objects

Network objects may be identified as abstract objects.

Abstract objects are network objects without defined content. You can use abstract objects to help you design an application flow before you know all the network details, such as type and IP address. Abstract objects appear in pale blue and with *(abstract)* after their name in flows and in the application diagram.

Change requests are not created when you add an abstract object to a flow because the object does not represent a change in the traffic required for the application. If a flow in an application has only an abstract object for either the source or destination field, the flow itself is abstract. It does not represent real traffic, so you cannot run a connectivity check on the flow. These flows are indicated with a pale blue border and striped connectivity indicator.

Name	Source	User	Destination	Network Application	Service	Comments
1	cats_support Dogs_New_LAX dogr_support mice.home	Any	FortiManagerZebra_https	Any	HTTPS	Original Rule Number = 15, from devices: violet_fortinet fasdfdsa
2	jalapeno.net	Any	RedPepper-Replacement (abs...	Any	HTTP	Original Rule Number = 18, Comment was: FireFlow #412, from devices: violet_fortinet
3	jalapeno.net	Any	red.pepper RedPepper-Replacement (abs...	Any	HTTPS	Original Rule Number = 19, Comment was: FireFlow #412, from devices: violet_fortinet
4	debby_int	Any	violet_int_10-8 violet_int_old	Any	HTTP ICMP_ANY	Original Rule Number = 4, from devices: violet_fortinet

At any point, you can update the abstract object with actual values, and the object will be identified as a regular network object. For details, see [Network object dashboard](#).

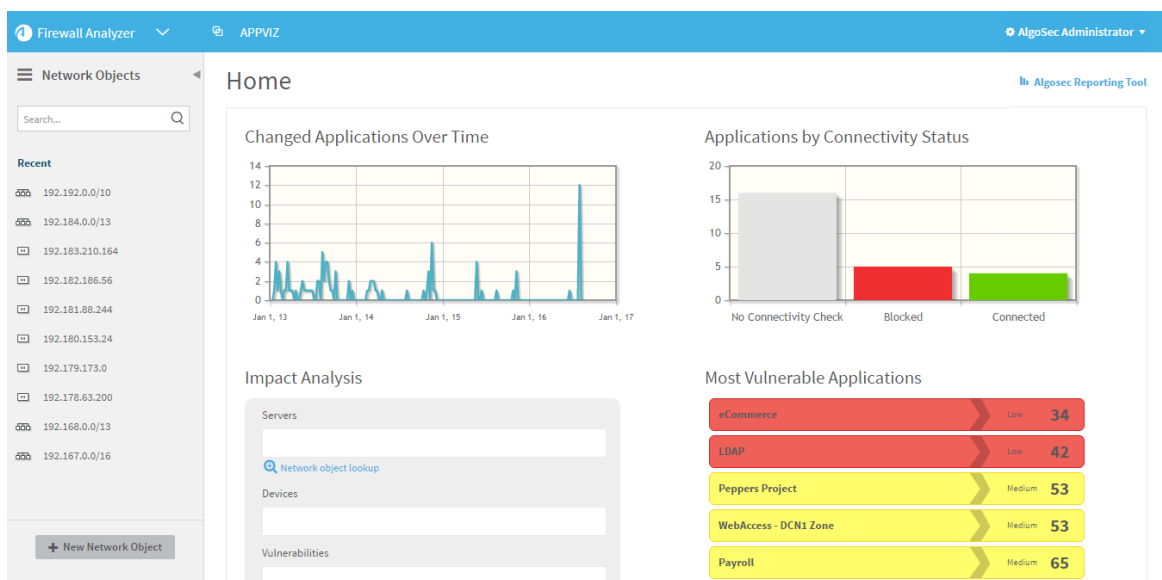
View a network object

This topic describes how to view network objects in AppViz.

Do the following:

1. In AppViz, from the main menu on the left, click **NETWORK OBJECTS**.

The Network Objects page opens, listing recently used network objects on the left.




The icon next to each network object indicates the object type:

 . A host.

 . A range.

 . A group.

 . An abstract network object.

Note: If you have AppChange configured to manage device objects on their devices, some of your network objects may be in the **Pending Deletion** status. Such objects appear greyed out in the list, but are still available for you to view. For more details, see [Device objects](#).

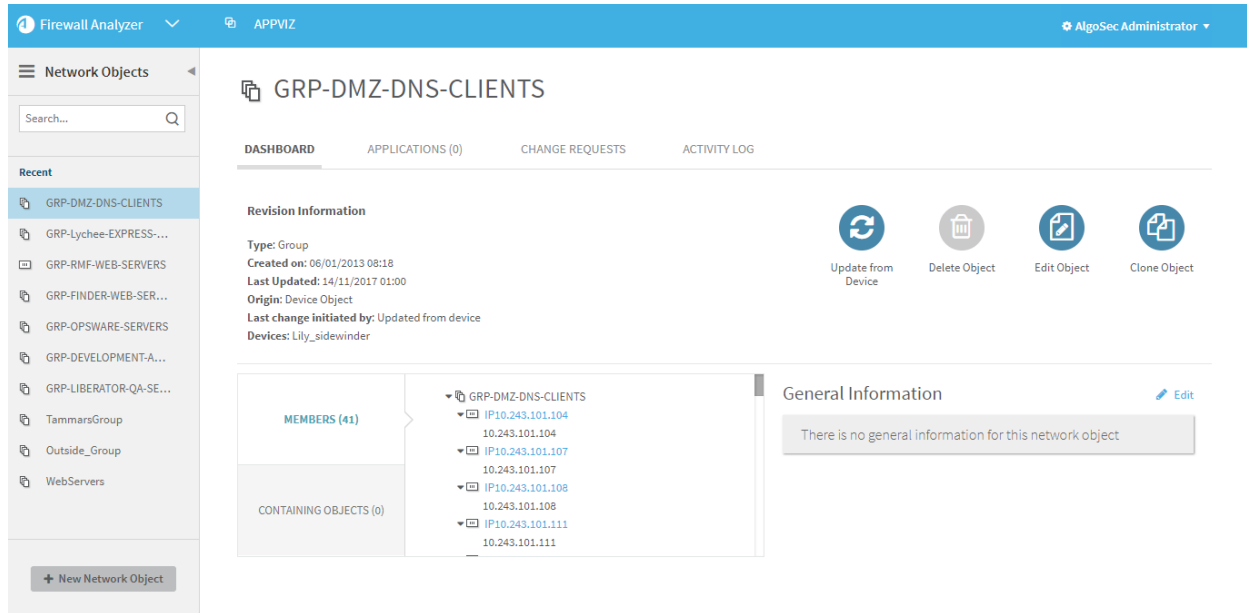
2. Either select a recent network object from the list, or use the search box above the list to perform a simple search.

To search for network objects, enter one of the following, and click  :

- Any part of the network object's name
- An IP address that intersects the object

The matching objects appear below the search box. Select a network object from the list.

The network object appears in the workspace. For example:



Network object dashboard

This topic describes the network object **DASHBOARD** tab, which provides an overview of the network object selected on the left.

DASHBOARD tab interface

The screenshot shows the AppViz dashboard for the network object 'GRP-DMZ-DNS-CLIENTS'. The top navigation bar includes 'Firewall Analyzer' and 'APPVIZ'. The left sidebar shows a search bar and a list of recent objects. The main content area is divided into several sections:



- Revision Information:**
 - Type: Group
 - Created on: 06/01/2013 08:18
 - Last Updated: 14/11/2017 01:00
 - Origin: Device Object
 - Last change initiated by: Updated from device
 - Devices: Lily_sidewinder
- Members (41):** A tree view showing the object's members, including IP addresses like 10.243.101.104, 10.243.101.107, 10.243.101.108, and 10.243.101.111.
- Containing Objects (0):** A section for objects contained within this group.
- General Information:** A section with an 'Edit' button and a message: 'There is no general information for this network object'.

At the top right of the main content area, there are four action buttons: 'Update from Device', 'Delete Object', 'Edit Object', and 'Clone Object'.

Revision information area



This area displays the following information about the network object you are viewing:



Type	<p>One of the following:</p> <ul style="list-style-type: none"> • <i>Host</i>. A single IP address. • <i>Range</i>. A range of IP addresses. • <i>Group</i>. A group which contains network objects. • <i>Abstract</i>. For details, see Network objects.
Created on	The date the object was created in AppViz.
Last updated	The date the object was last updated.
Origin	<p>Where the object was created. One of the following options:</p> <ul style="list-style-type: none"> • AppViz Object • Imported. This includes objects imported from a CSV file, CMDB, or created via the API. • Device object


Last change Initiated by	<p>How the object's current revision was initiated. One of the following options:</p> <ul style="list-style-type: none"> • ASMS user • Update from device • Update from file, including objects updated from a CMDB.
Devices	<p>The devices the object is defined on.</p> <p>Note: This field only appears for objects currently defined on devices. If a device object being used in an application is deleted from its devices, AppViz will keep the object alive, and the following warning appears:  <i>This object no longer exists on any device</i></p>
PCI In PCI Zone	<p>The object intersects the PCI zone that is defined in AFA.</p> <p>When an object is in the PCI zone, a pale teal background appears with the object's icon:  behind_port4</p> <p>Additionally, the PCI system label is automatically associated with all applications containing the object in their active revision.</p>


Object change status

Network objects may have one of the following change statuses:

In Change Process	<p>The object's definition in AppViz has been updated, and the FireFlow change request to modify the relevant traffic is pending.</p> <p>When an object has this change status,  appears in the upper right corner of its page. Additionally,  appears on the object's icon in any application flows, projects, or discovery processes.</p> <p>Note: Objects in change process cannot be edited, used in projects or included in discovery from traffic logs. They can be used in flows.</p>
--------------------------	--

Rejected	<p>The object was in change process, and its FireFlow change request was rejected.</p> <p>When an object has this change status,  appears in the upper right corner of its page. Additionally,  appears on the object's icon in any application flows, projects, or discovery processes.</p> <p>Note: Objects with the Rejected change status cannot be edited, used in projects, included in discovery from traffic logs or used in flows.</p>
-----------------	---

Some objects may have a notification that is not related to change status, but because it is in a problematic scenario. Some objects may have outdated revisions being used in applications. When this is the case,  appears in the upper right corner of

 *Some applications are not updated with this object's last revision* its page and  appears on the object's icon in any

application flows or projects using the outdated revision. This situation can only occur as the result of an import when the **Do not update the affected applications automatically** option is chosen. This is relevant to device object updates (from AFA) or network object imports from a CSV or CMDB. For more details, see [AppViz maintenance](#).

The object change statuses listed above are different for device objects when your AppViz environment is configured to open a FireFlow *object change* request via AppChange when deleting or editing device objects. The meaning of these statuses is slightly different and other status options exist. For more details, see [Edit device objects](#).

Network object actions

For each network object, the **DASHBOARD** tab provides the following options at the top-right:

Edit	<p>This action allows you to edit the network object. A change request opens in FireFlow to adjust traffic for the new object definition.</p> <p>You cannot edit network objects if they are in use by an application for which you do not have permissions or if they are in use by an application in the Pending Implementation status.</p>
-------------	--

Clone	This action creates a new network object with the same contents.
Delete	This action deletes the network object.
Replace	This action replaces abstract network objects with real objects.
Update Applications	<p>This action updates all the applications using the object to the current revision of the object. The outdated object is replaced with the current object, and a change request opens in FireFlow to adjust the traffic requirements.</p> <p>This action is only relevant for objects which were edited, and the applications using the object were not updated with the new revision of the object.</p>
Discard Change	<p>This action discards the revision of the object. A change request opens in FireFlow to adjust traffic for the previous object definition.</p> <p>Note: This is action is only relevant for Rejected objects.</p>
Re-apply Changes	<p>This action re-applies the new revision of the object. Use this action after further modifying a rejected object. A change request opens in FireFlow to adjust traffic for the new object definition.</p> <p>Note: This action is only relevant for Rejected objects.</p>
Update from Device	<p>This action updates the definition of a device object.</p> <p>Note: When a FireFlow change request is created as the result of an object action, the subject of the change request signifies the object.</p>

For more details, see [Add and edit network objects](#).

Object content and status information

Object content and status information includes:

Status details	<p>This appears when a group object is In Change Process or Rejected because of one of its members.</p> <p>If your AppViz environment is configured to open a FireFlow <i>object change</i> request via AppChange to change the definition of device objects on their devices, this tab also appears for objects pending creation on the device. For more details, see Device objects.</p>
Content or members	<p>The Content (in the case of a host or range) or Members (in case of a group) of the network object.</p> <p>If members of an object are Rejected, Outdated, or In Change Process, this is indicated with an exclamation point. If a member is rejected, the whole object is marked as rejected.</p>
Containing objects	<p>This includes objects which contain the network object or objects which contain an object which contains the network object.</p> <p>Click the desired tab to display the content.</p>

General Information area

This area displays custom fields for the object. For more details, see [Custom fields](#) and [AppViz maintenance](#).

Vulnerability Assessment area

This area displays all the vulnerabilities for the network object. This area only appears if the following are true:

- Vulnerability Assessment is enabled.
- The network object has been scanned.

Note: Network objects will not be scanned when the **Server Max Size** field is less than the number of IP addresses the object contains. The default value for this field is six.

For more details, see [Manage vulnerability assessment scanners](#).

Add and edit network objects

This topic describes how to add and edit network objects in AppViz.

Add a network object

Do the following:

1. In AppViz, from the main menu on the left, click **NETWORK OBJECTS**.
2. Click **+New Network Object**.

The New Network Object form appears in the workspace.

3. Complete the fields as needed. For details, see [Network object fields](#).
4. Click **Save Changes**.

The **Save Network Object** dialog box appears.

5. Click **OK**.

The network object is created, and the **DASHBOARD** tab appears. For details, see [Network object dashboard](#).

Network object fields

The following topic describes the fields available for network objects in AppViz.

Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Host. The object contains a single IP address. • Range. The object contains a range of IP addresses. • Group. The object contains network objects. • Abstract. The object contains an abstract object. For more details, see Network objects and Network object dashboard. <p>When editing or cloning a network object, you cannot change the type.</p>
Name	Type the name of the network object.
DNS Lookup	<p>Click to lookup the IP address.</p> <p>This link only appears when the type is Host.</p>
Description	<p>Type a description for the network object.</p> <p>This field does not appear when cloning a network object.</p>
IP Address	<p>Type the IP address.</p> <p>This field only appears when the type is Host.</p>
IP Addresses	<p>Type the range of IP addresses in range or CIDR notation.</p> <p>This field only appears when the type is Range.</p>
Members	<p>Do one of the following:</p> <ul style="list-style-type: none"> • Type the names of existing network objects. • Click Network object lookup to lookup existing network objects. For details, see Business applications. • Click +New to create a new network object. For details, see Add a new network object to a group. <p>Note: Objects that are rejected, pending deletion, or pending creation cannot be added as members of a group.</p> <p>To remove objects from the Members field, click X.</p> <p>This field only appears when the type is Group.</p>
Location	<p>Type the location of the network object.</p> <p>This field does not appear when cloning a network object.</p>

Operating System

Type the operating system for the network object.
This field does not appear when cloning a network object.

Add a new network object to a group

To add a new network object:

1. The **Add New Network Object** dialog box opens.

2. Select the type.
3. In the **Name** field, type the name of the new object.
4. To perform a reverse DNS lookup on the network object Name, click **DNS lookup**.
If the IP address is found for the object, the address is inserted in the **IP Address** field.
5. If reverse DNS lookup was not used or was unsuccessful, type a the IP address in the field.
6. Click **OK**.

Network objects applications

This topic describes the network object APPLICATIONS tab, which lists all the application that use the selected network object.


APPLICATIONS tab interface

The **Applications** tab lists all applications which use the object.

The screenshot shows the 'Firewall Analyzer' interface. The top navigation bar includes 'Firewall Analyzer', 'APPVIZ', and 'AlgoSec Administrator'. The left sidebar shows 'Network Objects' with a search bar and a 'Recent' list containing 'coyote_srv22', 'GRP-DMZ-DNS-CLIENTS', 'GRP-Lychee-EXPRESS...', 'GRP-RMF-WEB-SERVERS', and 'GRP-FINDER-WEB-SER...'. The main content area displays the 'coyote_srv22' object with tabs for 'DASHBOARD', 'APPLICATIONS (1)', 'CHANGE REQUESTS', and 'ACTIVITY LOG'. The 'APPLICATIONS (1)' tab is active, showing a table of applications:

Application Name	Date	Status	Implementation Status
Coyote	08/03/2017	Testing	Draft
Coyote	18/03/2017	Testing	Active
Coyote	09/11/2015	Testing	Pending Implementation

When there are applications using an old revision of the object, these applications are listed separately. When an application is in the pending decommission status, the application appears grayed out.

To view the flows that contain the object, click  next to the application name. For more details, see [View relevant applications](#).

View relevant applications

To view relevant applications:

1. View the object for which you want to view a relevant application. For details, see [View a network object](#) or [Service objects](#).

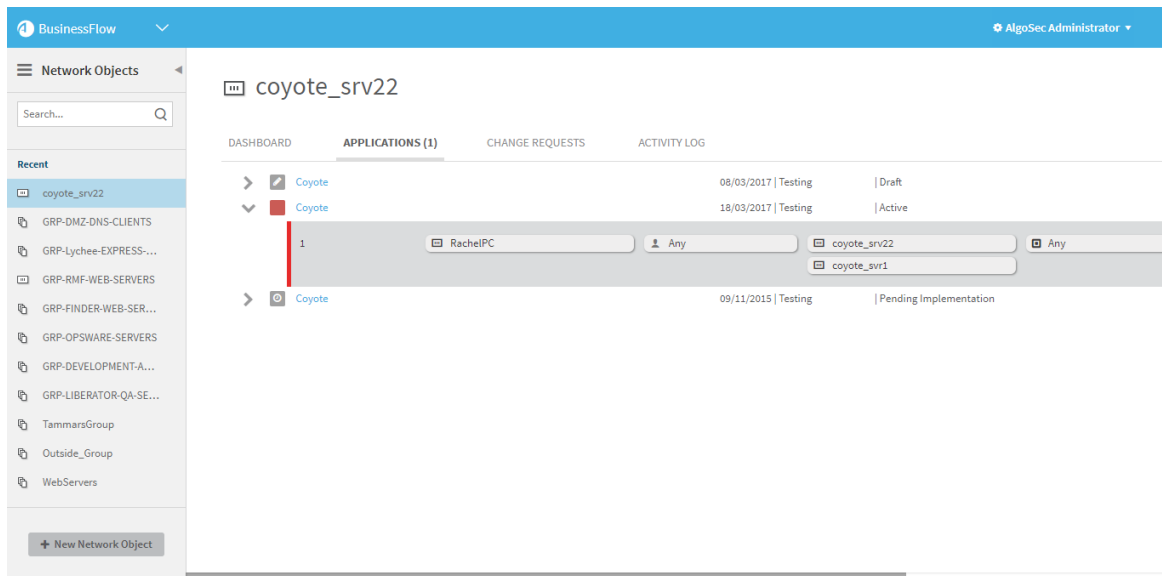
In the title of the **Applications** tab, the number of applications using the object appears in parenthesis.

2. Click the **Applications** tab.

The **Applications** tab appears.

3. To view the flows for an application, click  next to the application name.

The application flows appear.



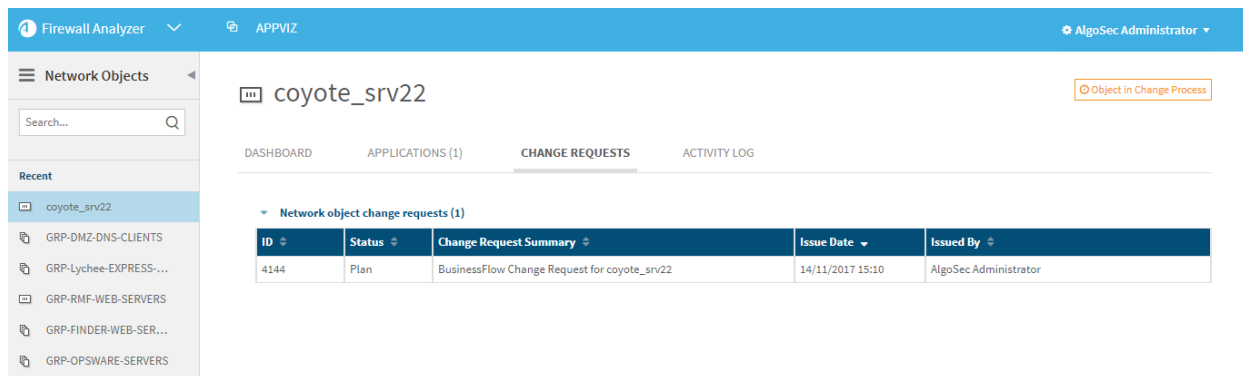
4. To view the application's page, click the name of the application.

The application appears.

Network object change requests

The **Change Requests** tab displays details for all FireFlow change requests that have been created for the network object.

Change Requests interface



View relevant FireFlow change requests

To view relevant FireFlow change requests:

1. View the application, network object, or service object for which you want to view a relevant change request. For more details, see [Business applications](#), [View a network object](#), or [Service objects](#).

2. Click the **Change Requests** tab.

The **Change Requests** tab appears.

3. To change the sort order of the list, click the desired column heading. To reverse the sort order, click the heading again. The sort direction is indicated by the white triangle in the location of the sort icon (▾).

4. Click the change request you wish to view.

A new window opens, displaying the change request in FireFlow.

Network object activity logs

This topic describes the network object's ACTIVITY LOG tab, which displays a log of all actions that affect the selected network object.

ACTIVITY LOG interface

The screenshot shows the FireFlow interface for the 'WebServers' network object. The 'ACTIVITY LOG' tab is selected, displaying a table of activity logs. The table has columns for Category, Description, User Name, and Time. The logs show that the object content was changed and that a change request was opened.

Category	Description	User Name	Time
Object Content	Content was changed from 10.30.152.50-10.30.152.61 to 10.30.152.50-10.30.152.60	admin	Nov 13 17:11
Status	WebServers is in change process. Change request #832 was opened.	admin	Nov 13 17:11

Category	The activity's category: Information, Status, System, or Object Content.
Description	Description of the activity.
User Name	Name of user who performed the activity.
Time	Date and Time the activity occurred.

Service objects

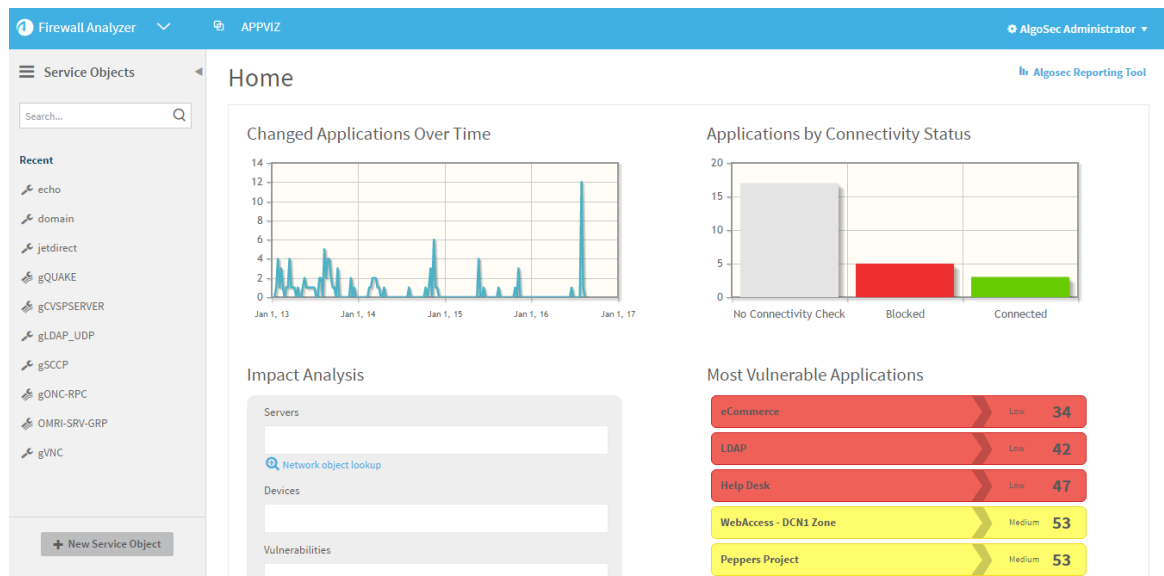
This topic describes how to manage service objects in AppViz.

View a service object

To view a service object:

1. In AppViz, from the main menu on the left, click **SERVICE OBJECTS**.

The **Service Objects** menu appears.



The icon next to each service object indicates the object type.




. A single service.




. A group or range of services.

2. Do one of the following:

- Select a service object from the list of recent objects.
- Perform a simple search for a service object. Type any part of the service object's name in the search box, and click . The matching objects appear below the search box. Select a service object from the list.

The service object appears in the workspace with the **Dashboard** tab displayed.

The screenshot shows the AppViz interface for a service object named 'gONC-RPC'. The top navigation bar includes 'Firewall Analyzer' and 'APPVIZ', with the user 'AlgoSec Administrator' logged in. The left sidebar shows 'Service Objects' with a search bar and a list of recent objects, including 'gONC-RPC'. The main content area displays the 'gONC-RPC' object with tabs for 'DASHBOARD', 'APPLICATIONS (0)', and 'CHANGE REQUESTS'. The 'DASHBOARD' tab is active, showing 'Revision Information' (Created on: 02/08/2016 01:02, Last Updated: 02/08/2016 01:03, Origin: Device Object, Last change initiated by: Device Object, Devices: 10_20_106_1) and 'General Information' (Edit, No general information). A 'CONTENTS' section shows 'TCP/111' and 'UDP/111'. A '+ New Service Object' button is at the bottom left.

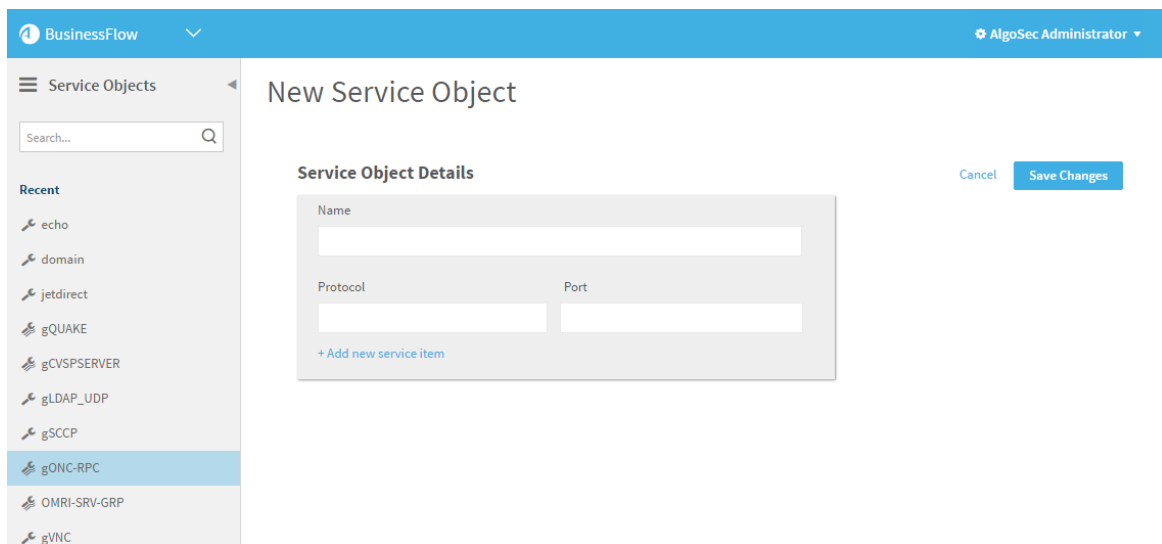
Tip: To return to the other areas available from the main menu, click the hamburger menu  at the top left, and select the page you want to navigate to.

Add a service object


To add a service object:

1. Go to the **Service Objects** area.
2. Click **+New Service Object**.

The **New Service Object** form appears in the workspace.



3. Complete the fields as follows:

Name	Type the name of the service object.
Protocol	Type the protocol of the service.
Port	Type the Port of the service.
+ Add new service item	Click this link to add an additional service to the service object. Another line with Protocol and Port fields appears to define the service.
	Click this icon to delete the service.

4. Click **Save Changes**. Click **OK**.

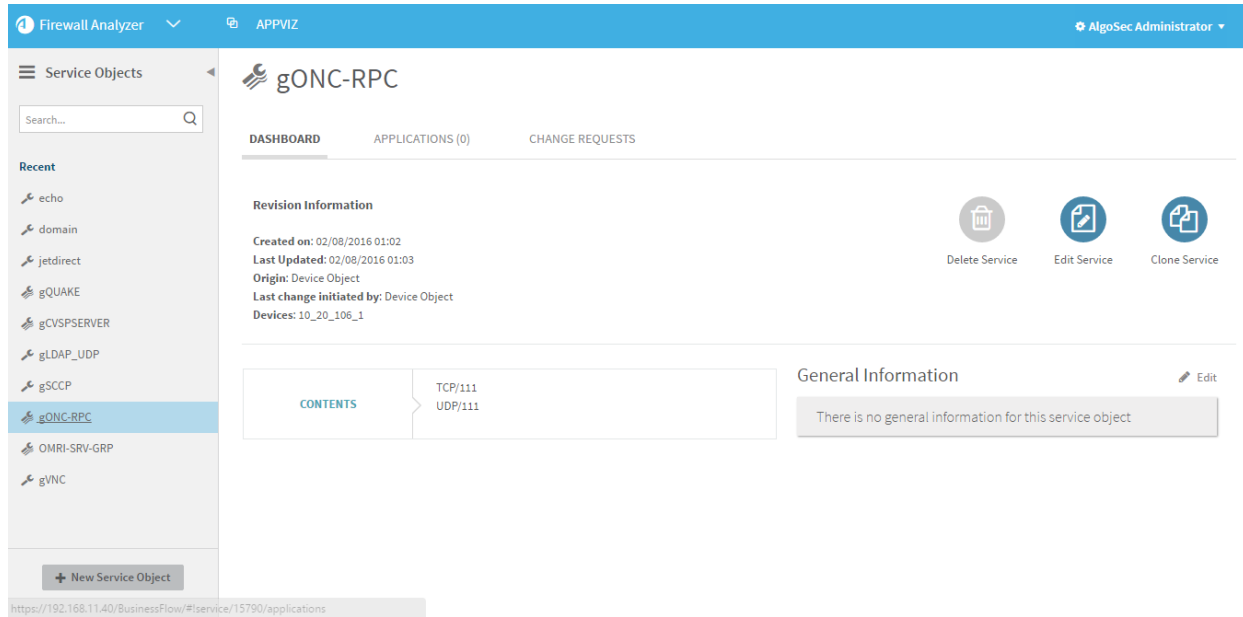
The service object is created, and the **DASHBOARD** tab for the new service object appears.

Service object DASHBOARD

The **DASHBOARD** tab provides the ability to:







- Quickly and easily view a summary of a service object's history and basic information.
- View a service object's contents and containing objects.


- Edit the service object, delete the service object, or create a new service object with the same contents.
- Edit service object information.



Dashboard tab areas

Area	Description
Revision Information	<p>This area displays the following information about the network object you are viewing:</p> <ul style="list-style-type: none">• Created on. The date the object was created in AppViz.• Last Updated. The date the object was last updated.• Origin. Where the object was created. One of the following options:<ul style="list-style-type: none">• AppViz Object• Imported. This includes objects created via the API.• Device Object• Last change Initiated by. How the object's current revision was initiated. The options for this field are the same as for the Origin field.• Devices. The devices the object is defined on. <p>Note: This field only appears for objects currently defined on devices. AppViz will keep a device object alive after it is deleted from its devices if the object is being used in an application.</p>

Area	Description
Object Change Status	<p>Service objects may have one of the following change statuses:</p> <ul style="list-style-type: none"> In Change Process. The object's definition in AppViz has been updated, and the FireFlow change request to modify the relevant traffic is pending. <p>When an object has this change status,  appears in the upper right corner of its page. Additionally,  appears on the object's icon in any application flows or discovery processes.</p> <p>Note: Objects in change process cannot be edited, used in projects or included in discovery from traffic logs. They can be used in flows.</p> Rejected. The object was in change process, and its FireFlow change request was rejected. <p>When an object has this change status,  appears in the upper right corner of its page. Additionally,  appears on the object's icon in any application flows or discovery processes.</p> <p>Note: Objects with the Rejected change status cannot be edited, included in discovery from traffic logs or used in flows.</p> <p>Note: Some service objects may have a notification that is not related to change status, but because it is in one of the following problematic scenarios:</p> <ul style="list-style-type: none"> Objects with invalid content. A service object with invalid content includes both TCP/UDP protocols and non-TCP/UDP protocols. When this is the case,  appears in the upper right corner of its page. AppViz does not allow adding invalid content to a service, but it is possible for invalid content to be imported. You cannot edit a service object with invalid content without resolving the problem. Objects with outdated revisions being used in applications. When this is the case,  appears in the

Area	Description
	<p>upper right corner of its page and  appears on the object's icon in any application flows using the outdated revision. This situation can only occur as the result of an import when the Do not update the affected applications automatically option is chosen. For more details, see AppViz maintenance.</p>

Area	Description
Actions	<p>This area provides the option to:</p> <ul style="list-style-type: none"> • Edit. This action allows you to edit the service object. A change request opens in FireFlow to adjust traffic for the new object definition. You cannot edit service objects if they are in use by an application for which you do not have permissions or if they are in use by an application in the Pending Implementation status. • Clone. This action creates a new service object with the same contents. • Delete. This action deletes the service object. You cannot delete the following objects: <ul style="list-style-type: none"> • Device Objects • Objects that are in use by an application • Update Applications. This action updates all the applications using the object to the current revision of the object. The outdated object is replaced with the current object, and a change requests opens in FireFlow to adjust the traffic requirements. For more details, see AppViz maintenance. This action is only relevant for objects which were edited, and the applications using the object were not updated with the new revision of the object. • Discard Object. This action discards the revision of the object. A change request opens in FireFlow to adjust traffic for the previous object definition. Note: This is action is only relevant for Rejected objects. • Re-apply Object. This action re-applies the new revision of the object. Use this action after further modifying a rejected object. A change request opens in FireFlow to adjust traffic for the new object definition. Note: This is action is only relevant for Rejected objects. • Update from Device. This action updates the definition of a device

Area	Description
	<p>object. For more details, see Device objects.</p> <p>For details, see Manage network / service objects and Application dashboard.</p> <p>Note: When a FireFlow change request is created as the result of an object action, the subject of the change request signifies the object. For more details, see Customize interactions with AFA and FireFlow.</p>
Object Content	The Contents of the service object.
General Information	This area displays custom fields for the object. For more details, see Custom fields .


Service object applications

The service object APPLICATIONS tab lists all applications which contain the service object.

The screenshot shows the AppViz interface for a service object named 'Apache httpd 2.2.25'. The interface includes a search bar with the object name, a sidebar with 'Service Objects', and a main content area with tabs for 'DASHBOARD', 'APPLICATIONS (10)', and 'CHANGE REQUESTS'. The 'APPLICATIONS' tab is active, displaying a list of applications with columns for application name, date, status, and draft/active status. A red notification box in the top right corner indicates 'Object Change Rejected'.

Application	Date	Status	Draft/Active
ATM	03/08/2016	Testing	Draft
Commercial Banking	03/08/2016	Testing	Draft
SugarCRM Clone	20/02/2017	Testing	Draft
PayIt-System	03/08/2016	Testing	Draft
ERP	03/08/2016	Testing	Draft
Internet Banking	03/08/2016	Testing	Draft
Human Resources	03/08/2016	Testing	Draft
Pension Management	03/08/2016	Testing	Draft
Inventory Management	03/08/2016	Testing	Draft
SugarCRM	20/02/2017	Testing	Active

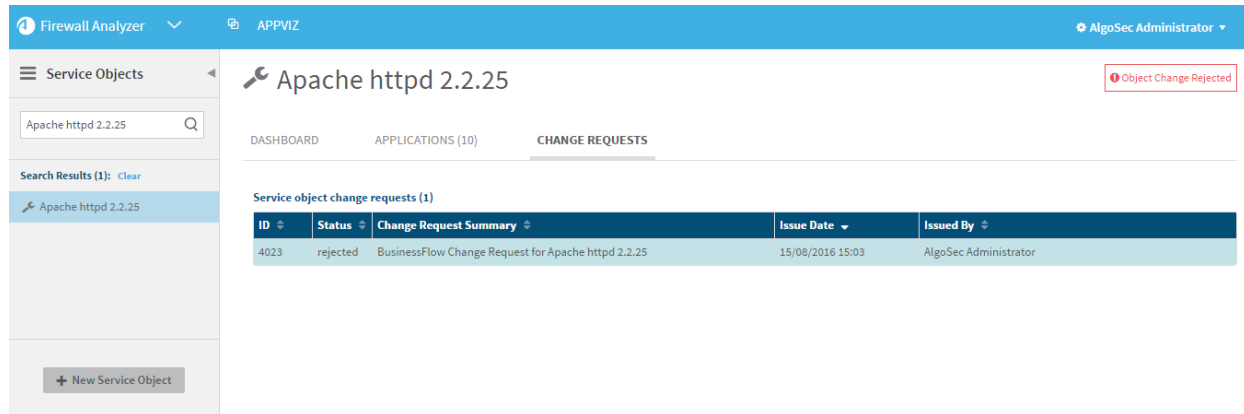
When there are applications using an old revision of the object, these applications are listed separately. When an application is in the pending decommission status, the application appears grayed out.

To view the flows that contain the service object, click  next to the application name.

For more details, see [Business applications](#).

Service object change requests

The **Change Requests** tab displays details for all FireFlow change requests that have been created for the service object.



The screenshot shows the 'Firewall Analyzer' interface for the 'APPVIZ' application. The 'Service Objects' sidebar is open, showing a search for 'Apache httpd 2.2.25' with one result. The main content area is titled 'Apache httpd 2.2.25' and has a red notification 'Object Change Rejected'. The 'CHANGE REQUESTS' tab is active, displaying a table of service object change requests.

ID	Status	Change Request Summary	Issue Date	Issued By
4023	rejected	BusinessFlow Change Request for Apache httpd 2.2.25	15/08/2016 15:03	AlgoSec Administrator

Manage network / service objects

This topic describes how to manage network and service objects in AppViz. For more details, see [Network objects](#) and [Service objects](#).

Some objects are not available for editing.

Edit a network or service object

This procedure describes how to edit a network or service object in AppViz, when AppViz / AppChange are *not* configured to open FireFlow change requests for changes to device network object definitions.

For more details, see [Device objects](#).

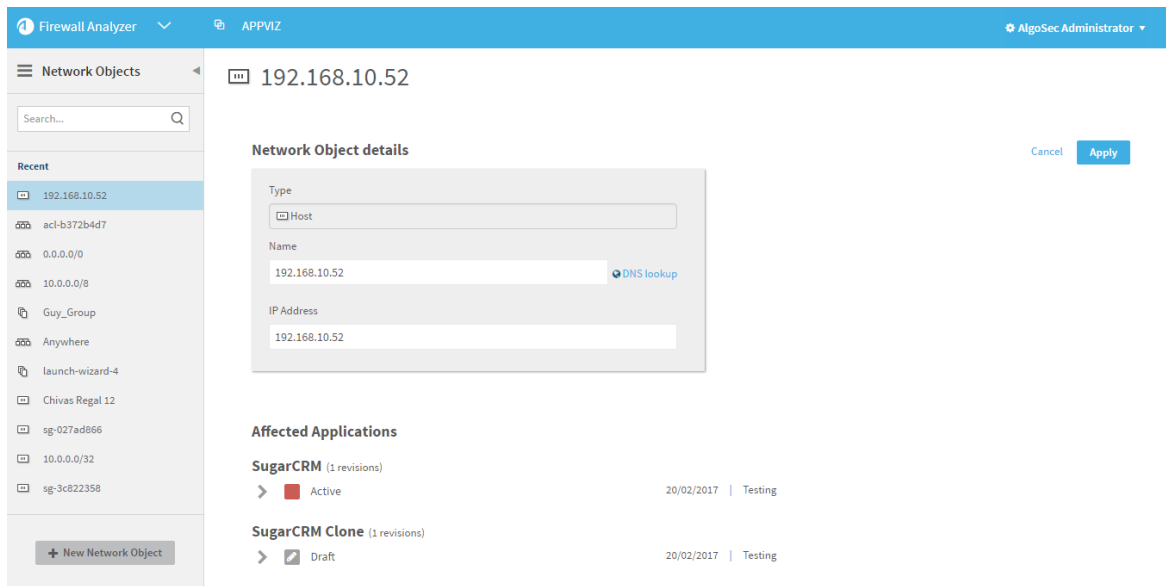
Do the following:


1. View the object you want to edit. For details, see [View a network object](#) or [Service objects](#).

Note: Some objects are not available for editing. For details, see [Objects with read-only permissions](#).

2. In the **Actions** area of the **Dashboard** tab, click .

The **Object details**, and if relevant, the **Affected Applications** appear.



The **Affected Applications** area lists the applications that contain the object. View any affected flows by clicking .

3. Edit the fields as needed. Device object names remain read-only.

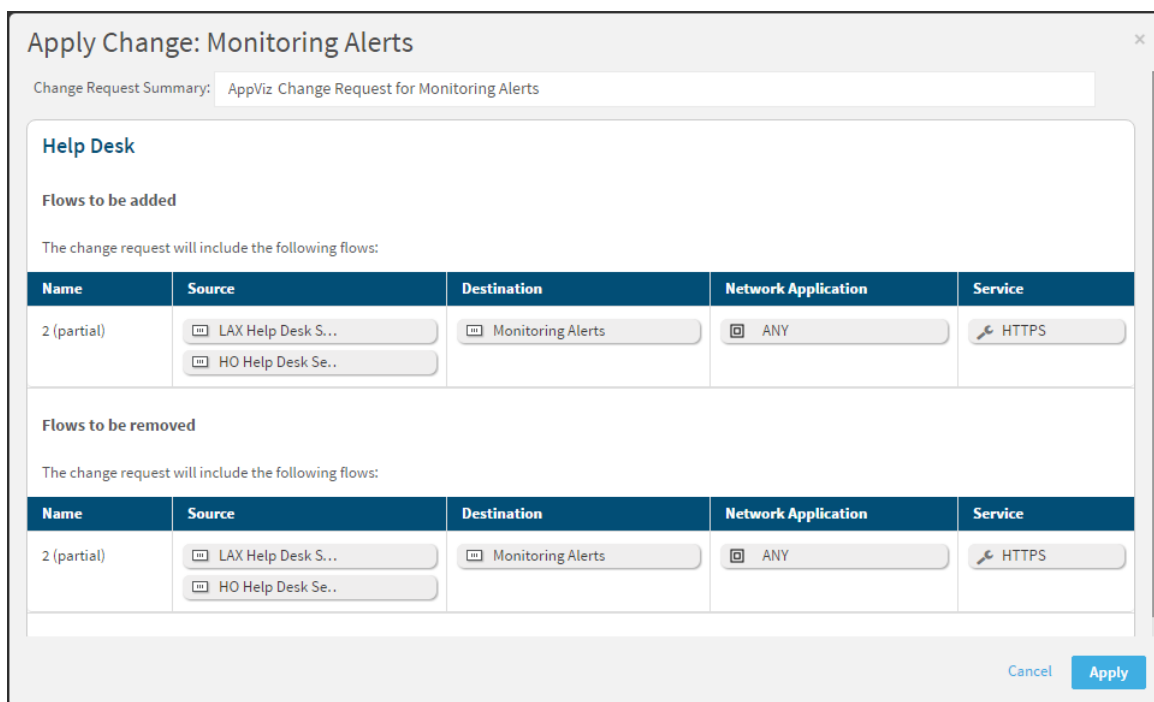
For more details, see [Add and edit network objects](#) or [Service objects](#).

4. Click **Apply**. One of the following occurs, depending on whether the object is used in an active application:

Objects are used in an active application

For objects used in an active application, the **Apply Change** dialog box appears.

For example:



This dialog box organizes the traffic included in the change request into the following categories:

Flows to be added	The change request will allow this traffic.
Flows to be removed	The change request will deny this traffic.
Flows used by other applications	The change request will not include this traffic as it is necessary for other applications.

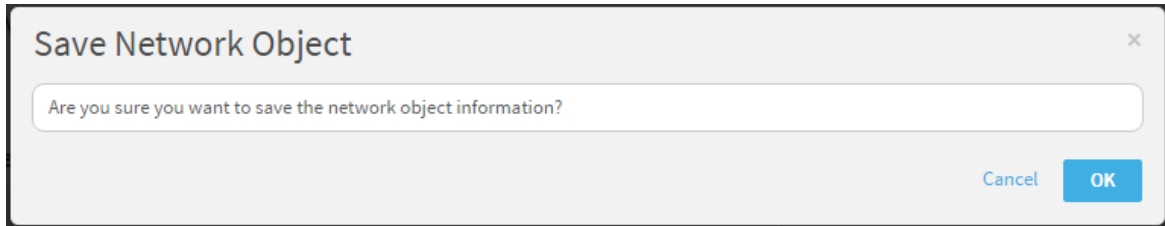
Note: Not all categories are relevant to every object edit.

If needed, edit the text in the **Change Request Summary** field at the top, and then click **Apply**.

Objects not used in an active application

For objects not used in an active application, the **Save Object** dialog box appears.

For example:



Click **OK** to save your changes. No new change request is opened.

One of the following occurs:

Edited object is used in an active application

If the object you are editing is used in an active application, the following occurs:

1. A traffic change request is opened in FireFlow to implement the changes made to the object, such as to allow any traffic now required or remove traffic no longer needed.

Note: Traffic is only removed if it is no longer needed for any other AppViz applications.

2. The object's status is changed to **In Change Process**, and no other edits are allowed.
3. Any applications using the object and automatically updated with the new object value. AppViz uses the new definition, without waiting for the change request to be resolved.
4. When the change request is resolved in FireFlow, the object leaves the **In Change Process** change status, and becomes editable again.

If the change request is rejected in FireFlow, the object moves from the **In Change Process** status to a status of **Rejected**.

Edited object is not used in any active application

If the object you are editing is not used in an active application, your changes are saved,

but no change request is opened.

Objects with read-only permissions

You can only edit objects for which you have editing permissions. Additionally, the following objects cannot be edited by anyone:


- Objects in use by applications for which you do not have editing permissions
- Objects that are involved in a pending application. For example if you change an application to include a new object, and the application is now pending implementation, you cannot edit that object.
- Objects that are part of a group that currently has the **In Change Process** status.

Clone an object

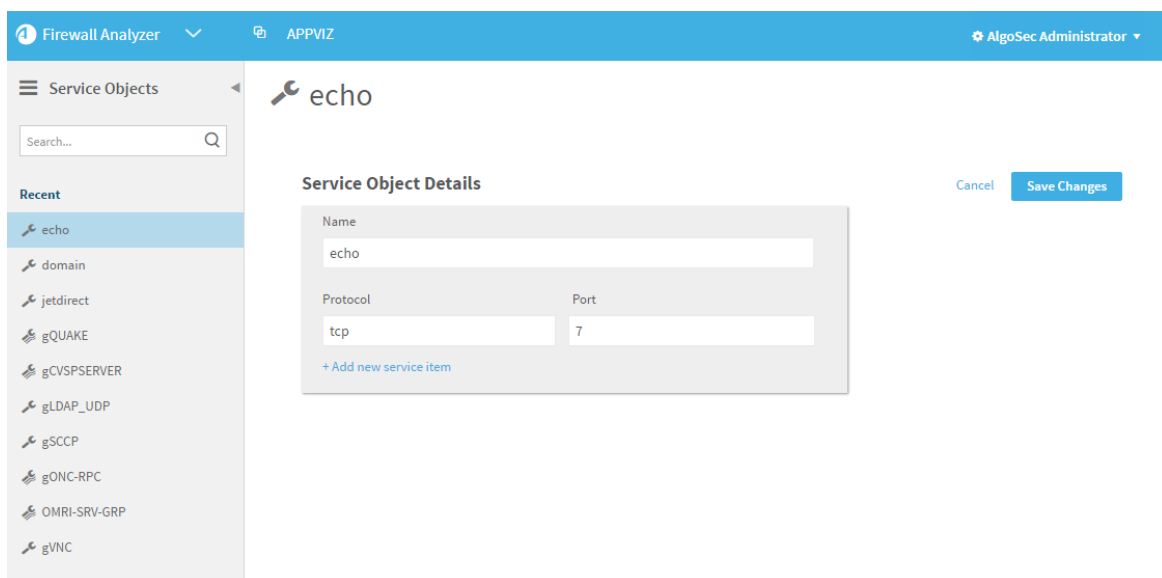
Cloning an object creates a new object with the same content as the original object.

Note: You cannot clone a group object if any member of the group has a change status (**Rejected**, **In Change Process**, etc.).

To clone an object:

1. View the object you want to edit. For details, see [View a network object](#) or [Service objects](#).
2. In the **Actions** area of the **Dashboard** tab, click .

The **Object Details** appear.

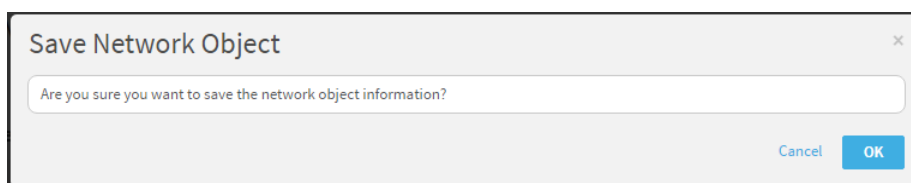


3. Edit the fields as needed. For details, see [Add and edit network objects](#) or [Service objects](#).

If you are cloning an object that originated in AppViz, you must edit the **Name** field.

4. Click **Save Changes**.

The **Save Object** dialog box appears.



5. Click **OK**.

The object is created.

Delete an object

Note: You cannot delete objects that are currently in use in an application, a member of a group object, or in use in a project with the status **In Progress**. Additionally, you must have permission to edit the object.

Note: You cannot delete any device objects when AppViz manages objects with its default behavior (device object definitions are *not* changed on their devices).

Note: This procedure is not relevant when AppViz is configured to open a FireFlow object change request via AppChange to change device network object definitions.

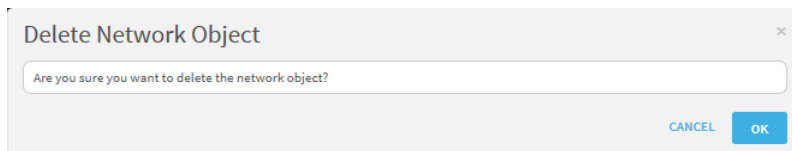
For more details, see [Device objects](#).

To delete an object:

1. View the object you want to edit. For details, see [View a network object](#) or [Service objects](#).

2. In the **Actions** area of the **Dashboard** tab, click .

The **Delete Object** dialog box appears.



3. Click **OK**.

The object is deleted and the **Home** page appears.

Note: The history of deleted network objects can be viewed in the activity logs.

For details, see [Network object activity logs](#).

Replace an abstract network object

There are two options for replacing an abstract network object with a regular network object:

- From Applications
- From Network Objects

Abstract network objects can be replaced with a new object or an existing one.

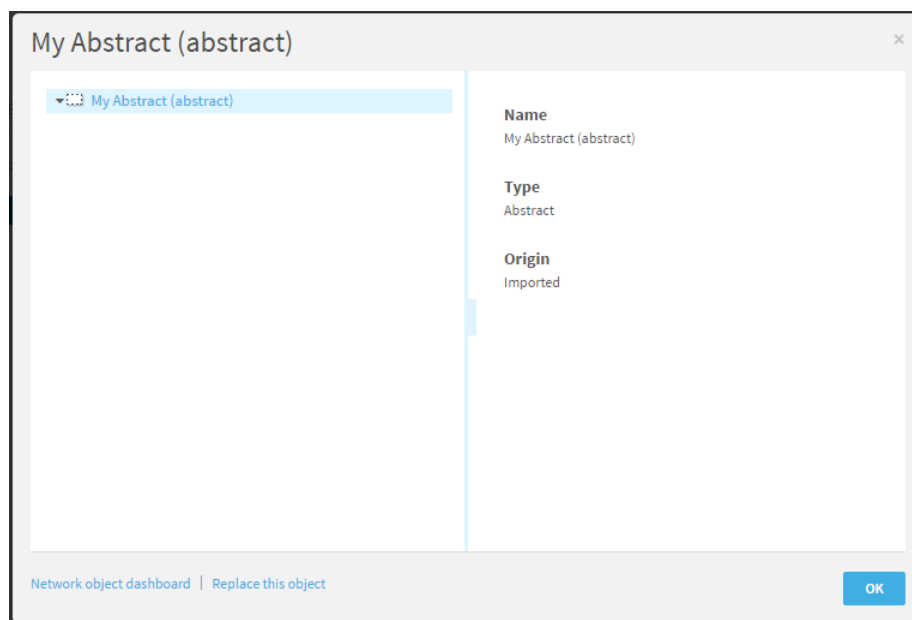
When you replace an abstract object, the following occurs:

- A change request opens in FireFlow to modify the relevant traffic for the object's new flow(s). The change request appears in the change request tab of the abstract object, not the real object.
- Affected applications behave the same as for other edited network objects.

To replace an abstract network object:

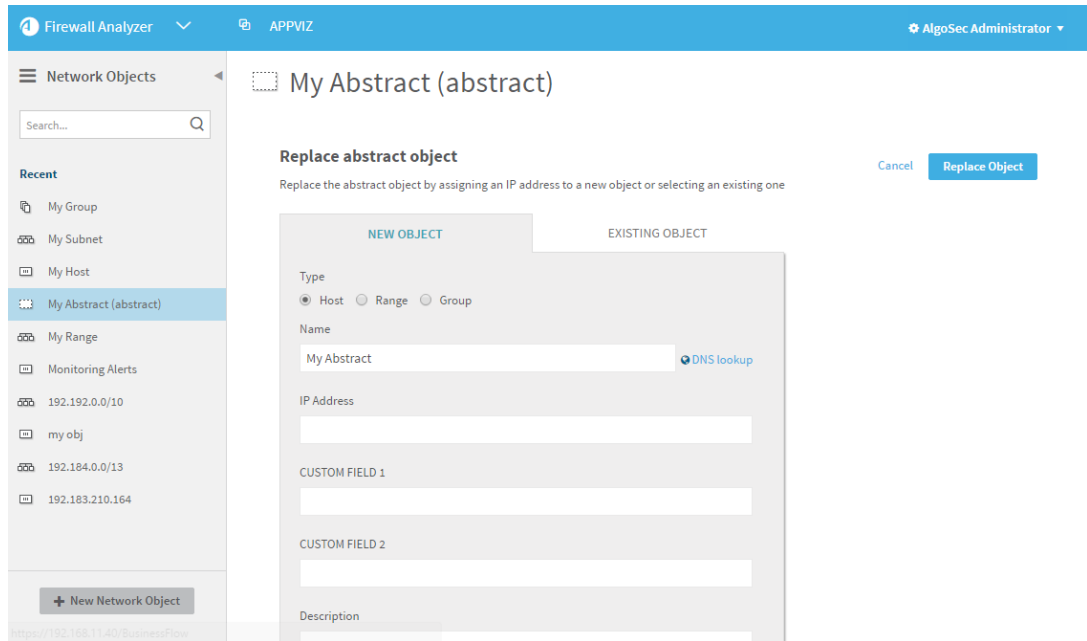
1. To replace from an Application:
 - a. View the application with the abstract object. For details, see [Business applications](#).
 - b. Click the **Flows** tab.
 - c. In the flow, click an abstract object.

The abstract network object information dialog box appears.




- d. At the bottom of the dialog box, click **Replace this object**.

The **Replace Abstract object** page appears in the workspace.



2. To replace from a Network Object:

- a. View the abstract network object. For details, see [View a network object](#).
- b. In the **Actions** area of the **Dashboard** tab, click .

The **Replace Abstract object** page appears in the workspace.

3. To replace with a new object, see [Replace with a new object](#).

4. To replace with an existing object, see [Replace with an existing object](#).

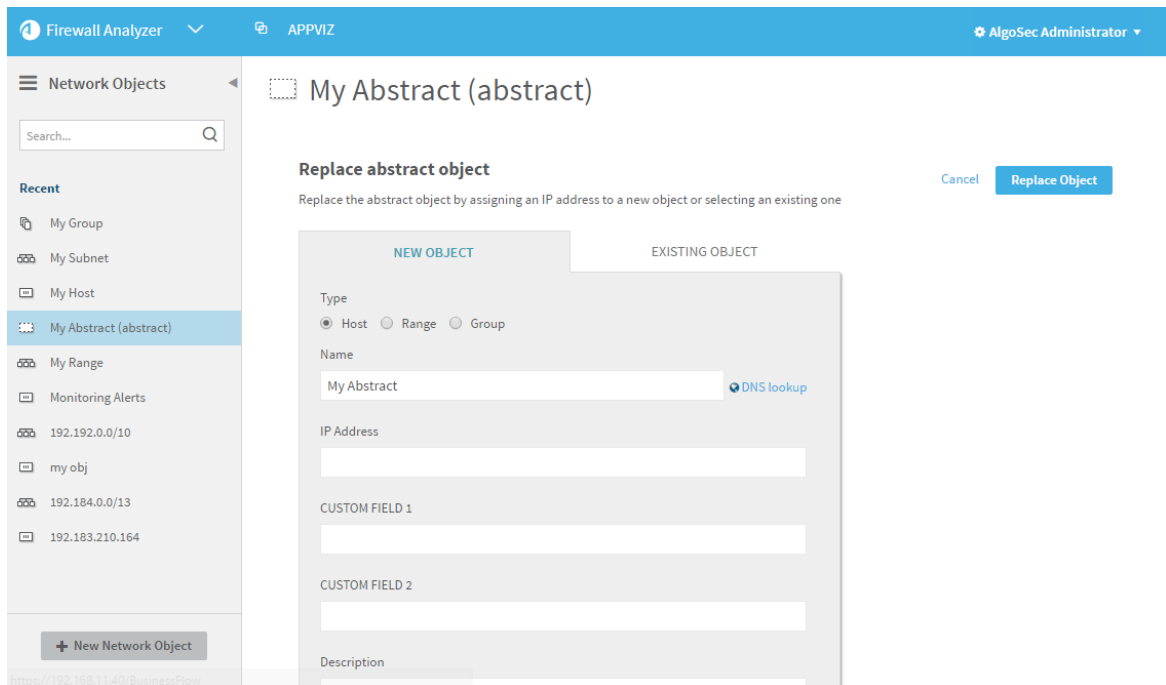
Replace with a new object

To replace with a new object:

1. Click the **New Object** tab.

The **Replace abstract object page** appears, displaying the **New Object** tab.

The abstract object fields, except for **Type** and **Address**, are pre-populated.



2. Select the network object **Type**.
 3. Type the appropriate **Address** value for the network object type.
 4. In the **Affected Applications** area, do the following:
 - Select the check box next to existing drafts you wish to update.
 - Select the check box next to applications that you want to create a new draft for with the replaced object.
 5. Click **Replace Object**.
- The **Apply Change** dialog box appears.

Apply Change: My Abstract (abstract)

Change Request Summary: AppViz Change Request for My Abstract (abstract)

Help Desk

Flows to be added

The change request will include the following flows:

Name	Source	Destination	Network Application	Service
1 (partial)	Help Desk Portal	1.0.0.0	ANY	HTTP

Cancel Apply

The dialog box organizes the traffic included in the change request into the following categories:

- **Flows to be added.** The change request will allow this traffic.
- **Flows to be removed.** The change request will deny this traffic.
- **Flows used by other applications.** The change request will not include this traffic as it is necessary for other applications.

Not all categories are relevant to every object edit.

6. (Optional) In the **Change Request Summary** field, edit the subject for the change request.
7. Click **Apply**.

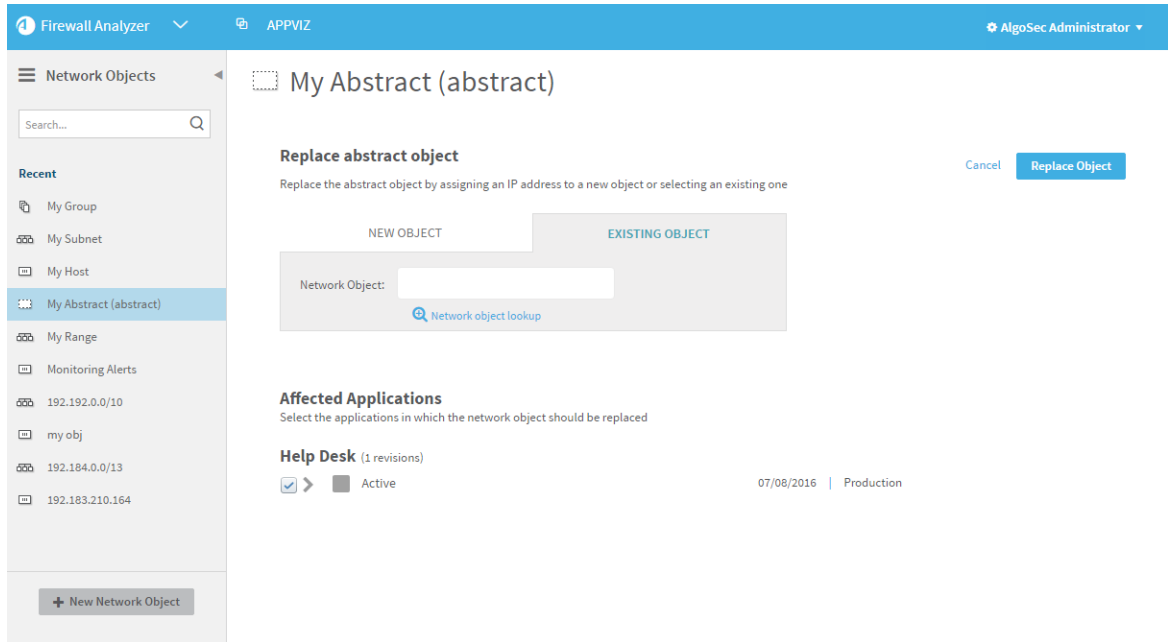
The abstract object is replaced with the specified network object. A change request opens in FireFlow to modify the relevant traffic relating to this object's new flow(s).

Replace with an existing object

To replace with an existing object:

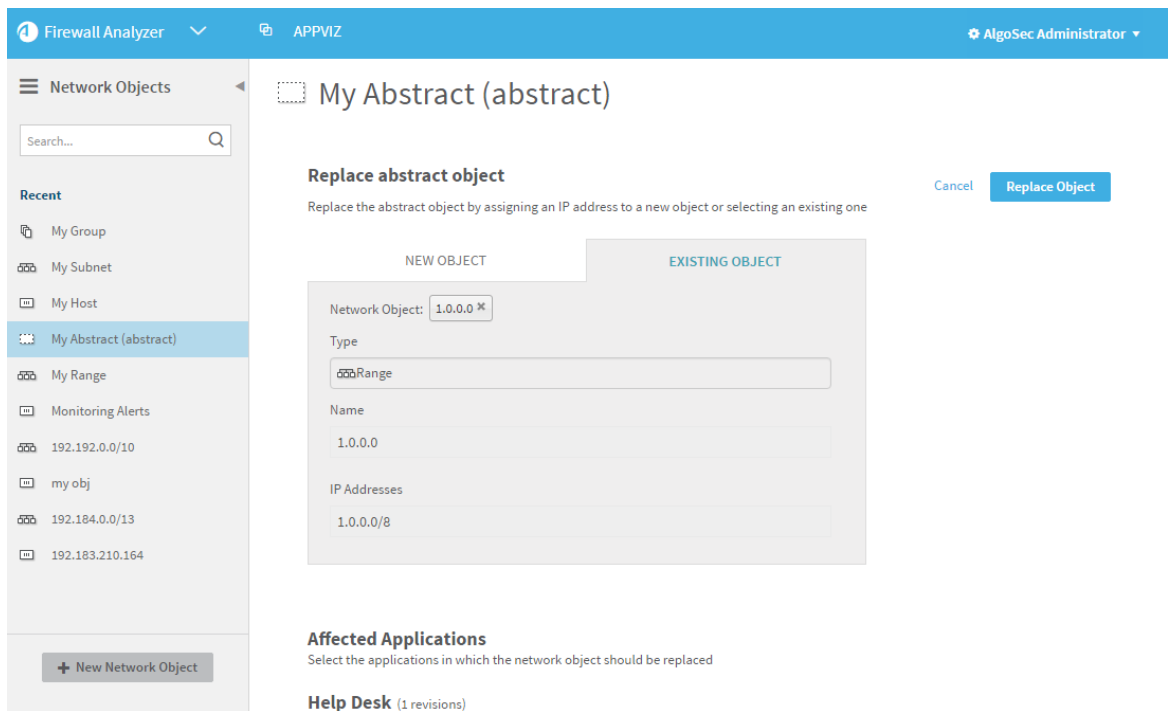
1. Click the **Existing Object** tab.

The **Replace abstract object** page appears, displaying the **Existing Object** tab.



2. To select the existing object, click **Network object lookup**. For details, see [Business applications](#).

The fields are filled with the selected network object's information.



3. In the **Affected Applications** area, select the check box next to existing applications you wish to update.
4. Click **Replace Object**.

The **Apply Change** dialog box appears.

The dialog box organizes the traffic included in the change request into the following categories:

- **Flows to be added.** The change request will allow this traffic.
- **Flows to be removed.** The change request will deny this traffic.
- **Flows used by other applications.** The change request will not include this traffic as it is necessary for other applications.

Not all categories are relevant to every object edit.

5. (Optional) In the **Change Request Summary** field, edit the subject for the change request.
6. Click **Apply**.

The abstract object is replaced with the specified network object. A change request opens in FireFlow to modify the relevant traffic relating to this object's new flow(s).


Update an object's applications

Updating applications replaces an old revision of the object with the new revision of the object in any application flows using an outdated revision of the object. A change request opens in FireFlow to allow and/or deny any traffic necessary for applications as a result of the updated object. Traffic is only removed when it is not necessary for any other applications in AppViz.

Once applications are updated, the following occurs:

- A FireFlow change request opens to modify the relevant traffic.
- The applications are immediately updated with the new object value. AppViz does not wait for the change request to be resolved.

To update applications:

1. View the object you want to edit. For details, see [View a network object](#) or [Service objects](#).
2. In the **Actions** area of the **Dashboard** tab, click .

The **Apply Change** dialog box appears.

The dialog box organizes the traffic included in the change request into the following categories:

- **Flows to be added.** The change request will allow this traffic.
- **Flows to be removed.** The change request will deny this traffic.
- **Flows used by other applications.** The change request will not include this traffic as it is necessary for other applications.

Not all categories are relevant to every object edit.

3. (Optional) In the **Change Request Summary** field, edit the subject for the change request.
4. Click **Apply**.


Discard changes made to objects

Discarding changes causes the object to revert to its previous revision in all relevant flows. Optionally, a change request opens in FireFlow to allow any traffic necessary as a result of discarding the object and remove any traffic that is no longer necessary.

Traffic is only removed when it is not necessary for any other applications in AppViz.

Note: This action is only relevant for **Rejected** objects.

To discard changes:

1. View the object you want to edit. For details, see [View a network object](#) or [Service objects](#).
2. In the **Actions** area of the **Dashboard** tab, click .

The **Discard Object Change** dialog box appears.

The dialog box organizes the traffic included in the change request into the following categories:

- **Flows to be added.** The change request will allow this traffic.
- **Flows to be removed.** The change request will deny this traffic.
- **Flows used by other applications.** The change request will not include this traffic as it is necessary for other applications.

Not all categories are relevant to every object edit.

3. (Optional) In the **Change Request Summary** field, edit the subject for the change request.
4. To specify that a change request not be opened in FireFlow, check the **Do not initiate a change request (all affected applications will be updated automatically)**.

Note: Because the original change to the object was rejected (and not implemented on the security policy), opening a change request to discard the changes may not be necessary. But, it is possible that the security policy was changed if, for example, an affected application was edited with the new object definition. If you are certain that no change was implemented on the policy and you don't want to enter the process of submitting a change request, having the object enter the **In Change Process** state, etc, you can specify not to open a change request. In this case, we recommend you manually review any updated

applications.

5. Click **Discard**.


The changes are rejected. The object reverts to its previous revision in all relevant flows, and if relevant, the FireFlow change request opens.

Re-apply changes made to objects

Re-applying changes updates all relevant application flows with changes that have been made to the object since it was rejected in FireFlow. A change request opens in FireFlow to allow any traffic necessary as a result of the changes to the object and remove any traffic that is no longer necessary. Traffic is only removed when it is not necessary for any other applications in AppViz.

Note: This action is only relevant for **Rejected** objects.

To re-apply changes:

1. View the object you want to edit. For details, see [View a network object](#) or [Service objects](#).
2. In the **Actions** area of the **Dashboard** tab, click .

The **Apply Change** dialog box appears.

The dialog box organizes the traffic included in the change request into the following categories:

- **Flows to be added.** The change request will allow this traffic.
- **Flows to be removed.** The change request will deny this traffic.
- **Flows used by other applications.** The change request will not include this traffic as it is necessary for other applications.

Not all categories are relevant to every object edit.

3. (Optional) In the **Change Request Summary** field, edit the subject for the change request.
4. Click **Apply**.

The changes are applied and the change request opens.

Projects

This section explains how to manage projects. It is intended for users with permission to edit all applications.

Tip: To view a training video that follows an application owner managing public and private cloud computing, see [Managing your hybrid cloud security](#).

The video covers migrating from a traditional server to a public cloud server and moving a newly developed application to production in a private cloud environment.

Project types

AppViz supports the following types of projects:

Server Migration Projects	Server Migration projects manage migration from current servers to new servers. The new servers are added to the flows of the relevant applications, but the old servers are not removed. This allows for testing the new environment. Once the server migration project is complete, AppViz offers you the option to initiate removal of the old servers from the traffic flows via a decommission project.
Application Migration Projects	Application Migration projects manage migration of applications to new servers. You select applications to migrate, and you are given the option to migrate any or all of the servers used in the application. AppViz provides a detailed impact analysis of the planned changes, including risk analysis and vulnerability assessment for the application and affected flows.
Application Lifecycle Projects	Application Lifecycle projects manage the migration of multiple applications between different lifecycle phases. They provide the ability to easily plan the server migrations that must occur when transitioning from testing, staging, or production all the way through to decommission.
Server Decommission Projects	Server Decommission projects manage the decommissioning of servers. The servers are removed from the flows of relevant applications.

Note: You cannot add an application to a project if it is pending decommission. If an

application currently being used by a project is decommissioned, it will appear grayed out while it is in the **Pending Decommission** status, and it will be removed from the project once it has the **Decommissioned** status.

Note: You cannot add an object to a project that is pending deletion or add an application to a project if the application has outdated objects. If a project is using an object that is deleted or using an application where the definition of one of its objects has become outdated, an "invalid tasks" warning appears when you attempt to edit the project. You must correct the project to keep it relevant.

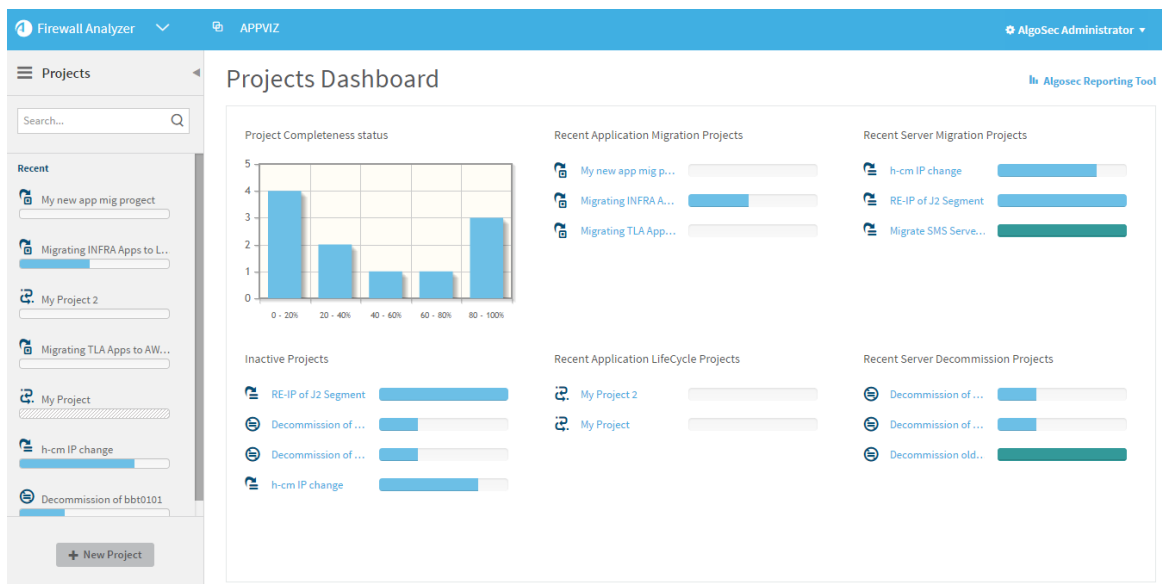
Note: If an object is deleted while it is being used in a project, it will appear grayed out and the delete icon appears on the object's icon. This is true for AppViz objects and imported objects once the object is deleted in AppViz. For device objects, this is true once the FireFlow change request deleting the object is resolved. Note that objects can never be deleted when they are being used by a project **In Progress**. For more details, see [Device objects](#).

View a project


To view a project:

1. Go to the **Projects** area. For details, see [Welcome to AppViz](#).

The **Projects** area appears.



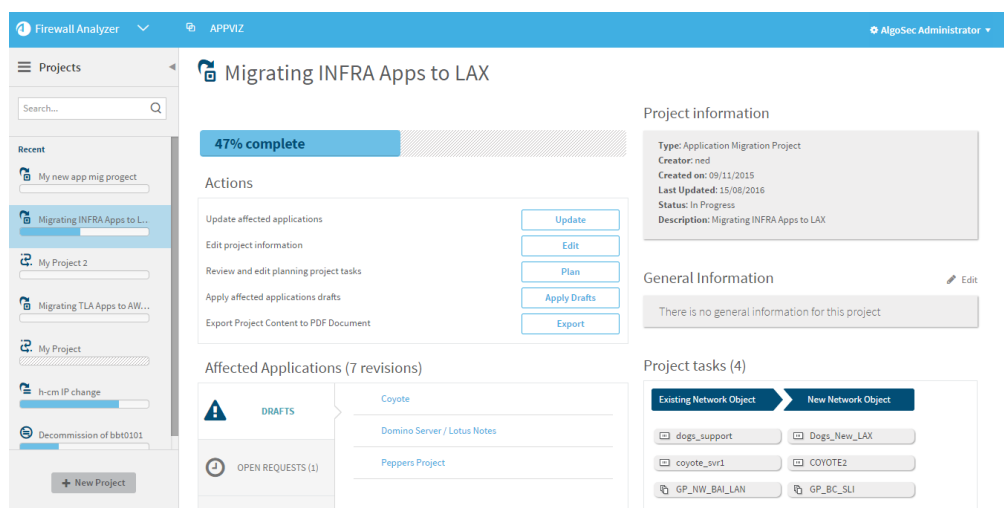
2. Do one of the following:

- Select a project from one of the lists of recent or inactive projects.
- Perform a simple search for a project by doing the following:
 - i. Type any part of the project's name in the search box, and click .


The matching projects appear below the search box.

- ii. Select a project from the list.

The project appears in the workspace.



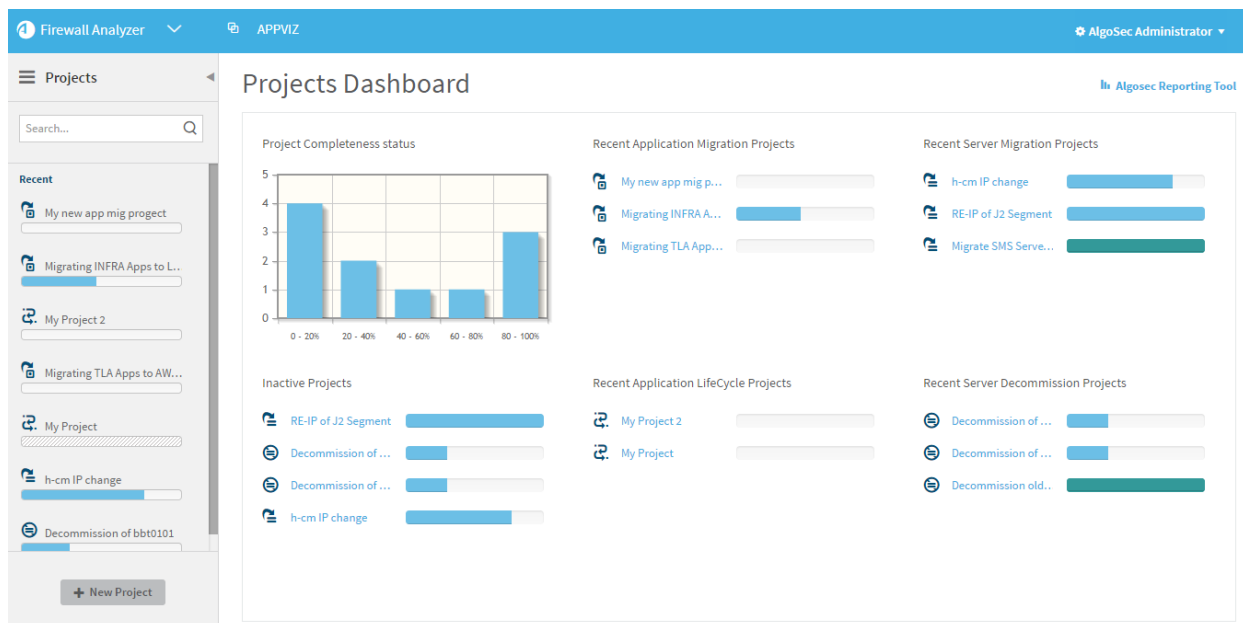
For more details, see [Manage projects](#).

Tip: To return to the other areas available from the main menu, click  at the top left, and select the page you want to navigate to.

Project dashboard

The **Projects Dashboard** provides the ability to:





- Quickly and easily view a summary of the status of current migration, application migration, and decommission projects.
- View a general summary of the completeness of your projects.
- View recent projects and their completeness progress bar.
- View any inactive projects.





The Projects Dashboard Areas

Area	Description
Recent	The left panel displays a list of recent projects of all types. Each project's type is designated by its icon, and each project's completeness is designated by its progress bar.
Project Completeness Status	Displays a graph which shows the number of projects in each range of completeness.
Inactive Projects	Displays a list of inactive projects.
Recent Application Migration Projects	Displays a list of recent application migration projects.
Recent Server Migration Projects	Displays a list of recent server migration projects.
Recent Server Decommission Projects	Displays a list of recent server decommission projects.
Recent Application Lifecycle Projects	Displays a list of recent application lifecycle projects.

The icons next to each project indicate the project type.

This icon...	Indicates...
	Server Migration Project
	Application Migration Project
	Server Decommission Project
	Application Lifecycle Project

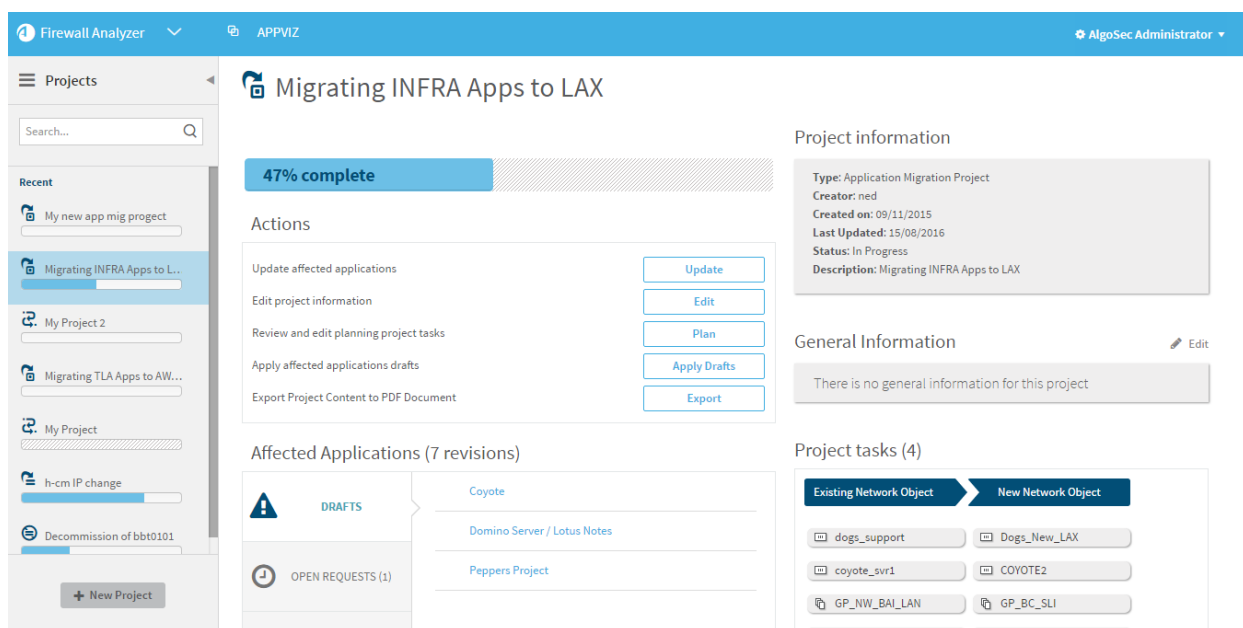
Each project has a progress bar which indicates the completeness of the project.

This color...	Indicates...
	An incomplete project.
	A complete project.

Manage projects

This topic describes how to manage projects in AppViz.

Project interface



The screenshot shows the AppViz interface for a project titled "Migrating INFRA Apps to LAX". The top navigation bar includes "Firewall Analyzer", "APPVIZ", and the user "AlgoSec Administrator". A left sidebar lists recent projects, with the current project highlighted. The main content area features a progress bar at 47% complete, an "Actions" panel with buttons for Update, Edit, Plan, Apply Drafts, and Export, and a list of "Affected Applications (7 revisions)" including Coyote, Domino Server / Lotus Notes, and Peppers Project. On the right, there are sections for "Project information" (Type, Creator, Created on, Last Updated, Status, Description), "General Information" (with an Edit button), and "Project tasks (4)" showing a transition from Existing Network Objects (dogs_support, coyote_svr1, GP_NW_BAI_LAN) to New Network Objects (Dogs_New_LAX, COYOTE2, GP_BC_SLI).

Project Areas

Area	Description
Progress Bar	The project's progress bar displays the project's completeness.

Area	Description
Actions	<p>This area provides the option to:</p> <ul style="list-style-type: none"> • Update. This action allows you to update the applications that are affected by the project. Updating causes new drafts to be created for each of these applications, and you have the option to apply these drafts. For details, see Update a project's applications. • Edit. This action allows you to edit the project. For Server Migration and Server Decommission Projects, this includes editing project tasks. For details, see Edit a project. • Apply Drafts. This action allows you to apply the drafts of all the affected applications. For details, see Apply all application drafts. • Plan. This action allows you to plan tasks for Application Migration or Application Lifecycle projects. For details, see Create an application migration project or Create an application lifecycle project. • Discard. This action allows you to discard the project. For details, see Discard a project. This option is only available for projects which have yet to start. • Close. This action allows you to close a project. For details, see Close a project. This option is only available for projects which have reached completion. • Decommission. This action allows you to open a decommission project to decommission old servers. For details, see Decommission retired servers. This option is only available for server migration projects and application migration projects which are closed. • Export. This action allows you to export the project content to a PDF document. You have the option of selecting which project sections to export: information, affected applications, and project tasks, including detailed Network Object information. For details, see Export project content to PDF.

Area	Description
Affected Applications	<p>This area displays the applications affected by the project and change requests that were initiated for the project. These appear sorted in the following categories:</p> <ul style="list-style-type: none"> <p>• Drafts. All affected applications in the draft revision status. These affected applications have been updated, but have not been applied.</p> <p>In this tab, you have the option to apply all the application drafts. For details, see Apply all application drafts.</p> <p>• Open Requests. All open change requests which were initiated for the project, and their corresponding applications. The applications have been updated and applied, and their change requests are currently being processed.</p> <p>These applications are now in the pending revision status.</p> <p>• Resolved. All resolved change requests which were initiated for the project, and their corresponding applications. The applications have been updated and applied, and their change requests have been resolved.</p> <p>These applications are now in the active revision status.</p> <p>• Rejected. All rejected change requests which were initiated for the project, and their corresponding applications. The applications have been updated and applied, and their change requests have been rejected.</p> <p>These applications are now in the rejected revision status.</p> <p>You can view an application by clicking on the application's name, or view the change request (in FireFlow) by clicking on the change request's ID.</p>

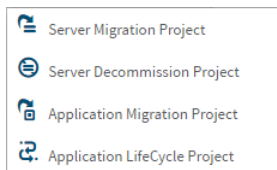
Area	Description
Project Information	<p>Displays the following information about the project:</p> <ul style="list-style-type: none"> • Type. One of the following: <ul style="list-style-type: none"> • Server Migration Project • Application Migration Project • Server Decommission Project • Application Lifecycle Project • Creator. The user that created the project. • Created on. The date the project was created. • Last Updated. The date the project was last updated. • Status. One of the following: <ul style="list-style-type: none"> • Initial (when the project has not yet been planned) • New • In Progress • Complete
General Information	Displays general information that is entered by the creator or project user.
Project Tasks	Displays the project's tasks.

Start a new project

To start a project:

1. Go to the **Projects** area. For details, see [Welcome to AppViz](#).
2. Click **+New Project**.

A menu appears.



3. Select the project type.

The new project form appears in the workspace.

The screenshot shows the 'New Server Migration Project' form in the AppViz workspace. The form is titled 'New Server Migration Project' and has a 'Cancel' button and a 'Create Project' button. The form includes the following fields and sections:

- Project Name:** A text input field with a red asterisk indicating it is required.
- Project Description:** A larger text area for describing the project.
- + Add Task:** A button to add tasks from a file.
- Task List:** A table with three columns: 'Existing Server', 'New Server', and 'Comment'. Below the columns are input fields for each, with a search icon and the text 'Network Object Lookup' and 'Create or Lookup Network Object'.

4. Complete the fields as needed. For details, see:

- [Server migration project fields](#)
- [Application migration project fields](#)
- [Server decommission project fields](#)
- [Application lifecycle project fields](#)

5. Click **Create Project**.

One of the following occurs:

- For Server Migration and Server Decommission projects, the project is created and appears in the workspace.
- For Application Migration and Application Lifecycle projects, the project is created and the **Plan Project** dialog box appears.

The screenshot shows the 'Plan Project' dialog box. The dialog box has a title bar with 'Plan Project' and a close button (X). The main content area contains the question 'Would you like to start planning the project now?' and two buttons: 'Not Now' and 'Start Planning'.

6. For Application Migration and Application Lifecycle projects, do one of the following:

- To start planning the project, click **Start Planning**.


For details, see:

- [Create an application migration project](#)
- [Create an application migration project](#)
- To skip planning for now, click **Not Now**.

The project appears in the workspace.



Server migration project fields

In this field...	Do this...
Project Name	Type the name of the project.
Project Description	Type a description of the project.
+ Add Task	Click this button to add a new task to the project. Each task represents a migration from one server to another.
Add tasks from file	Click this link to upload a CSV file of many tasks to the project. The headers must be the following: Existing IP, New IP, Comment
Existing Server	Do one of the following: <ul style="list-style-type: none"> • Type the Network Object name or IP address of the existing server. • Click Network Object Lookup and select the existing server using the Network Object Lookup wizard. For details, see Create an application migration project. <p>Only single hosts (not groups or ranges) appear in the wizard.</p>


In this field...	Do this...
New Server	<p>Do one of the following:</p> <ul style="list-style-type: none"> Type the Network Object name or IP address of the new server. Click Network Object Lookup and select the new server using the Network Object Lookup wizard. For details, see Create an application migration project. <p>Only single hosts (not groups or ranges) appear in the wizard.</p>
Comment	<p>Type a comment for the task.</p> <p>This field is optional.</p>
	Click this icon to delete a task from the project.

Application migration project fields

In this field...	Do this...
Project	
Project Name	Type the name of the project.
Project Description	Optionally, type a description of the project.
Save Project	Click to create the project. You are asked whether you want to start planning now or wait until later.
Plan	Click this button to start planning.
Plan - Objects for Migrations	

In this field...	Do this...
Applications	<p>Click Add Applications. For details, see Network objects applications.</p> <p>The selected applications are listed in the left panel and all of their network objects are listed in the center panel under View and Add Network Objects.</p>
View and Add Network Objects	<p>In this area select the network objects to include in the migration.</p> <p>To filter the list, you can combine one or more of the following:</p> <ul style="list-style-type: none"> • In the Search box, type all or part of an object name or IP address. Press ENTER to start search. In the drop-down list, select a search match operator. • To filter by network type, click one or more of the type buttons (Host, Range, and Group) to exclude them from the search. Types with available buttons are included in the search. Abstract network objects are not included in application migration projects. • Select or clear the Include Any check box. <p>To select objects, do the following:</p> <ul style="list-style-type: none"> • Select individual objects by clicking their check box, or select all by clicking the check box in the heading. Click Add Selected. • Hover over an object and click +Add.
View Diagrams	<p>Select a network object and click  to show the server connections.</p>
Server Migration List	List of network objects selected for migration.
	To delete a network object from the server migration list, hover over the object and click the trash icon.

Server decommission project fields

In this field...	Do this...
Project Name	Type the name of the project.
Project Description	Type a description of the project.
+ Add Task	Click this button to add a new task to the project. Each task represents the decommissioning of a single server.
Add tasks from file	Click this link to upload a CSV file of many tasks to the project. The headers must be the following: Server IP, Comment
Server IP	Do one of the following: <ul style="list-style-type: none"> Type the Network Object name or IP address of the server. Click Network Object Lookup and select the server using the Network Object Lookup wizard. For details, see Create an application migration project. <p>Only single servers (not groups) appear in the wizard.</p>
Comment	Type a comment for the task. This field is optional.
	Click this icon to delete a task from the project.

Application lifecycle project fields

In this field...	Do this...
Project Name	Type the name of the project.
Project Description	Type a description of the project.

Update a project's applications

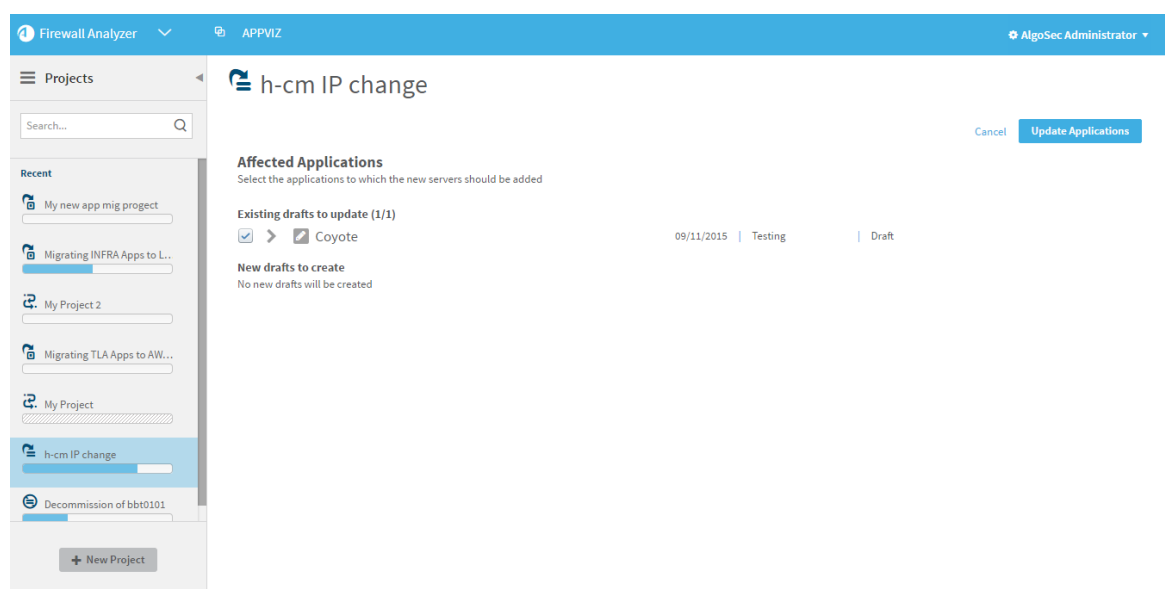
Updating applications creates draft revisions (or edits current drafts) for specified affected applications; these drafts detail the specific changes the project requires for the

application. If desired, you can then apply the application drafts for all or some of the applications.

To update applications:

1. View the project for which you want to update applications. For details, see [Projects](#).
2. In the **Actions** area, click **Update**.

The **Affected Applications** page appears.



The project's affected applications appear, sorted in the following lists:

- **Existing drafts to update.** Applications with a current draft revision. Updating these applications will edit the draft revision of the application with the requirements for the project.
- **New drafts to create.** Applications which do not have a current draft revision. Updating these applications will create a draft revision of the application with the requirements for the project.

- **Flows that will not be updated.** Affected applications which contain flows which contain the decommissioned server. This is only relevant for decommission projects.

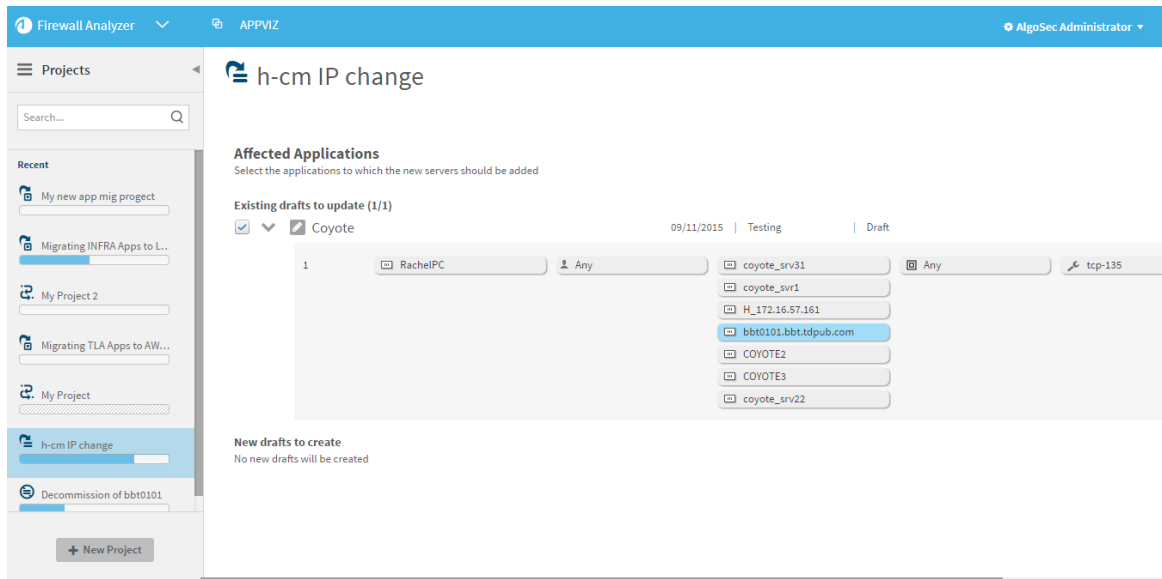
- **Shared flows to be updated**

Note: Shared flows with no instances do not cause a new draft to be created.

- **Applications to decommission**
- **Applications to clone**

3. Select the check box next to each application you want to update.

You can view an application's affected flows by clicking .

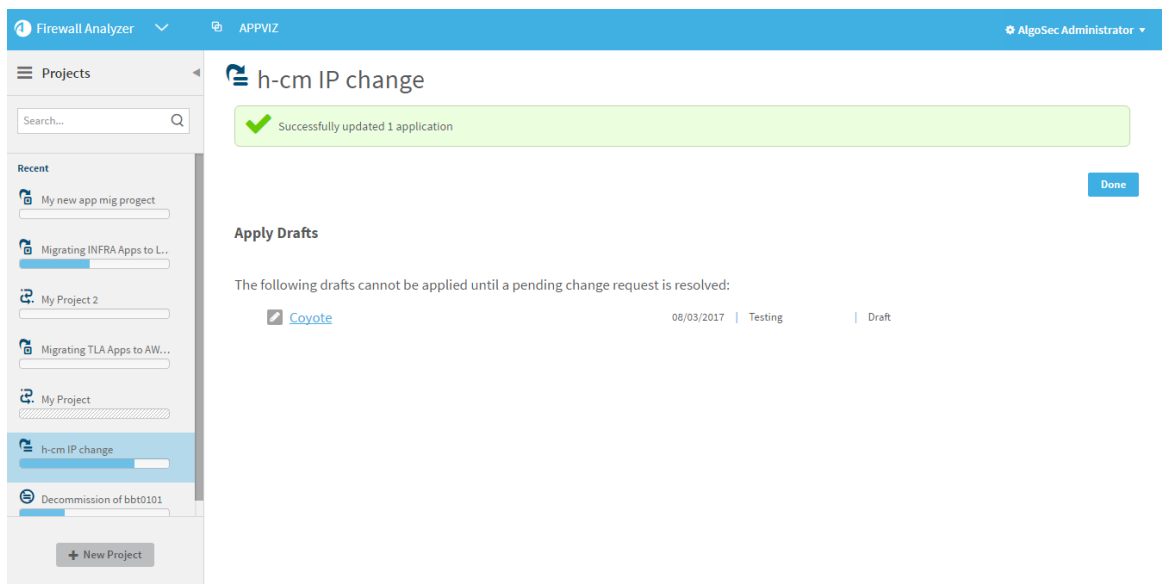


The screenshot shows the Firewall Analyzer interface. The top navigation bar includes 'Firewall Analyzer', 'APPVIZ', and 'AlgoSec Administrator'. The left sidebar shows a list of projects, with 'h-cm IP change' selected. The main content area displays the 'Affected Applications' section for the selected project. It includes a search bar, a 'Recent' list, and a table of 'Existing drafts to update (1/1)'. The table has columns for draft ID, application name, user, date, testing status, and draft type. The 'Affected Applications' section also includes a 'New drafts to create' section, which states 'No new drafts will be created'.

Existing drafts to update (1/1)	09/11/2015	Testing	Draft
1	RachelPC	Any	coyote_srv31 coyote_srv1 H_172.16.57.161 bbt0101.bbttdpub.com COYOTE2 COYOTE3 coyote_srv22

4. Click **Update Applications**.

A new draft with the change dictated by the project is created for each selected application (or the existing draft is updated), and the **Apply Drafts** page appears.



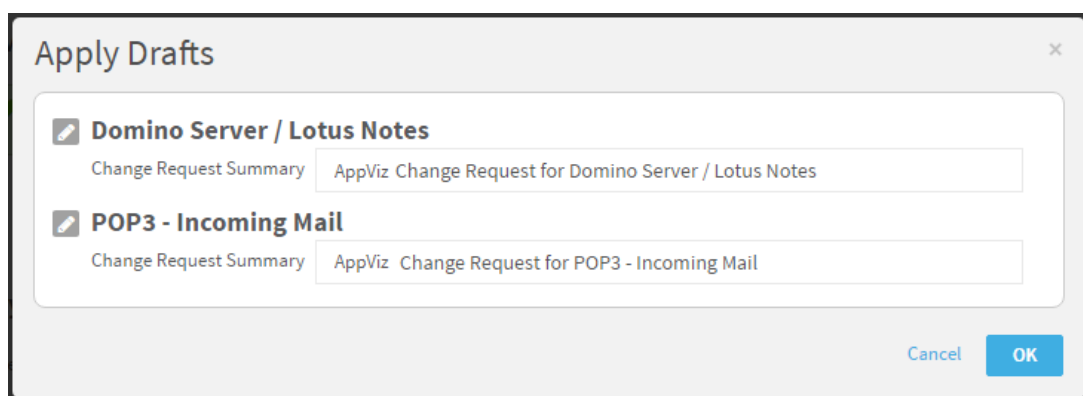
5. Do one of the following:

- To exit without applying the application drafts, click **No thanks**.
- To apply some or all of the application drafts, do the following:

Note: AppChange will create one change request for each application.

1. Select the check box next to each application whose draft you want to apply.
2. Click **Apply Selected**.

The **Apply Drafts** dialog box appears.



3. (Optional) Change the subject of the change request that will open in

FireFlow for each application by editing the **Change Request Summary** field.

Note: You can optionally customize a default change request summary specifically for Decommission change requests. For details, see [Customize interactions with AFA and FireFlow](#).

4. Click **OK**.

The drafts are applied and the change requests are created in FireFlow.

The project appears.

Edit a project

To edit projects:

1. View the project you want to edit. For details, see [Projects](#).
2. In the **Actions** area, click **Edit**.

The project's details appear in an editable format.

The screenshot displays the 'Edit Server Migration Project' interface in AppViz. The top navigation bar includes 'Firewall Analyzer', 'APPVIZ', and 'AlgoSec Administrator'. The sidebar on the left shows a 'Projects' list with a search bar and a 'Recent' section containing several project entries. The main content area is titled 'Edit Server Migration Project' and includes a 'Cancel' button and a 'Save Changes' button. The form contains the following fields:

- Project Name:** h-cm IP change
- Project Description:** Due to duplication made by IP assignment mistake we need to change the ip of the h-cm-segment to new IP addresses. Thanks, Joe

Below the form is an '+ Add Task' button with the text 'Add tasks from file'. A table below that shows the migration process:

Existing Server	New Server	Comment
10.176.51.2 (h-cm-10.176.51.2-wsb)	h-cm-10.176.61.203	
10.176.57.131 (h-cm-10.176.57.131)	PC_GEO_PICTALK_Temp	
66.101.58.38 (PC_SCR_scr0801_EXT)	dogs_support	

3. Edit the fields as needed. For details, see:

- [Server migration project fields](#)
- [Application migration project fields](#)
- [Server decommission project fields](#)
- [Application lifecycle project fields](#)

4. Click **Save Changes**.

The changes are saved.

Apply all application drafts

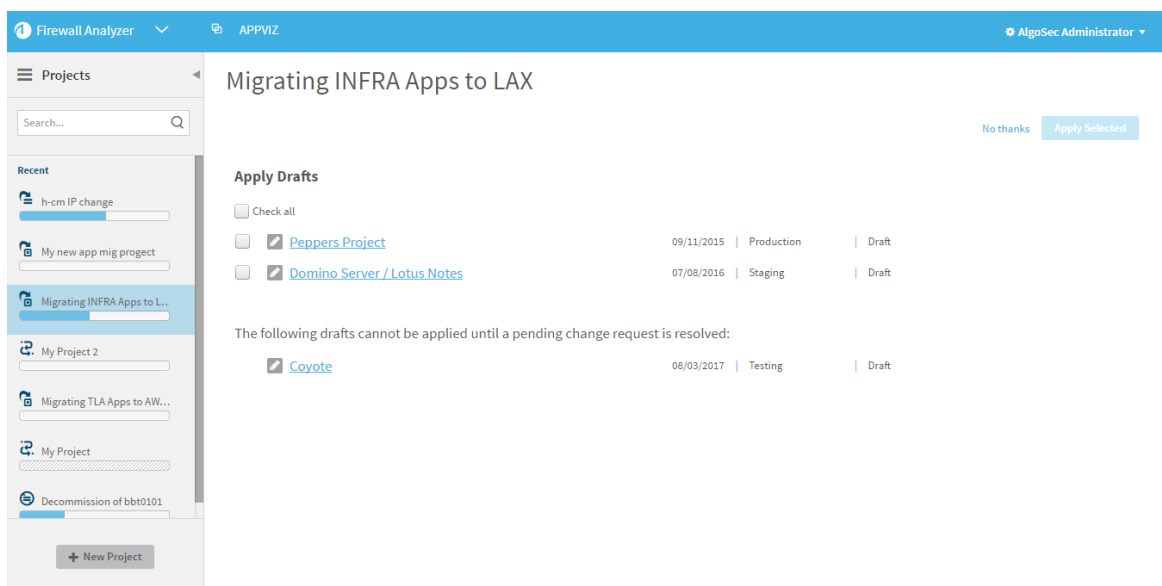
You have the option to simultaneously apply the drafts of many or all a project's affected applications. Otherwise, this can be accomplished immediately after creating the drafts (as a part of updating applications) or manually, one application at a time.

Note: AppChange will create one change request for each application.

To apply all application drafts:

1. View the project you want to edit. For details, see [Projects](#).
2. In the **Actions** area, click **Apply Drafts**.

The **Apply Drafts** page appears.

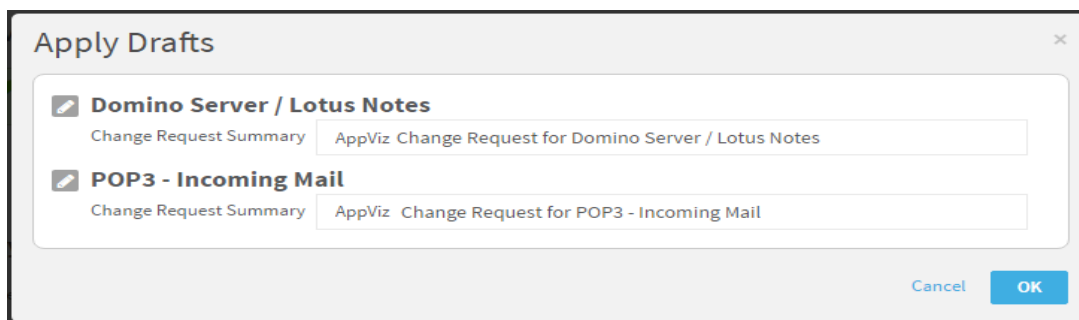


3. Select the check box next to the application drafts you want to apply.

If an application's draft includes changes other than the changes relevant to the project, a warning message appears when the application is selected.

4. Click **Apply Selected**.

The **Apply Drafts** dialog box appears, with a list of the selected applications.



5. (Optional) Change the subject of the change request that will open in FireFlow for each application by editing the **Change Request Summary** field.
6. Click **OK**.

The drafts are applied, and the change requests are created in FireFlow.

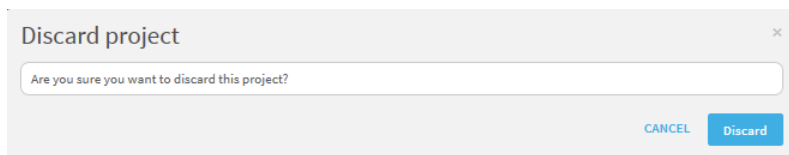
Discard a project

Note: You can only discard projects which have not been started.

To discard projects:

1. View the project you want to edit. For details, see [Projects](#).
2. In the **Actions** area, click **Discard**.

A confirmation message appears.



3. Click **Discard**.

The project is discarded.

Close a project

Note: You can only close projects which have reached completion.

To close projects:

1. View the project you want to edit. For details, see [Projects](#).
2. In the **Actions** area, click **Close**.

The project is closed without confirmation.

Decommission retired servers

Once a Server Migration or Application Migration project is completed, you can automatically open a decommission project to decommission the retired servers.

To decommission the retired servers:

1. View the project you want to edit. For details, see [Projects](#).
2. In the **Actions** area, click **Decommission**.

The new decommission project appears with editable fields. The servers to decommission are already added as tasks for the project.

3. Edit the fields as desired. For details, see [Server decommission project fields](#).
4. Click **Save Changes**.

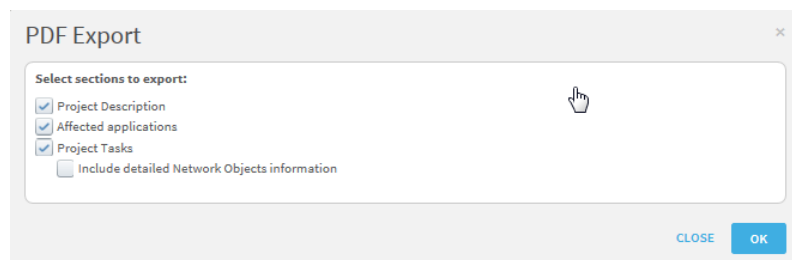
The project is created and appears.

Export project content to PDF

To export project content:

1. View the project you want to edit. For details, see [Projects](#).
2. In the **Actions** area, click **Export**.

The **PDF Export** dialog box appears.



3. Select the information to export, and click **OK**.

Your browser will prompt you to save or open the PDF file.

Create an application migration project

This topic describes how to create an application migration project. For more details, see [Projects](#) and [Manage projects](#).

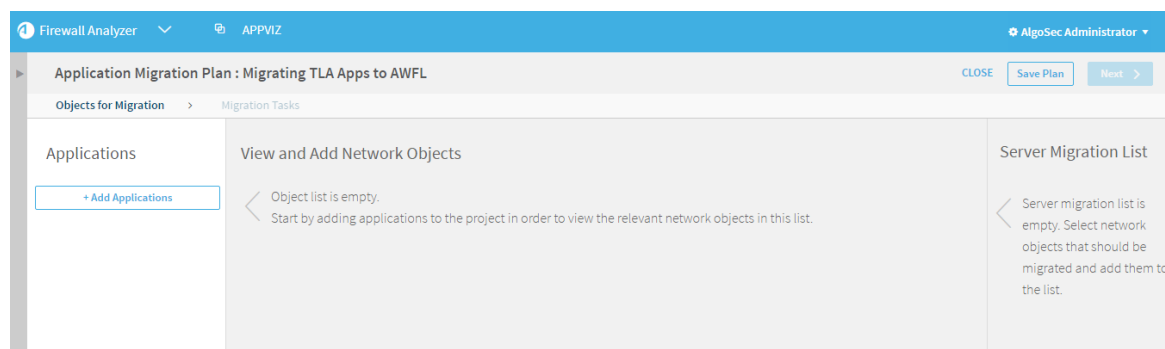
Plan an application migration project

Note: You can save and close the plan at any point. For details, see [Save an incomplete plan](#).

To plan an application migration project:

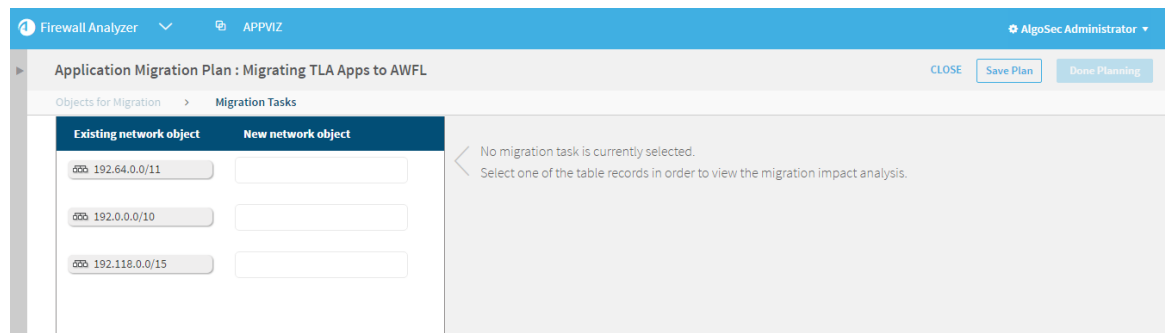
1. View the project you want to edit. For details, see [Projects](#).
2. In the **Actions** area, click **Plan**.

The **Application Migration Plan** page appears in the **Objects for Migration** stage. The left menu automatically hides.



3. Select applications and network objects to migrate. For details, see [Select applications and network objects](#).
4. Click **Next**.

The project proceeds to the **Migration Tasks** stage.



5. Select the network objects to migrate to. For details, see [Migrate network objects](#).

6. Click **Done Planning**.

Note: This option is only enabled once all objects have been assigned.

The project's page appears, displaying the **Project Tasks** and each task's details.

The screenshot displays the AppViz interface for a project titled "Migrating INFRA Apps to LAX". The top navigation bar shows "Firewall Analyzer" and "APPVIZ" with the user "AlgoSec Administrator". The left sidebar lists recent projects, with "Migrating INFRA Apps to LAX" selected. The main content area shows a progress bar at 47% complete. Below the progress bar is an "Actions" panel with buttons for "Update", "Edit", "Plan", "Apply Drafts", and "Export". The "Affected Applications (7 revisions)" section lists "Coyote", "Domino Server / Lotus Notes", and "Peppers Project". The "Project tasks (4)" section shows a transition from "Existing Network Object" to "New Network Object" and lists tasks: "dogs_support", "Coyote_Svr1", "GP_NW_BAI_LAN", "Dogs_New_LAX", "COYOTE2", and "GP_BC_SLI".

Save an incomplete plan

You have the option to save a project plan at any time. You can return to the saved plan at any time by clicking **Plan** in the project's action area.

To save an incomplete plan:

1. In the top right corner, click **Save Plan**.

The changes you made to the plan are saved and a notification appears at the top of the page.

2. To exit the project, click **Close**.

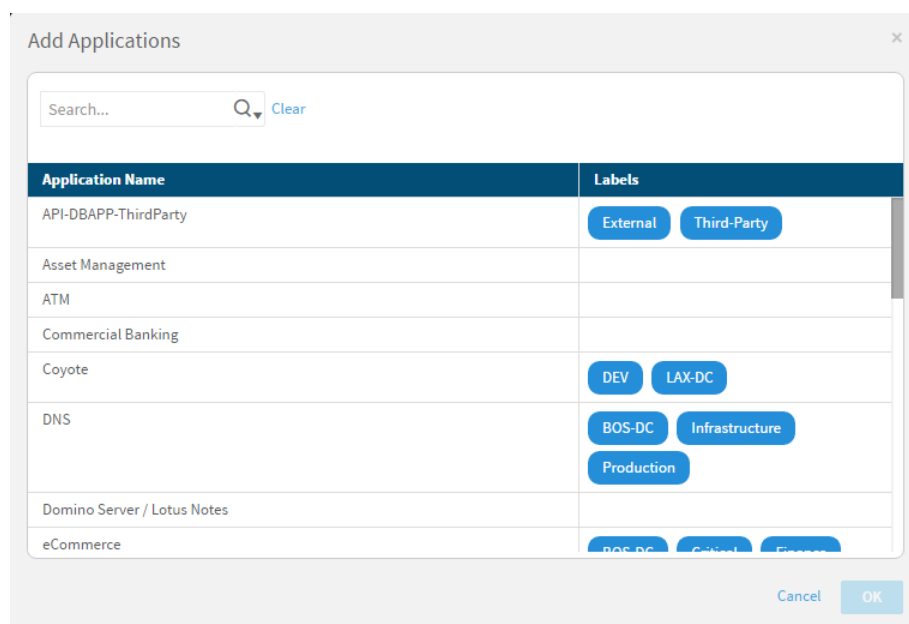
Select applications and network objects

Note: Only the most recent revision is shown in all services.

To select applications and network objects:

1. Click **+Add Applications**.

The **Add Applications** dialog box appears.



2. Select applications using the information in For details, see [Use the Add Applications wizard](#).

Selected applications appear in the left panel, in the **Applications** list.


The network objects used in the selected applications appear in the center panel, in the **Object** column. The **Affected Applications** column displays the number of affected applications for each object.


Note: If the object affects an application that has not been added to the project, the **Affected Applications** column additionally contains a notification stating the number of affected applications which are not in the project.

The screenshot shows the 'Application Migration Plan' interface. The main content area is titled 'View and Add Network Objects'. It includes a search bar with the text 'Find Name or IP', a dropdown menu set to 'Auto', and a checked 'Include Any' checkbox. There are three buttons: 'Host', 'Range', and 'Group'. Below this is a table with 16 objects. The table has two columns: 'Object' and 'Affected Applications'. The objects listed are: 192.64.0.0/11 (1), 192.0.0.0/10 (1), 192.118.0.0/15 (1), 192.97.14.71 (1), 192.125.114.238 (1), 192.168.12.22 (1 (2 not in project)), and 192.168.10.40 (1 (1 not in project)). To the right of the table is a 'Server Migration List' which is empty and contains a message: 'Server migration list is empty. Select network objects that should be migrated and add them to the list.'

- To hide an application's network objects, click  next to the application's name.

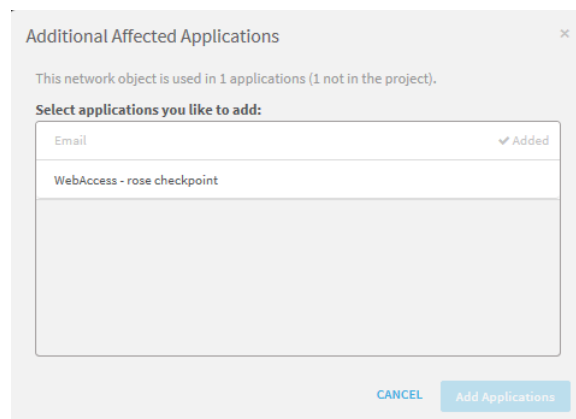
Note: Even though the objects do not appear, the application is not removed from the project.

To reveal the application's network objects, click  next to the application's name.

- To remove an application and its network object from the project, click .
- To filter the list of network objects, do one or more of the following:
 - In the search box, type a name or IP address.
Optionally, select an operator in the **Auto** drop-down list. For details, see [Application dashboard](#).
 - Clear or select the **Include Any** check box.
 - To filter by network object type, click one or more of the **Show** buttons (**Host**, **Range**, and **Group**).
 - The first **Show** button you click causes all other buttons to become disabled (and consequently not appear in the results).

- Clicking additional buttons causes the object type you click to toggle: if it was enabled it will become disabled and vice versa.
 - By default, all **Show** buttons are enabled (all objects appear in the results).
6. To add affected applications to the project, do the following:
- a. Click the **not in project** link in the affected applications column.

The **Additional Affected Applications** dialog box opens.



All affected applications, including those which are not included in the project, are listed.

- b. Select the application you want to add to the project.
- c. Click **Add Applications**.

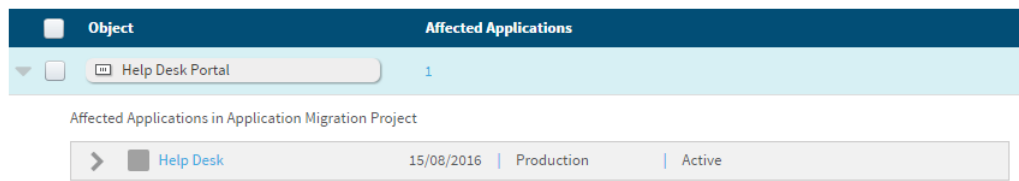
The application is added to the project. The application appears in the **Applications** list in the left panel, and all of its network objects appear in the list of network objects in the center panel.

Note: Adding additional applications may result in additional network objects with affected applications not in the project.

7. To view the affected applications and flows for a specific network object, do the following:

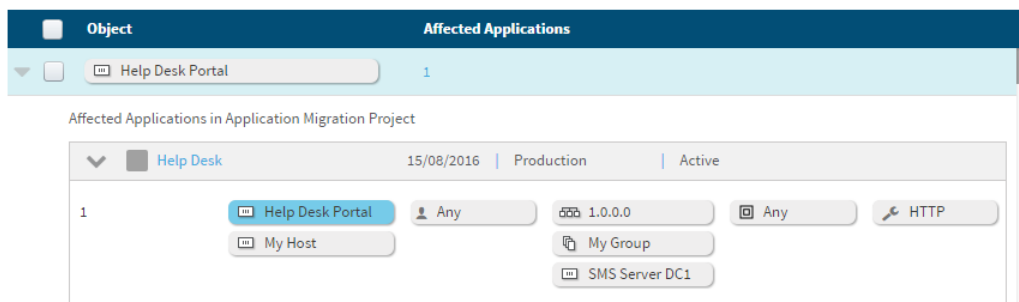
- a. To view the affected applications, click ▶ to the left of the object.

The application appears.



- b. To view the affected application's affected flows, click >.

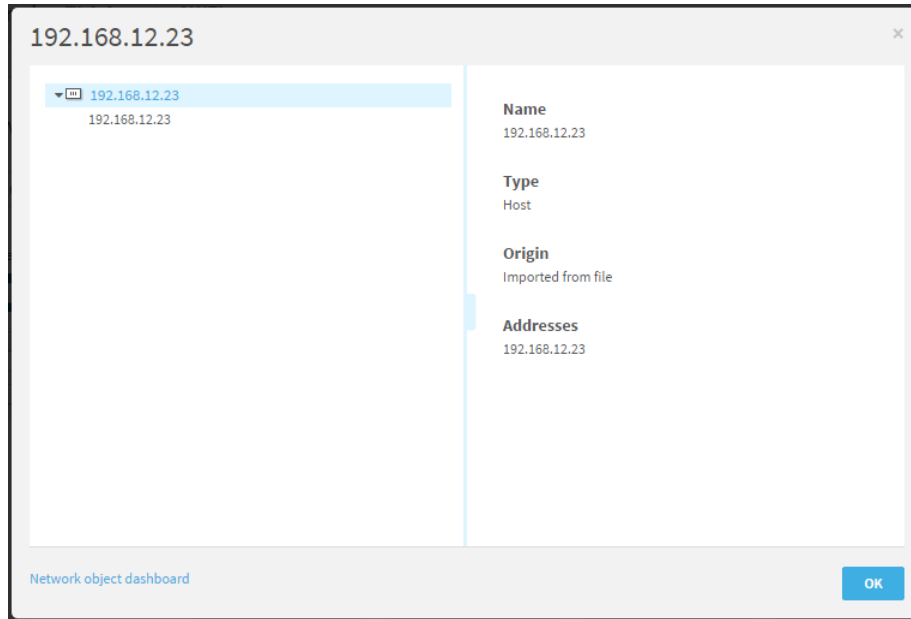
The affected flows appear. The network object appears in orange.



The relevant network object appears highlighted in blue. Hovering over any object displays its contents.

- c. To view network object details, double click on an object.

A window opens with network object's information.



To see the network object's AppViz page, click **Network object dashboard**.

To view application flow diagrams :

1. Do one of the following:

- To view the application diagrams relevant to a specific network object, hover over the network object and click the  icon.

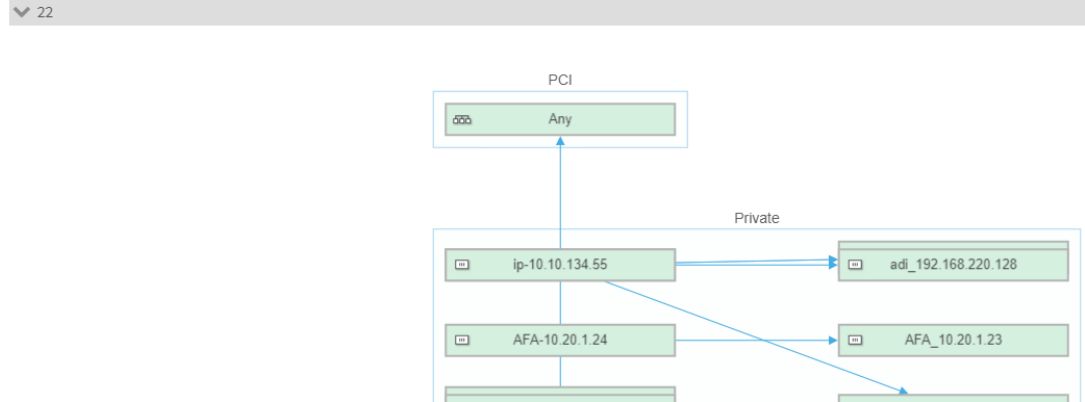
The **View instances of** page opens for the specified network object.

The specific network object is highlighted in yellow.

- To view all the application diagrams for the project's applications, click [VIEW DIAGRAMS](#)

The **View Diagrams** page appears.

View Diagrams
0 selected



To view an application's diagram, click **>** next to the application's name.

To select objects for migration :

1. Do one of the following:

- To migrate all, select the check box at the top of the list and click **Add Selected.**
- Select the check box at the top of the list and clear the check boxes of those objects to not migrate. Click **Add Selected.**
- Hover over the object to select and click **+Add** on the right.

At the top are the number of objects and number selected for migration.

View and Add Network Objects



Find Name or IP Auto Include Any

42 Objects | 8 Selected VIEW DIAGRAMS ADD SELECTED

Object	Affected Applications	
<input type="checkbox"/> DomainController1	1	ADDED
<input type="checkbox"/> NET10.243.101.0-24	1	ADDED
<input type="checkbox"/> AuthCenter	1	ADDED
<input type="checkbox"/> 10.10.85.11	1	
<input checked="" type="checkbox"/> h-cm-10.176.57.163	1	+ADD
<input type="checkbox"/> IP10.1.47.192	1	
<input type="checkbox"/> GP_NW_SLL_LAN	1 (1 not in project)	

The selected objects are added to the Server Migration List and **ADDED** appears in the object row.

To remove network object and application selections:


1. To remove a network object from the Server Migration List:
 - Hover in center table row and click **Remove**, or
 - In the Server Migration List, hover over the object and click .
 2. To remove an application from migration, hover over the application and click .
- The associated network objects are removed also.

If an application is deleted only those network objects related only to the application are deleted from the project.

If a network object belongs to non-deleted applications, it remains on the list.

Use the Add Applications wizard

To use the add applications wizard :

1. To filter the applications, do one or both of the following:
 - Perform a simple search for an application:
 - i. To specify whether to search only by label or only by application name, Click  and select the desired parameter in the drop-down menu.

By default, both application labels and names are searched.
 - ii. Type any part of the application name in the search box and press enter.
 - (For adding applications to Application LifeCycle projects only) Filter the list of applications by lifecycle phase, by clicking one or more of the **Show** buttons.

Clicking the **Show** button excludes applications in that lifecycle phase from the list. If all **Show** buttons are selected, all applications appear.

- The first **Show** button you click causes all other buttons to become disabled (and consequently not appear in the results).
- Clicking additional buttons causes the phase you click to toggle: if it was enabled it will become disabled and vice versa.
- By default, all **Show** buttons are enabled (all applications appear in the results).

2. Select one or more applications from the list.

The number of selected applications appears in the top of the window.

3. To deselect all applications, click **Clear**.
4. Click **OK**.

Migrate network objects

To assign network objects to migrate to:

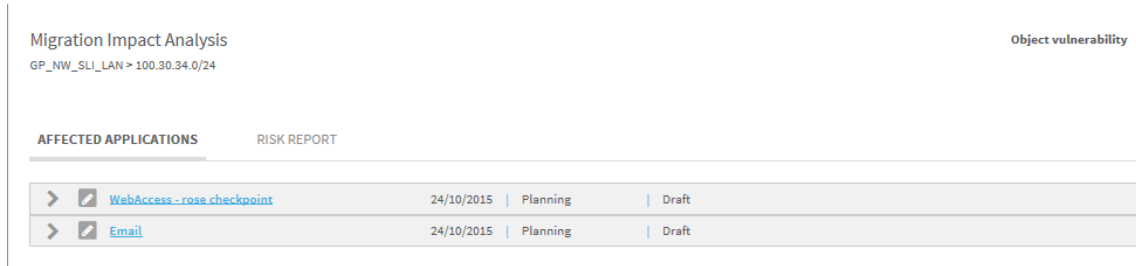
1. For each existing network object, in the new network object column, click **Create or Lookup Network Object**.

The **Lookup Network Object** wizard opens.

2. Select an existing object, or create a new network object. For details, see [Use the network object lookup wizard](#).

The selected or new object appears in the New network object column.

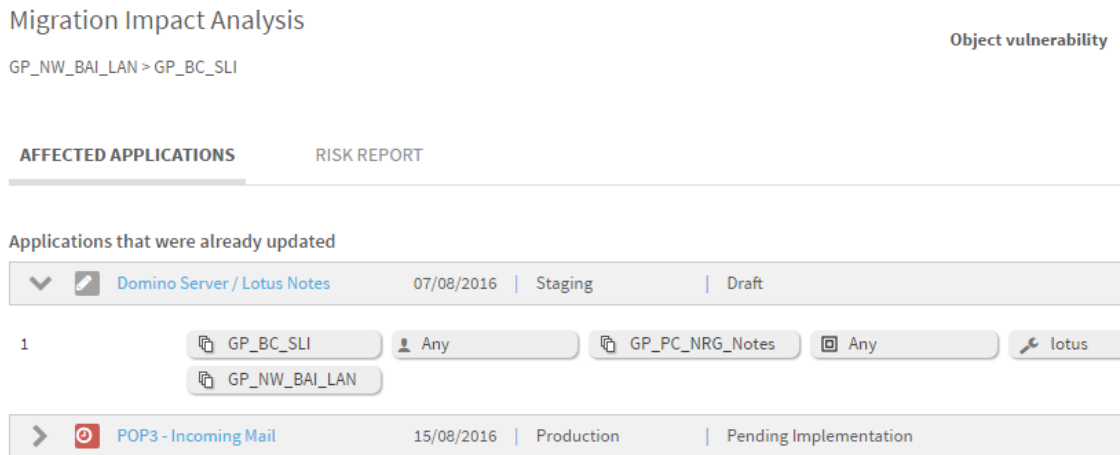
As the assignments are made for each new network object, AppViz performs a Migration Impact Analysis.



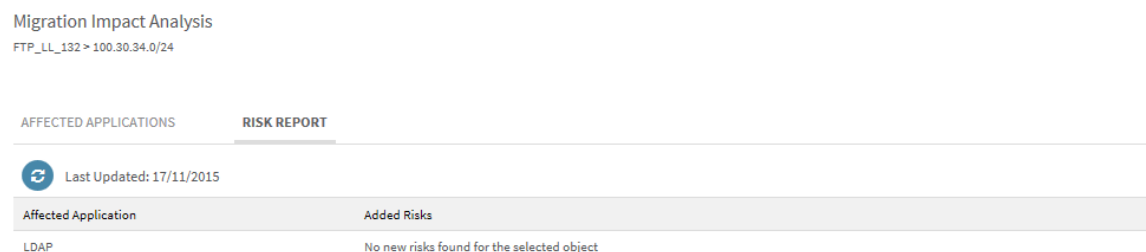
3. Click the **Affected Applications** tab.

The affected applications are listed in the central pane with the application name, date last modified, lifecycle phase, and status.

4. Click next to the application to show the details for each application.




5. Click the **Risk Report** tab. If a report is not available, AlgoSec performs the risk analysis.



The date the last update to the report is shown. For each Affected Application, the Added Risks, if any, are listed.

For additional information, see [Application risks](#).

6. If vulnerability assessment is configured, also view the Vulnerability Analysis (see [Application vulnerability](#)) for the vulnerability score of existing and new objects.
7. At this point you can:
 - a. Change the network object assignment, by clicking **x** in the New network object input box and selecting a new object. A new Impact Analysis is performed.
 - b. Remove the Existing network object from the project by clicking  at the end of the network object row.

Use the network object lookup wizard

Use this procedure while selecting or adding a network object for an Application Migration or Application Lifecycle Projects.

To select a network object using the Network Object Lookup wizard:

1. Click the **Create or Lookup Network Object** link below the field in the new network object column.

The **Network Object Lookup** wizard appears.

Network Object Lookup

AUTO ▾ +New Network Object

Show HOST RANGE GROUP

Name	Members	Addresses
0.0.0.0/0		0.0.0.0/0
10.0.0.0/8		10.0.0.0/8
10.0.0.0/8		10.0.0.0-11.0.0.0
100.120.130.7		100.120.130.7
100.30.34.0/24		100.30.34.0-100.30.35.0
100.77.19.103		100.77.19.103
100.77.19.195		100.77.19.195
100.77.20.51		100.77.20.51

CLOSE Add

Note: If device objects with the same name (but different content) appear, the device on which the object is defined is indicated.

2. Do one of the following:


- Select one or more network objects from the list, and click **Add**.
- To filter the list, click one or more of the **Show** buttons to exclude the type of object from the list. For example, to not show servers of the type Group, click **Group**.

If all **Show** buttons are selected, all objects appear.

- Search for a network object, by doing the following:

- i. (Optional) Select a search parameter by clicking AUTO ▾ and selecting one of the following options from the drop-down menu.

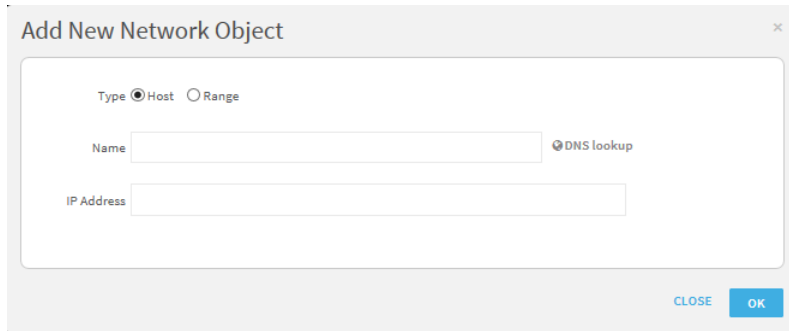
Search parameter	A search will return...
Containing the range	All network objects that contain the searched content.
Contained within the range	All network objects that are entirely contained in the searched content.
Exact address match	All network objects that are an exact match of the searched content.
Intersection	All network objects that have any overlap with the searched content.
Match as object name	All network objects whose name contains the searched phrase.
Auto	All network objects whose names contain the searched phrase.

2. Type the search into the search box, and click .
3. Select a network object from the list below the search box.
 - Add a new network object by clicking **+New Network Object** and following the directions [Add a network object for migration](#).
3. Click **OK**.

Add a network object for migration

To add a new network object:

1. The **Add New Network Object** dialog box opens.



2. Select the type.
3. In the **Name** field, type the name of the new object.
4. To perform a reverse DNS lookup on the network object Name, click **DNS lookup**.
If the IP address is found for the object, the address is inserted in the **IP Address** field.
5. If reverse DNS lookup was not used or was unsuccessful, type a the IP address in the field.
6. Click **OK**.

Create an application lifecycle project

This topic describes how to create a AppViz application lifecycle project. For more details, see [Projects](#) and [Manage projects](#).

Note: You can save and close the plan at any point. For details, see [Save an incomplete plan](#).

Plan your project to determine the changes that occur as the related applications move between lifecycle stages.

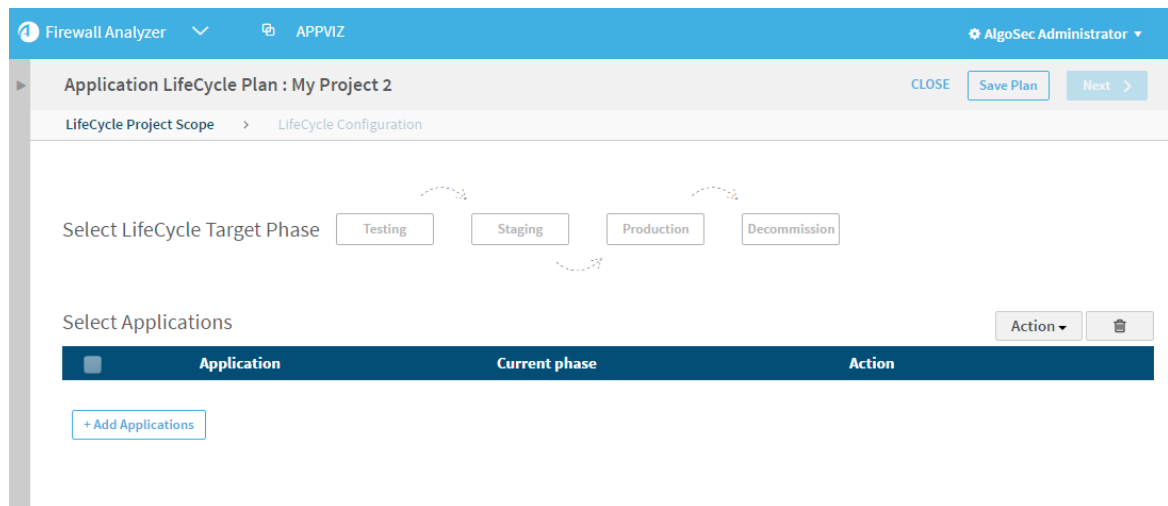
At each stage:

- Applications defined with **Move** actions will be changed as defined when the application enters the target phase.
- Applications with **Clone** actions are duplicated, and the change is applied to the duplicate instead. The original application is not affected.

Do the following:

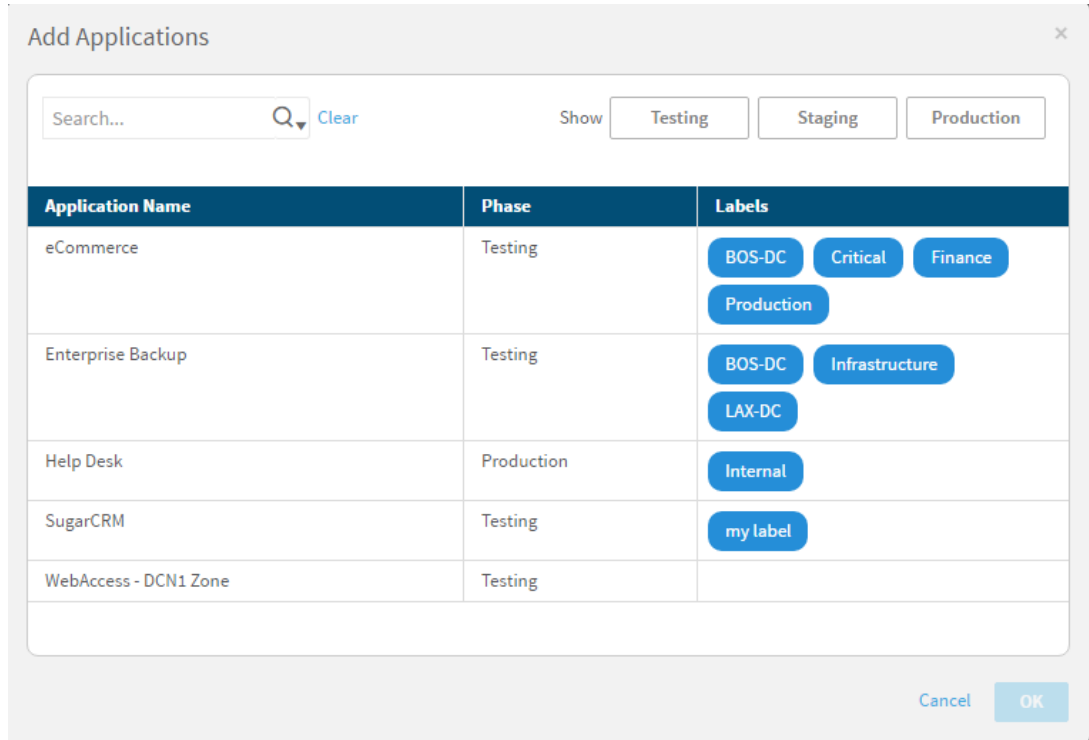
1. View the project you want to plan. For details, see [Projects](#).
2. In the **Actions** area, click **Plan**.

The **Application LifeCycle Plan** page appears in the **LifeCycle Project Scope** stage.



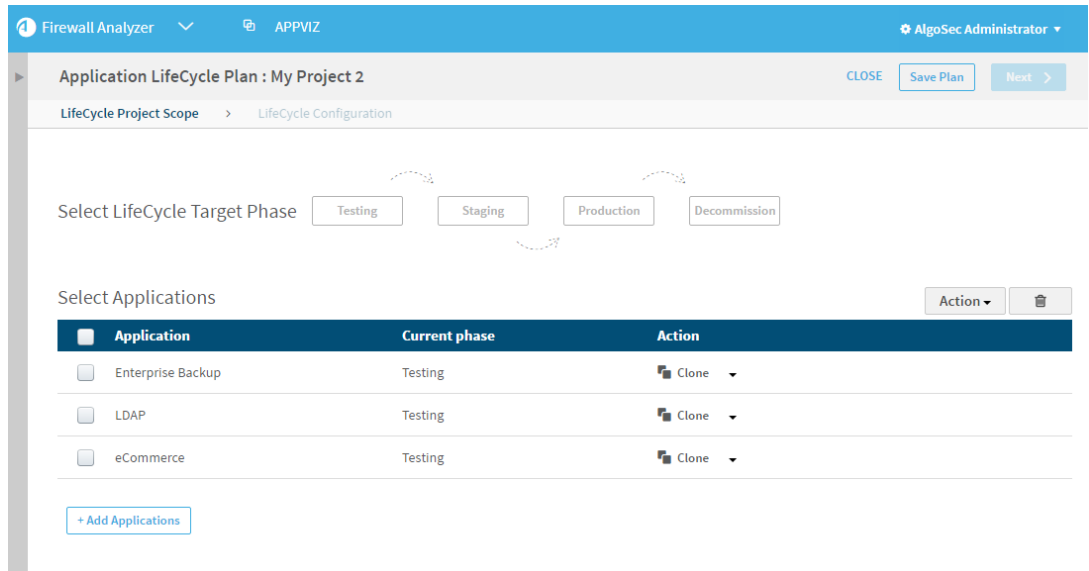
3. Define the changes that you want to occur as the related applications move between lifecycle phases:
 - a. Select a **Target Phase**. The changes you specify in the next steps occur when the application moves into this phase.
 - b. Click **+ Add Application**, and select the applications you want to add to the project.

For example:

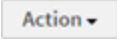



The selected applications appear in the **Application Lifecycle Plan** page assigned the default action, **Clone**.

For example:



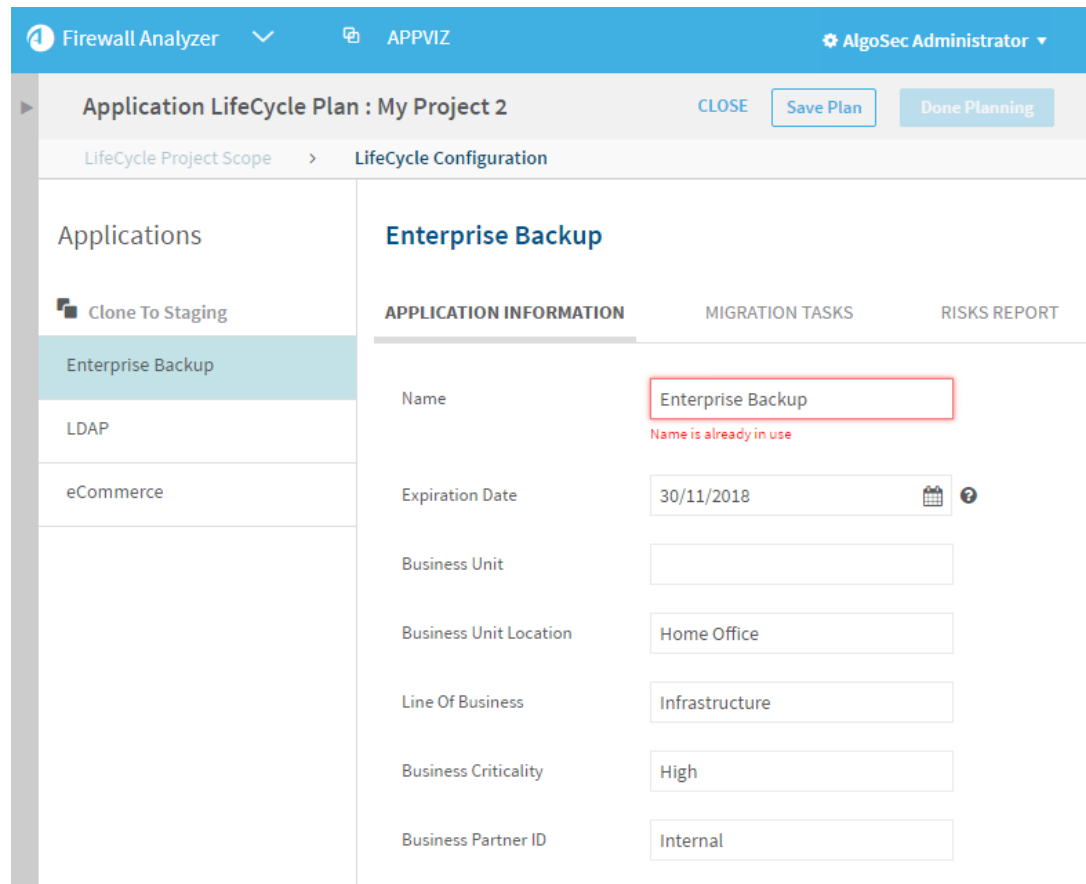
For more details, see [Business applications](#).

- c. Assign an action for each application by doing one of the following:
- Select an action for a single application from the **Action** column.
 - Use the checkboxes to select one or more applications.
- Click  and select an action to apply to all selected applications.

Note: To remove an application, use the checkbox to select one or more applications, and then click .

4. Do one of the following:
- For the **Decommission** phase, skip to the [last step](#) to complete the planning.
 - For all other phases, click **Next**. The **Application Lifecycle Plan** page appears in the **LifeCycle Configuration** stage. The selected applications appear in the left panel, sorted by their **Action**.

For example:



5. Define the **APPLICATION INFORMATION** fields for each application configured.

Select the application on the left, and then define values for the following fields:

<p>Name</p>	<p>Enter a name for the application.</p> <p>Note: When cloning applications, you must change the name of the application.</p>
<p>Expiration Date</p>	<p>Click the calendar icon to select an expiration date.</p> <p>Note: Expiration date may be modified in edit mode.</p>
<p>Business Unit</p>	<p>Type the name of the business unit.</p>

7. View risk details for each application defined.

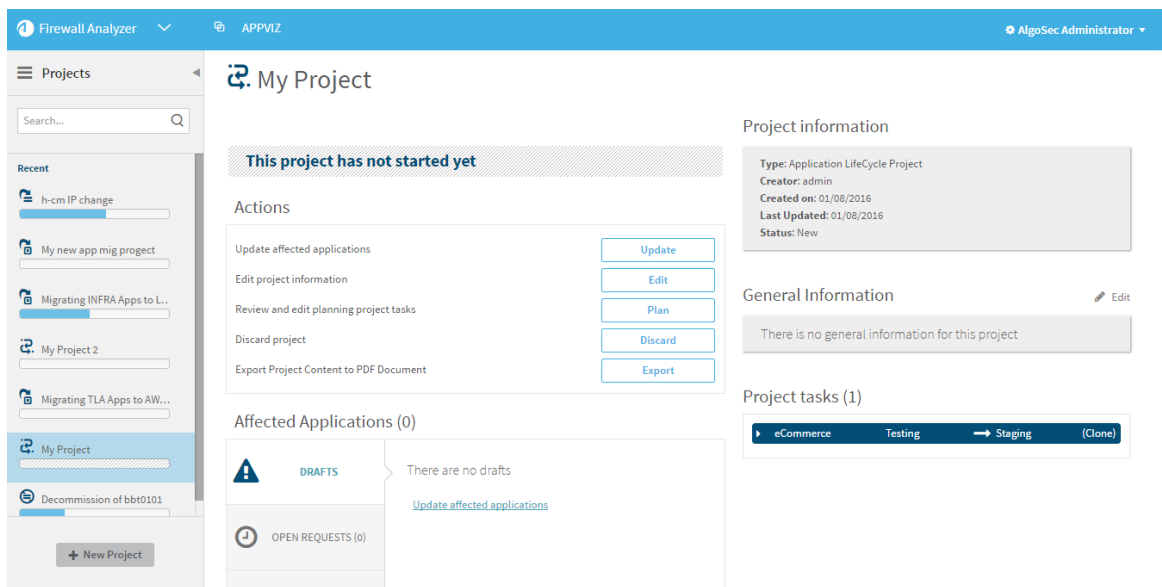
Click the **RISKS REPORTS** tab, where AppViz displays risk information retrieved from AFA that is relevant to the new network objects.

Note: You must specify the migration tasks for each object in the **Migrations Tasks** tab before accessing the **Risks Report** tab.

8. Click **Done Planning**.

Note: This option is only enabled once all objects have been assigned.

The project's page appears, displaying the **Project Tasks** and each task's details.



AppViz administration

Relevant for AppViz administrators

This section describes how administrators can configure and customize AppViz.

For details, see:

- [AppViz users, permissions, and roles](#)
- [Custom fields](#)
- [Security zones](#)
- [Critical processes](#)
- [Configure applications](#)
- [Manage vulnerability assessment scanners](#)
- [Customize interactions with AFA and FireFlow](#)
- [Logging and notifications](#)
- [Discovery settings](#)
- [AppViz maintenance](#)

After some AppViz configurations, you may be required to restart AppViz. For details, see [Restart AppViz](#).

AppViz users, permissions, and roles

Relevant AppViz administrators

This section describes how to manage AppViz users, roles, and permissions.

Roles and permissions

AppViz supports the ability to customize application permissions for individual users or roles. You can manage permissions from the perspective of the user/role, or from the perspective of the application. The table below describes the default permissions for each user type.

Role	Permissions
Unprivileged user (FireFlow requestor)	<ul style="list-style-type: none"> • Create application • View and refresh vulnerability • Edit network object • Edit service object
Privileged user	<ul style="list-style-type: none"> • All unprivileged permissions • View and refresh risks data
Administrator	All permissions

Note: Users automatically have permissions for any applications they create.

Create new unprivileged users

This procedure describes how to create a new unprivileged user for a AppViz application. Users are created in FireFlow, and are visible in both FireFlow and AppViz.

Do the following:

1. In AppViz, at the top-right, click your username and select **Administration**.
2. In the **Administration** area, navigate to the **GENERAL** tab > **Settings and Permissions** > **Manage application permissions**, and click **Manage**.

The **Application Permissions** page appears, displaying a list of applications on the left.

3. On the right, click **Add Users**.
4. At the bottom of the dialog that appears, click **Create Users in FireFlow**.

Continue with creating your user as a requestor in FireFlow.

Manage permissions for applications


You can give single users, or all users with a specific role, permission to view or edit an application that they do not have permission for by default. The procedure below describes how to manage user permissions for a specific application.

To manage permissions for an application:

1. In AppViz, at the top-right, click your username and select **Administration**.
2. In the **Administration** area, navigate to the **GENERAL** tab > **Settings and Permissions** > **Manage application permissions**, and click **Manage**.

The **Application Permissions** page appears, displaying a list of applications on the left.

3. Do one of the following:

- Select an application from the list.
- Perform a simple search for an application by doing the following:
 - i. Type any part of the application name in the search box, and click  .

The matching applications appear below the search box.

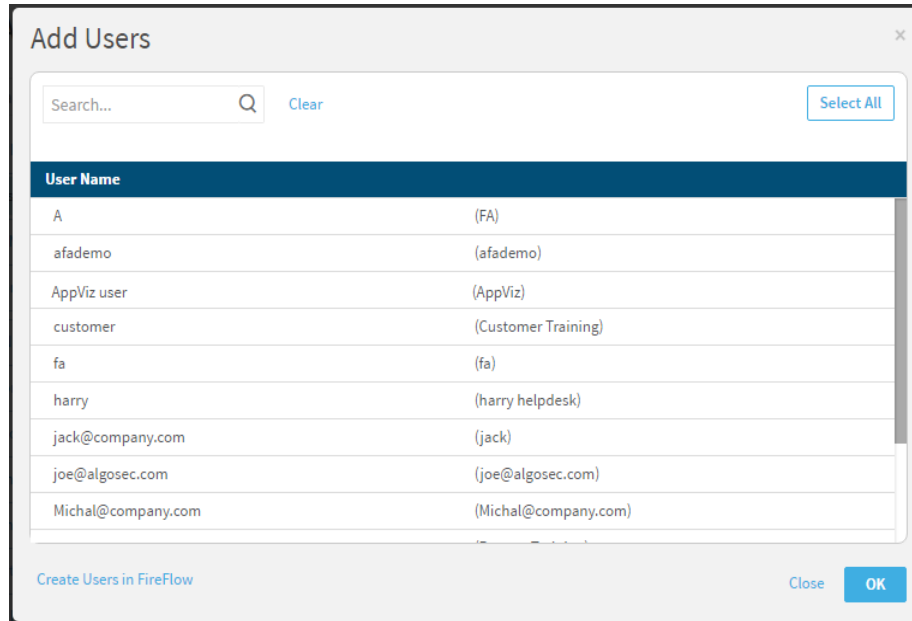
- ii. Select an application from the list.

The **Authorized Roles and Users** area for the selected application appears on the right.

Note: A role or user will appear disabled in the list for one of the following reasons: the user inherited permission to the application from a role, or the user or role has **User has edit all applications permission**.

4. To give single users permission to view or edit the application, do the following:
 - a. Click **+Add Users**.

The Add Users window appears.



b. Do one of the following:

- Select users from the list.
- Perform a simple search for a user by entering any part of the user's name or username in the search box, and click . The matching users appear below the search box.
- To deselect users, click **Clear**.

c. Click **OK**.

Once added, the user(s) appear in a list below the application. By default they are only given permission to view the application.


d. To give the user permission to edit an application, click the **Can View** drop-down list for the application and select **Can Edit**.

5. To give all users with a specific role permission to view or edit the application, do the following:

a. Click **+Add Roles**.

The **Add Roles** window appears.

b. Do one of the following:

- Select roles from the list.
- Perform a simple search for a role by typing any part of the role's name in the search box, and clicking . The matching roles appear below the search box. Select roles from the list.
- To deselect roles, click **Clear**.

c. Click **OK**.

The role(s) appear in a list below the application. By default they are only given permission to view the application.

d. To give the role permission to edit an application, click the **Can View** drop-down list for the application and select **Can Edit**.

6. To remove the permissions of a user or role for the application, click .

7. To remove all user and role permissions for the application, click **Remove all**.

8. Click **Save Changes**.

Manage permissions for users

You can manage permissions for users in two ways:

- You can grant permissions to individual users. This gives users permission to view or edit an application that they do not have permission for by default.
- You can assign users a role; consequently, the users with the role receive all the permissions of the role.

Assign/revoke user permissions

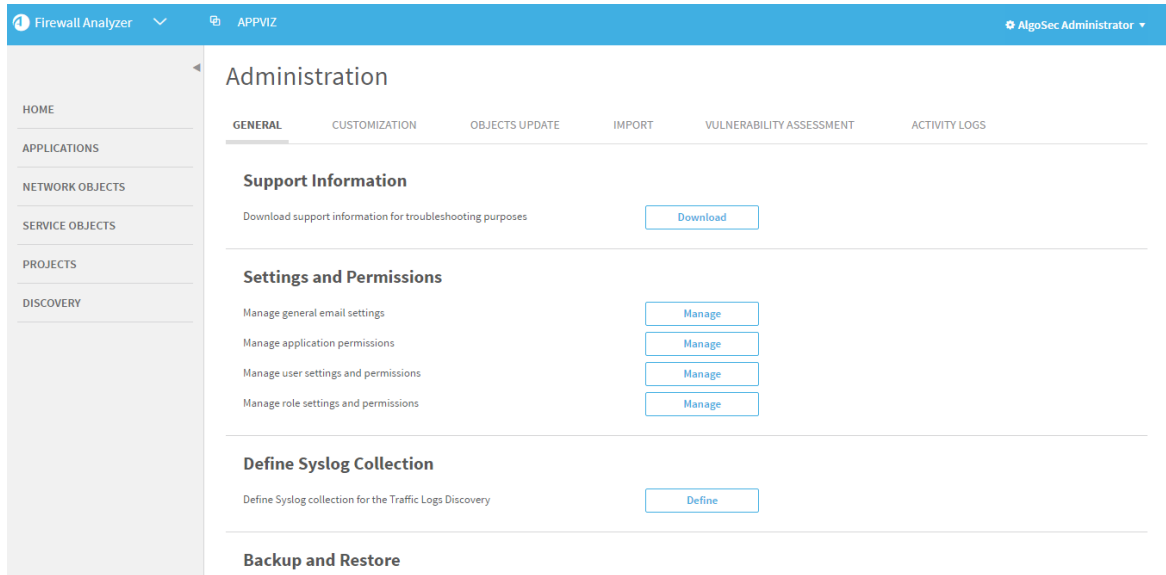
The procedure below describes how to manage application permissions for a specific user.

1. In the toolbar, click your username.

A drop-down list appears.

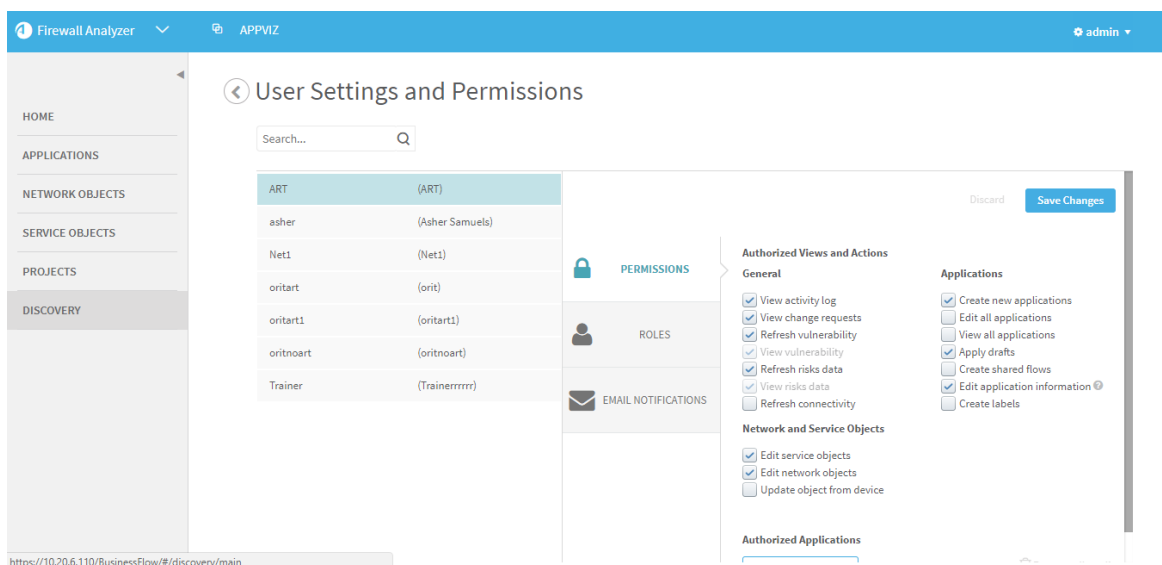
2. In the drop-down list, select **Administration**.

The administration page appears in the workspace.




3. In the **Settings and Permissions** area, next to **Manage user settings and permissions**, click **Manage**.

The **User Settings and Permission** page appears.



4. Do one of the following:

- Select a user from the list.
- Perform a simple search for a user by doing the following:
 1. Type any part of the user's name or username in the search box, and click  .


The matching users appear below the search box.

2. Select a user from the list.

The information for the selected user appears on the right.

5. In the **Authorized Views and Actions** area, edit the permissions given to the user as needed. For details, see [Authorized views and actions fields](#).
6. To give the user permission to view or edit an application, do the following:
 - a. In the **Authorized Applications** area, click **+Add Applications**.
The **Add Applications** wizard appears.
 - b. Select applications using the information in [Use the Add Applications wizard](#).

The selected application(s) appear in a list below the user. By default the user is given permission to view the application.

- c. To give the role permission to edit an application, click the **Can View** drop-down list for the application and select **Can Edit**.
7. To revoke the user's permissions to an application, click .
8. To revoke the user's permissions for all applications, click **Remove all applications**.
9. Click **Save Changes**.

Authorized views and actions fields

In this field...	Do this...
General	
View activity log	Select this check box to give the user permission to view the activity log tab of applications and network objects.
View change requests	Select this check box to give the user permission to view the change requests tab of applications, network objects, and service objects.
Refresh vulnerability	Select this check box to give the user permission to update the vulnerability assessment of network objects. All users with permission to update the vulnerability assessment have permission to view vulnerability , as well.
View vulnerability	Select this check box to give the user permission to view the vulnerability tab of applications.
Refresh risks data	Select this check box to give user permission to refresh risks data.
View risks data	Select this check box to give user permission to view risks data.

In this field...	Do this...
Refresh connectivity	Select this check box to give the user permission to update the connectivity of applications.
Applications	
Create new applications	Select this check box to give user permission to create new applications.
Edit all applications	Select this check box to give user permission to edit all applications. All users with permission to edit all applications automatically have the View all applications permission and the Edit application information permission .
View all applications	Select this check box to give user permission to view all applications.
Apply drafts	Select this check box to give the user permission to apply drafts to applications. Note: If a user has this permission, they will only be able to apply drafts to applications they have permission to edit.
Create shared flows	Select this check box to give user permission to create shared traffic flows.
Edit application information	Select this check box to give user permission to edit application custom fields, labels, and contacts.
Create labels	Select this check box to give user permission to create user-defined application labels.
Network and Service Objects	
Edit service objects	Select this check box to give user permission to edit service objects.

In this field...	Do this...
Edit network objects	Select this check box to give user permission to edit network objects.
Update object from device	Select this check box to give the user permission to synchronize a device object's definition in AppViz with the definition on the device.

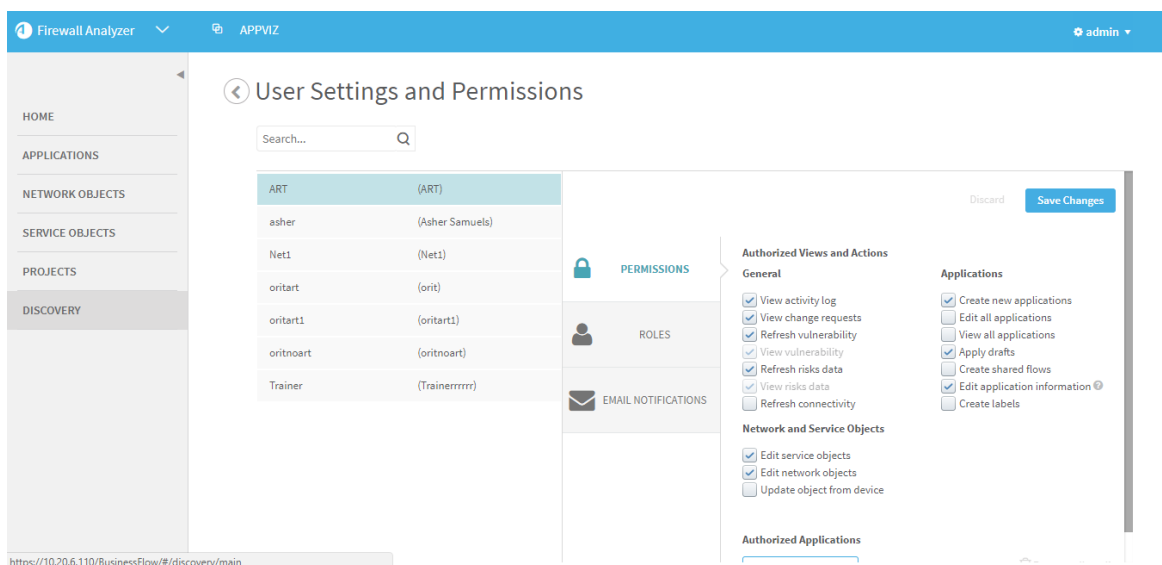
Assign / revoke user roles

You can manage user permissions by assigning roles to users. All users with a specific role receive all of the permissions assigned to the role. The procedure below describes how to assign and revoke roles.


Note: When fetching data from an LDAP server, you cannot manually assign/revoke roles. You must map roles using the LDAP Group DN. For details, see [Map LDAP groups to roles](#).

To assign/revoke user roles:

1. In the toolbar, click your username.
A drop-down list appears.
2. In the drop-down list, select **Administration**.
The administration page appears in the workspace.
3. In the **Settings and Permissions** area, next to **Manage user settings and permissions**, click **Manage**.
The **User Permission** page appears.



4. Do one of the following:

- Select a user from the list.
- Perform a simple search for a user by doing the following:
 1. Type any part of the user's name or username in the search box, and click .

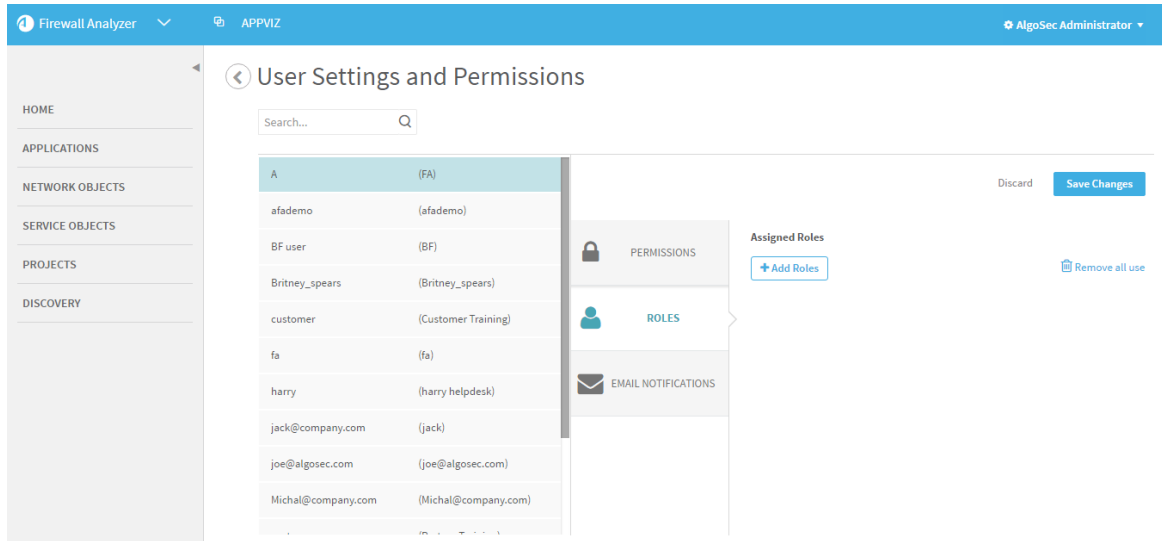
The matching users appear below the search box.

2. Select a user from the list.

The information for the selected user appears on the right.

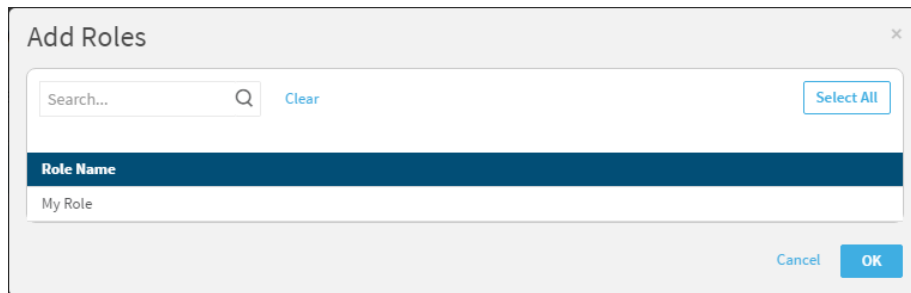
5. Click the **Roles** tab.


The **Assigned Roles** area appears.



6. Edit the roles given to the user, by doing the following:
 - a. In the **Assigned Roles** area, click **+Add Roles**.


The **Add Roles** window appears.



- b. Do one of the following:
 - Select roles from the list.
 - Perform a simple search for a role by doing the following:
 1. Type any part of the role's name in the search box, and click .
 - The matching roles appear below the search box.
 2. Select roles from the list.
 - c. To deselect roles, click **Clear**.

d. Click **OK**.

The roles appear in the Assigned Roles list.

7. To remove the revoke the role from the user, click  .
8. To revoke all of the user's roles, click **Remove all users**.
9. Click **Save Changes**.

Manage user roles

Do any of the following:

- [Assign/Revoke role permissions](#)
- [Add users to roles](#)
- [Create new roles](#)
- [Delete a role](#)
- [Map LDAP groups to roles](#)

Assign/Revoke role permissions

You can give roles permission to view or edit specific applications. Users assigned a role inherit all permissions granted to the role. The procedure below describes how to manage application permissions for roles.

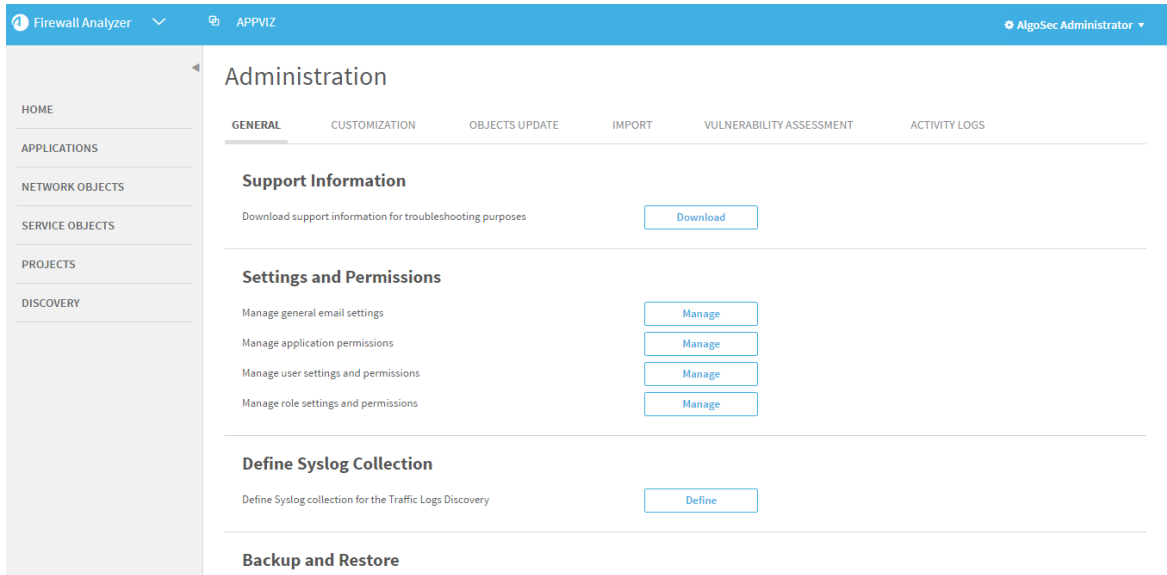
To assign/revoke role permissions:

1. In the toolbar, click your username.

A drop-down list appears.

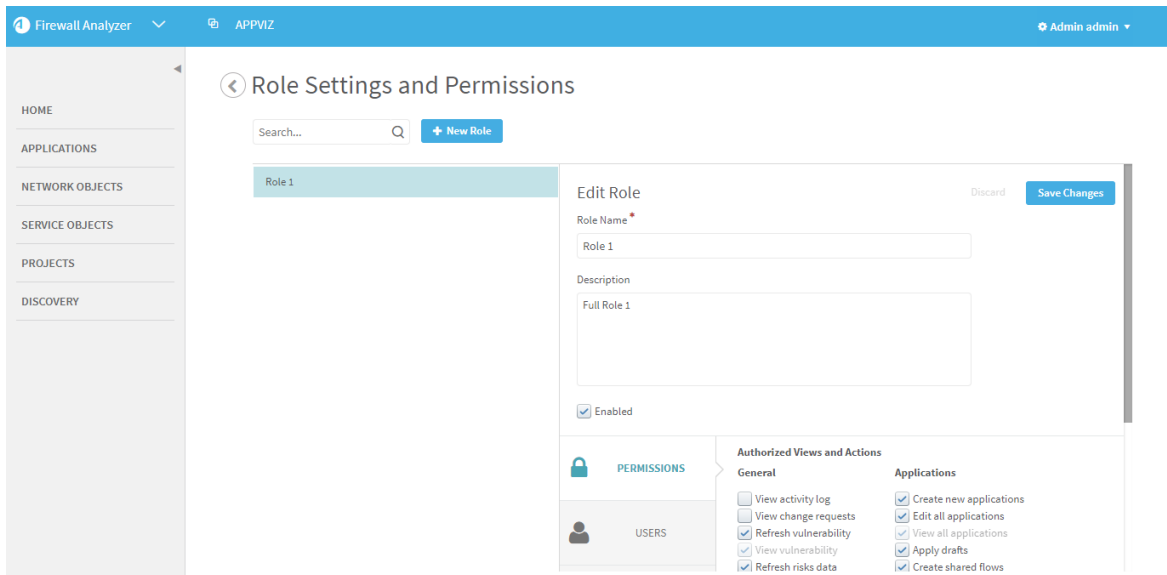
2. In the drop-down list, select **Administration**.

The administration page appears in the workspace.




- In the **Settings and Permissions** area, next to **Manage role settings and permissions**, click **Manage**.

The **Role Settings and Permissions** page appears.



4. Do one of the following:

- Select a role from the list.
- Perform a simple search for a role by doing the following:
 1. Type any part of the role's name in the search box, and click  .

The matching roles appear below the search box.

2. Select a role from the list.

The information for the selected role appears on the right.

5. In the **Authorized Views and Actions** area, edit the permissions given to the role.

For details, see [Authorized views and actions fields](#).

6. To give the role permission to view or edit an application, do the following:

- a. In the **Authorized Applications** area, click **+Add Applications**.

The **Add Applications** wizard appears.

- b. Select applications using the information in [Use the Add Applications wizard](#).

The selected applications appear in a list. By default, the role is given permission to view the applications.

- c. To give the role permission to edit an application, click the **Can View** drop-down list for the application and select **Can Edit**.

7. To revoke the role's permissions to an application, click  .

8. To revoke the user's permissions for all applications, click **Remove all applications**.

9. Click **Save Changes**.

Add users to roles

To add users to a role:

1. In the toolbar, click your username.

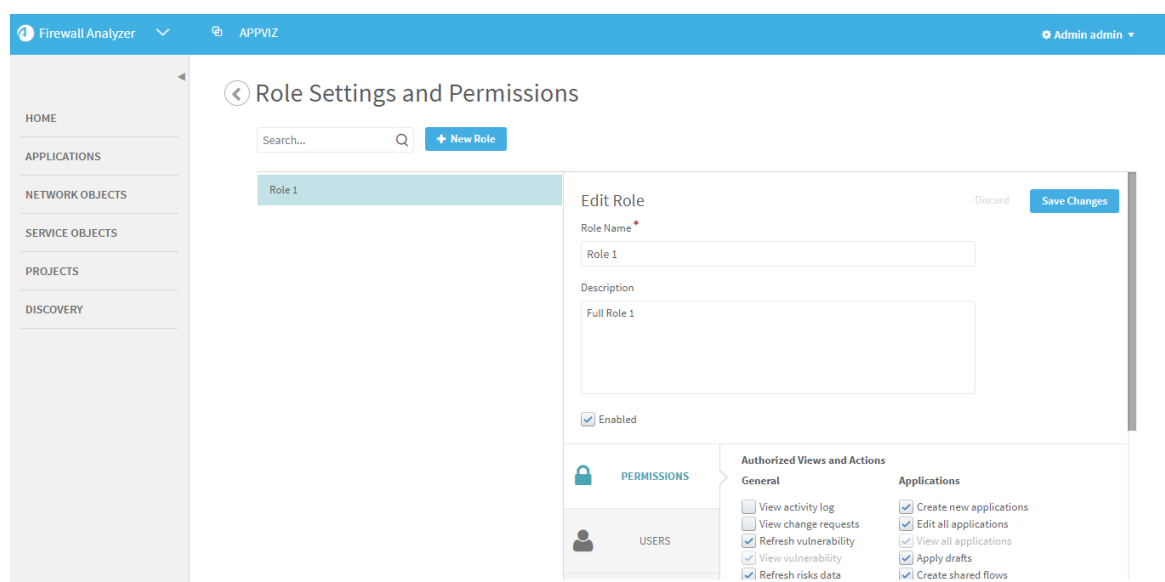
A drop-down list appears.

2. In the drop-down list, select **Administration**.


The administration page appears in the workspace.

3. In the **Settings and Permissions** area, next to **Manage role settings and permissions**, click **Manage**.

The **Role Settings and Permission** page appears.



4. Do one of the following:

- Select a role from the list.
- Perform a simple search for a role by doing the following:
 1. Type any part of the role's name in the search box, and click .

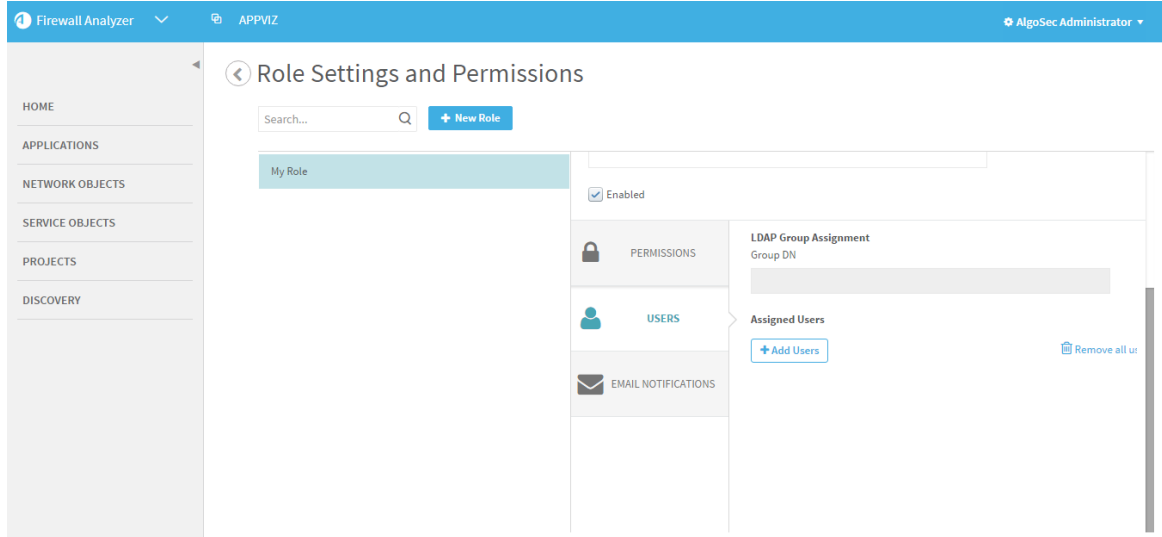
The matching roles appear below the search box.

2. Select a role from the list.

The information for the selected role appears on the right.

5. Click the **Users** tab.

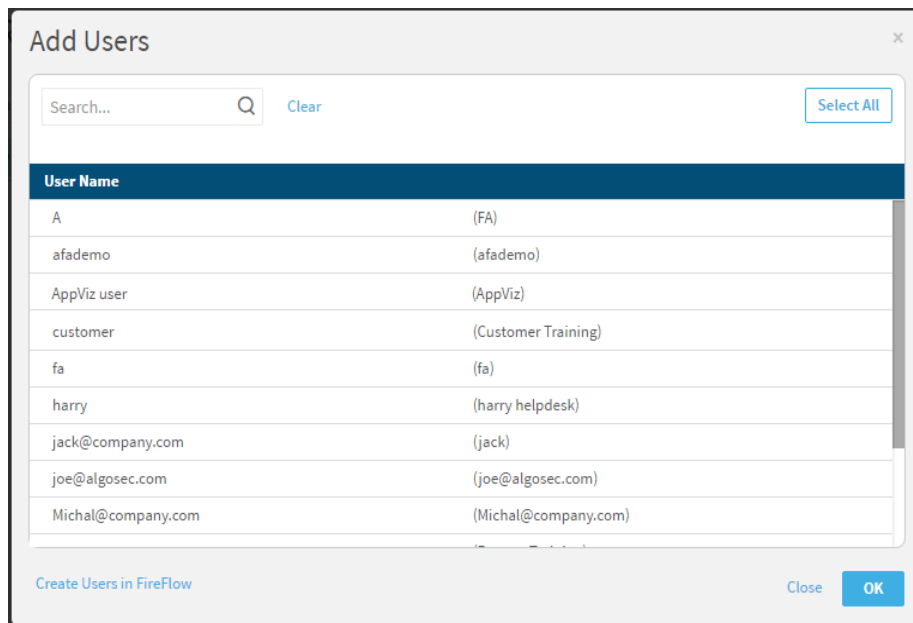
The **Users** tab appears.




6. Edit the users assigned the role, by doing the following:

- a. In the **Assigned Users** area, click **+Add Users**.

The **Add Users** wizard opens.



b. Do one of the following:

- Select users from the list.
- Perform a simple search for a user by doing the following:
 1. Type any part of the user's name or username in the search box, and click .

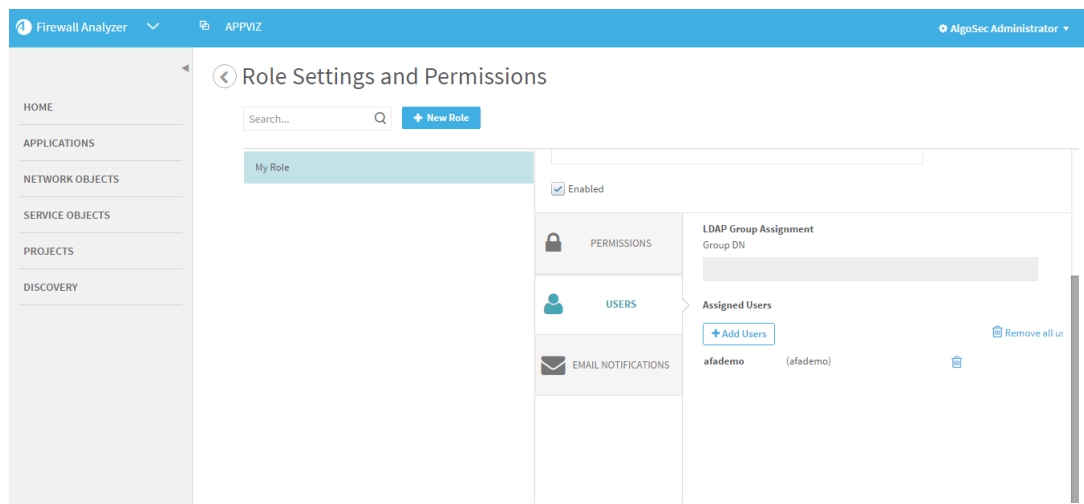
The matching users appear below the search box.


2. Select users from the list.

c. To deselect users, click **Clear**.

d. Click **OK**.

The user(s) appear in the **Assigned Users** area.



7. To revoke the role from the user, click .
8. To revoke all of the role's users, click **Remove all users**.
9. Click **Save Changes**.

Create new roles

To create a new role:

1. In the toolbar, click your username.

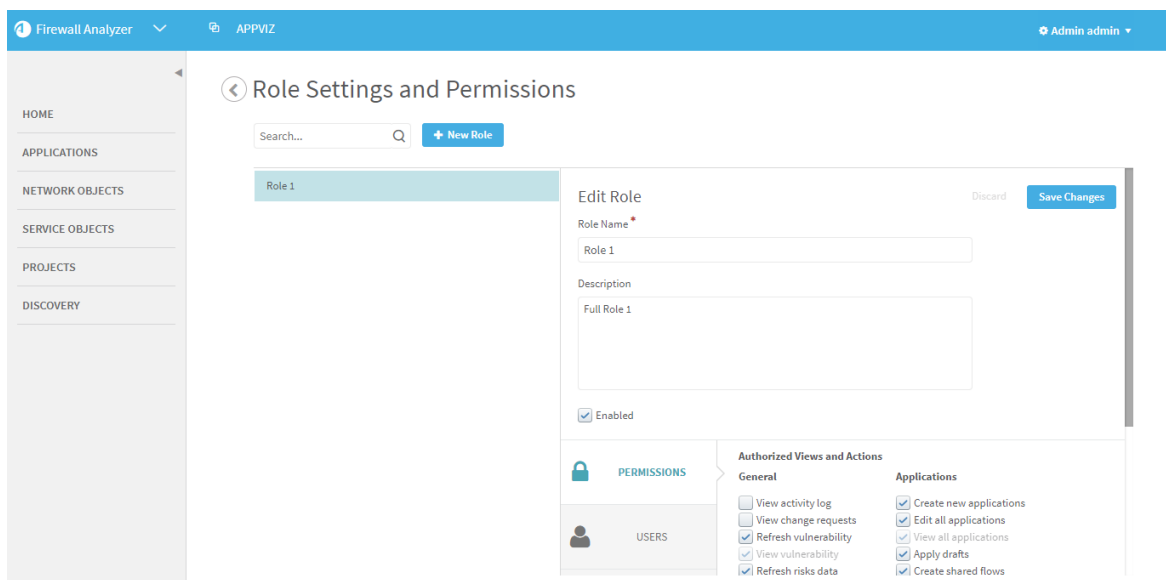
A drop-down list appears.

2. In the drop-down list, select **Administration**.

The administration page appears in the workspace.

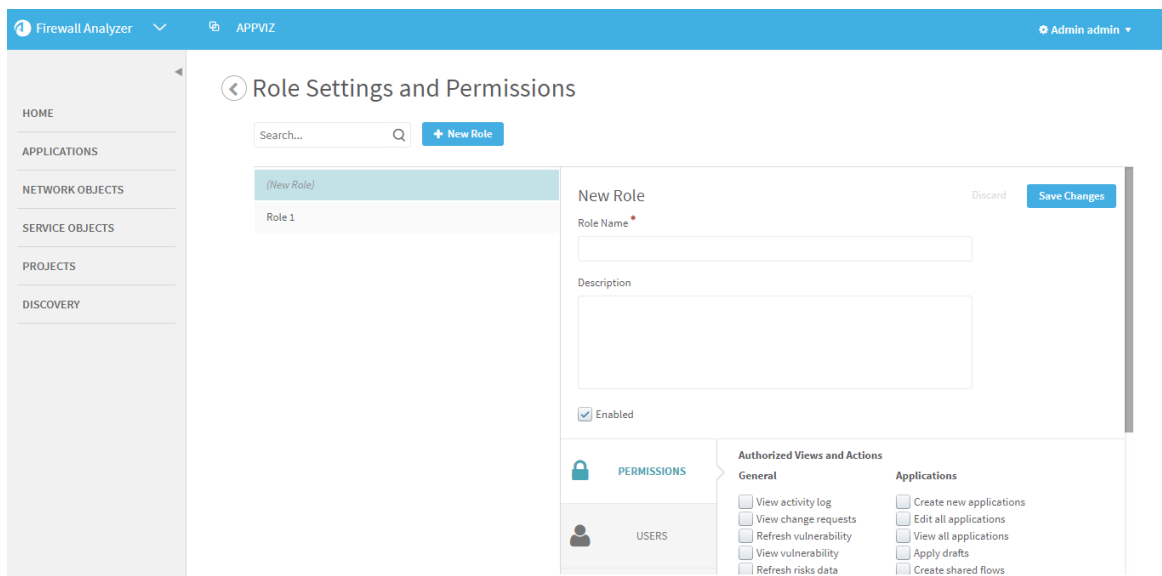
3. In the **Settings and Permissions** area, next to **Manage role settings and permissions**, click **Manage**.


The **Role Settings and Permission** page appears.



4. Click **+New Role**.

New fields appear on the right.



5. Complete the fields as needed. For details, see [New role fields](#).
6. Continue completing the fields. For details, see [Authorized views and actions fields](#).
7. To give the role permission to view or edit an application, do the following:
 - a. In the **Authorized Applications** area, click **+Add Applications**.
The **Add Applications** wizard appears.
 - b. Select applications using the information in [Use the Add Applications wizard](#).
The selected applications appear in a list. By default, the role is given permission to view the applications.
 - c. To give the role permission to edit the applications, do the following:
 - i. For the desired application, click **Can View**.
 - ii. In the drop down menu, select **Can Edit**.
8. To revoke the role's permissions to an application, click .
9. To revoke the role's permissions for all applications, click **Remove all users**.

10. Click **Save Changes**.

New role fields

In this field...	Do this...
Role Name	Type the name of the role.
Description	Type a description for the role. This field is optional.
Enabled	Default is Enabled. Clear check box to disable the role.

Map LDAP groups to roles

If you are importing user data from an LDAP server, you can map LDAP groups to AppViz roles. The user will be assigned the relevant role upon login.

Note: If your environment is configured to import user information from an LDAP server, changes to user settings must be made only on the LDAP server (changes made in the AlgoSec Suite may be overridden the next time the user logs in).

To map LDAP groups to a role:

1. In the toolbar, click your username.

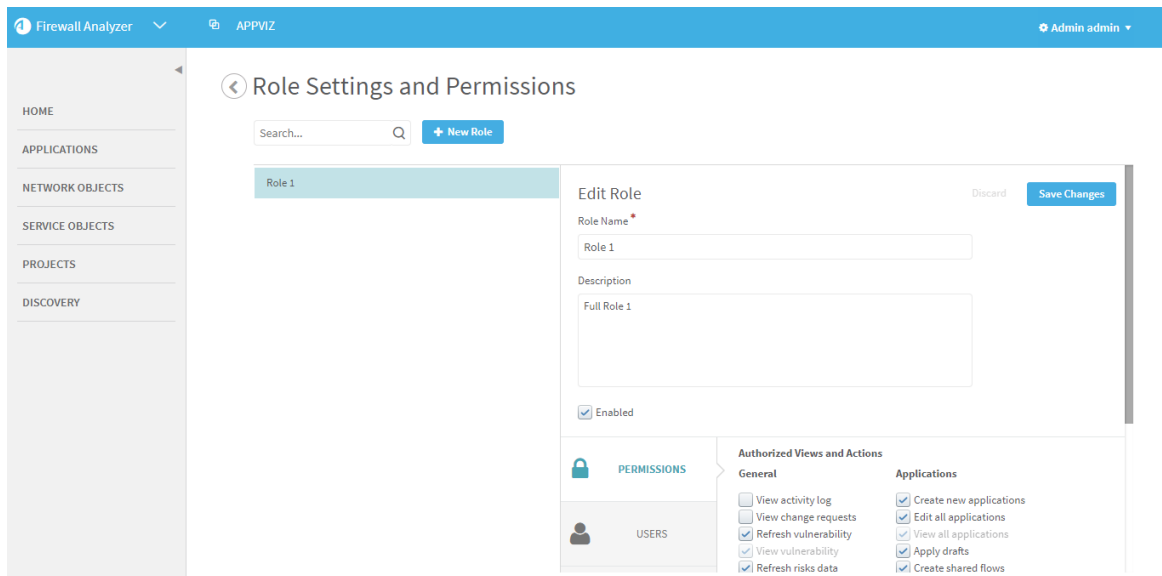
A drop-down list appears.

2. In the drop-down list, select **Administration**.


The administration page appears in the workspace.

3. In the **Settings and Permissions** area, next to **Manage role settings and permissions**, click **Manage**.

The **Role Settings and Permissions** page appears.



4. Do one of the following:

- Select a role from the list.
- Perform a simple search for a role by doing the following:
 1. Type any part of the role's name in the search box, and click  .

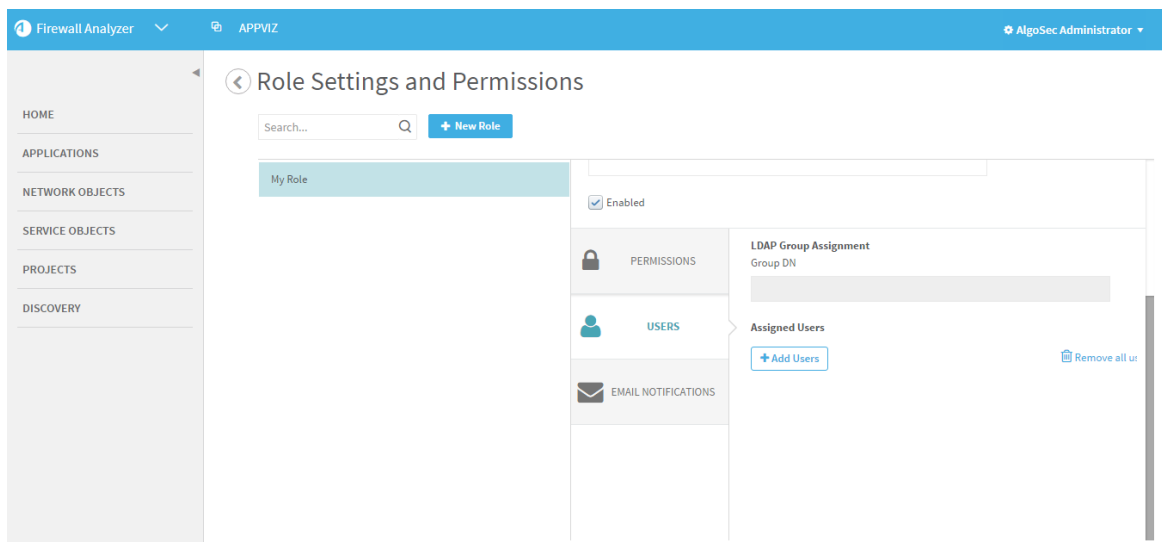
The matching roles appear below the search box.

2. Select a role from the list.

The **Edit Role** area for the selected role appears on the right.

5. Click the **Users** tab.

The **Users** tab appears.




6. In the **Group DN** field, type the LDAP group DN you wish to map to the role.

Note: This field is disabled for the Administrator role. Administrators have all roles.

7. Click **Save Changes**.

Delete a role

To delete a role:

1. In the toolbar, click your username.
A drop-down list appears.
2. In the drop-down list, select **Administration**.
The administration page appears in the workspace.
3. In the **Settings and Permissions** area, next to **Manage role settings and permissions**, click **Manage**.
The **Role Settings and Permission** page appears, with a list of all roles on the left.
4. Hover over the desired role and click .

A confirmation message appears.

5. Click **OK**.

Custom fields

AppViz supports custom fields for applications, flows, network objects, projects, and contacts.

Note: When viewing the **Flows** tab of an application, custom flow fields only appear if you display them or when you are editing a flow.

Add custom fields to flows

Do the following:

1. In the toolbar, click your username.

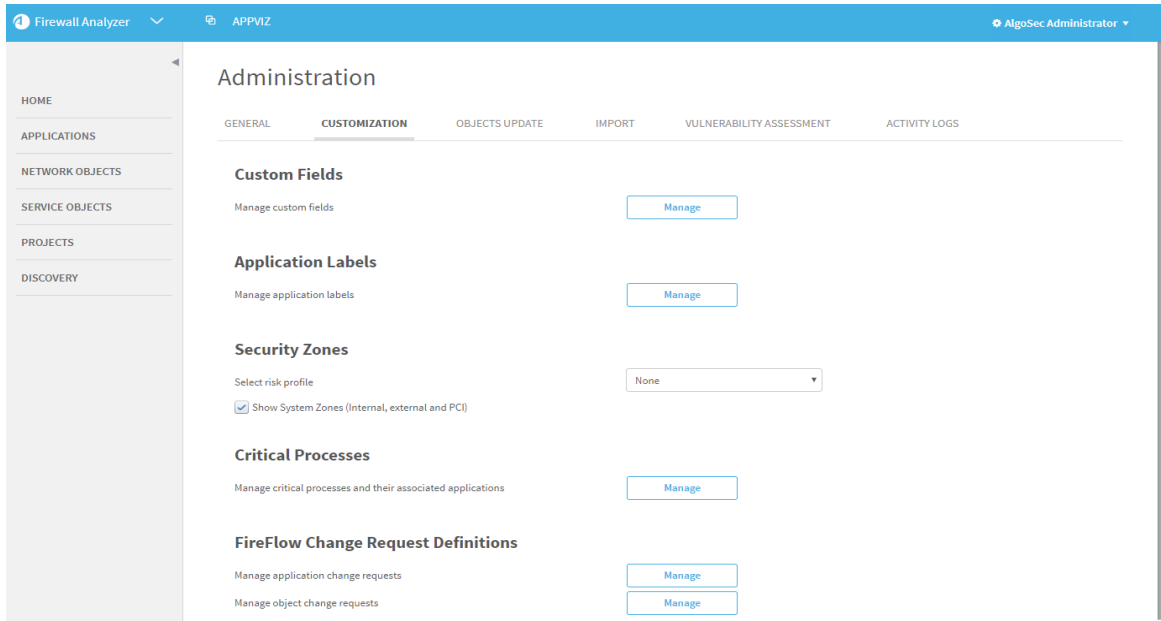
A drop-down list appears.

2. In the drop-down list, select **Administration**.

The administration page appears in the workspace.

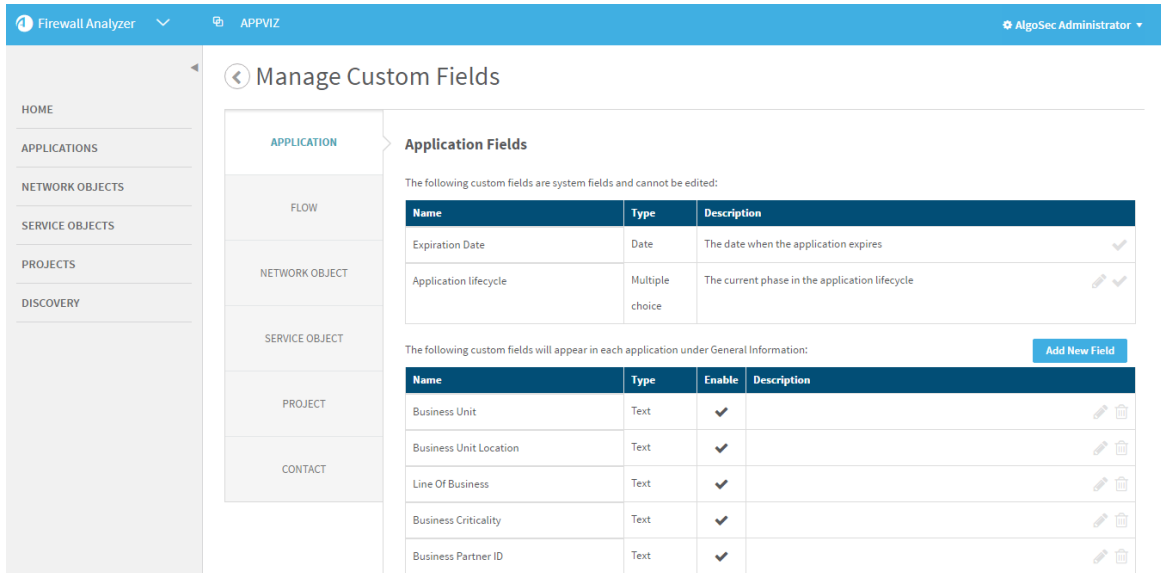
3. Click the **Customization** tab.

The **Customization** tab appears.



4. In the Custom Fields area, click **Manage**.

The **Manage Custom Fields** area appears.



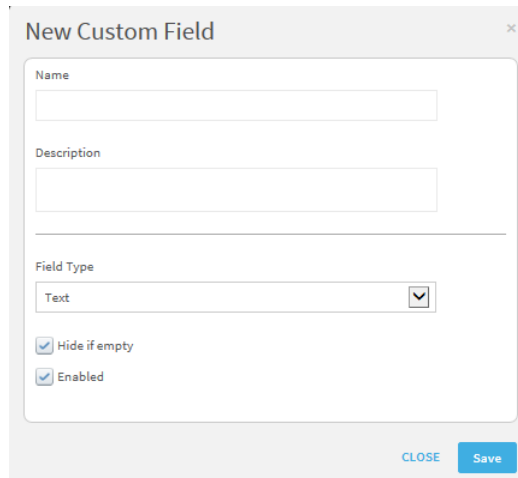
- Enabled fields are marked with ✓.
- Disabled fields are marked with ⊗.

5. In the left panel, select the information area in which the custom field appears: **Application, Flow, Object, Project, or Contact**.

6. To add a new field, do the following:

- a. Click **Add New Field**.

The New Custom Field window appears.




The screenshot shows a dialog box titled "New Custom Field" with a close button (X) in the top right corner. Inside the dialog, there are two text input fields: "Name" and "Description". Below these is a "Field Type" dropdown menu currently showing "Text". At the bottom of the form area, there are two checkboxes: "Hide if empty" and "Enabled", both of which are checked. In the bottom right corner of the dialog, there are two buttons: "CLOSE" and "Save".

- b. Complete the fields using the information in Custom Field Fields (see [Custom Field Fields](#)).

- c. Click **Save**.

7. To edit a custom field, do the following:

- a. Click .
- b. Edit the fields you desire using the information in Custom Field Fields (see [Custom Field Fields](#)).
- c. Click **Save**.

Note: When editing the **Application lifecycle** fields, you must have at least two stages, one of which must be **Decommission**.

8. To delete a custom field, do the following:

- a. Click .

A confirmation message appears.

b. Click OK.

Custom Field Fields

In this field...	Do this...
Name	Type the name of the field.
Description	Type the description of the new field.
Field Type	<p>In the Field Type list, select one of the following field types:</p> <ul style="list-style-type: none"> • Text. The field will be text. When editing the general information for an application, type the text in the text box. • Link. The field will be a link to a URL. When editing the general information for an application, type the text for the link in the text box. • Date. The field will be in date format. When editing the general information for an application, select the date from the date selection wizard. • Multiple Choice. The field will contain a list of values for the user to select. In each Values box, type a value. Click + Add Value to continue adding values. <p>When editing the general information for an application, select one value from the list.</p> <p>To change the display order of the multiple choice values, click the value and move it to its new position in the list.</p>

In this field...	Do this...
URL Template	<p>Type the URL you want the link to direct to. You can include the following variables:</p> <ul style="list-style-type: none"> • {Value}. This variable will be replaced by the link text a user types into the text box. For example, if the template is <code>domain.com/{Value}</code>, and the user types <code>Value1</code> in the text box, the link will appear with the text <code>Value1</code>, and direct you to <code>domain.com/Value1</code>. • Variable name enclosed in curly brackets depending on field usage. The variable will be replaced by the name of the current application, flow name, object name, project name, or contact name: <ul style="list-style-type: none"> • <code>{AppName}</code> • <code>{FlowName}</code> • <code>{ObjectName}</code> • <code>{ProjectName}</code> • <code>{ContactName}</code> <p>For example, if the template is <code>domain.com/{AppName}</code>, and you are viewing an application called "App1", the link will appear with the text the user types in the text box, and the link will direct you to <code>domain.com/App1</code>.</p> <p>This field only appears when the selected type is Link.</p>
Hide if empty	If you do not want the field to appear if empty, select the Hide if empty check box. Clear the check box to display the field if empty.
Enabled	If you want the field to be enabled after creation, select the Enabled check box. Clear the check box to disable the field.

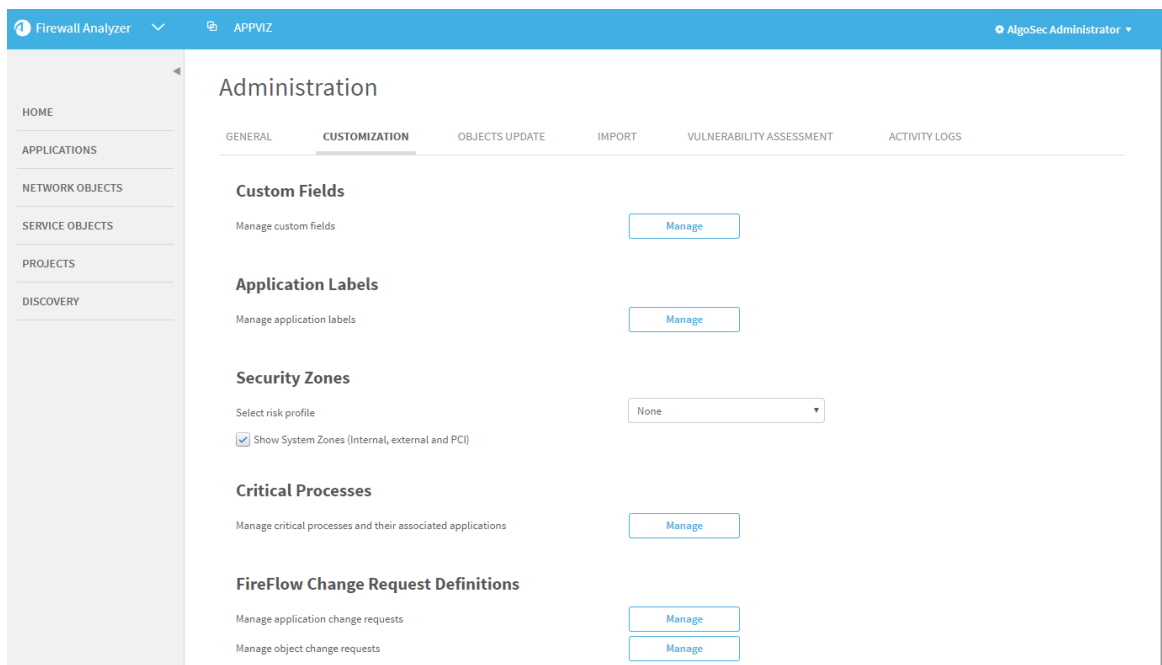
Security zones

Security zone configurations in AppViz define the zones used to group objects in application diagrams.

By default, AppViz uses system zones (as defined below). When custom risk profile spreadsheets exist in AFA, AppViz additionally uses the zone definitions in the first profile in the alphabetically ordered list.

Define security zones

1. In the toolbar, click your username.
A drop-down list appears.
2. In the drop-down list, select **Administration**.
3. Click the **Customization** tab.



4. In the **Security Zones** area, do one or both of the following:

<p>Select a custom risk profile spreadsheet in the drop-down menu.</p>	<p>Application diagrams will define zones according to the definitions in the spreadsheet. All spreadsheets defined in AFA appear.</p>
--	--

<p>Select / deselect the Show System Zones check box.</p>	<p>Application diagrams will define zones according system zones, including PCI, internal, and external.</p> <ul style="list-style-type: none"> • The PCI zone will appear according to its definition in AFA. • The private (internal) zone is defined as 10.0.0.0/8, 172.16.0.0/12, and 92.168.0.0/16 by default. To edit the private zone, see Configure the Internal zone. • The external zone is defined as all IP addresses not included in another zone.
--	--

Configure the Internal zone

By default, AppViz defines the Internal / Private zone as 10.0.0.0/8, 172.16.0.0/12, and 92.168.0.0/16. If desired, you can customize this.

To configure the Internal zone

1. Open a terminal and log in using the username "bflow" and the related password.
2. Open `/home/bflow/config/user.properties`.
3. On a new line, add the configuration item `security_zones.default_internal_network_ranges`.
4. Set the value to a semi-colon delimited list of networks in CIDR format


For example, the following sets the internal zone to 172.16.0.0/12 and 92.168.0.0/16:

```
security_zones.default_internal_network_ranges=172.16.0.0/12;92.168.0.0/16
```

5. Save the file.
6. Restart AppViz.

Critical processes

AppViz critical processes are groups of applications that support a crucial business function. Defining Critical Processes allows you to schedule connectivity and risk checks for the applications which matter most. Additionally, all applications which are a part of a critical process are tagged with a system label, indicating the critical process to which the application belongs.

 **Defining Critical Processes:** Watch to learn how to define specific application flows as critical processes.

Critical Process scope

AppViz supports defining up to 20 applications as a part of Critical Processes, in any of the following configurations:

- 20 Critical Processes with one application each
- One Critical Process with 20 applications
- Any other combination which does not exceed 20 applications

Each application may only be added to a single Critical Process.

Note: Vulnerability checks are run on the entire environment and not per application, and therefore are not specific to Critical Processes.

For details, see [Manage vulnerability assessment scanners](#).

Supported label actions

Possible label actions are:

- **Add.** Create a new Critical Process, assign it one or more applications, and schedule its connectivity and risk checks. For details, see [Add a new critical process](#)
- **Edit.** Modify the Critical Process. For details, see [Edit a critical process](#).

- **Delete.** Delete a Critical Process from the system and all its applications and scheduled checks. For details, see [Delete a critical process](#).
- **Export.** Export a CSV file of all the Critical Processes in the system. For details, see [Export all critical processes to CSV](#).

The change request summary for any FireFlow change request which is opened for a critical application indicates the relevant Critical Process, signifying the importance of the process the requested traffic supports. If desired, you can customize the default summary. For details, see [Customize interactions with AFA and FireFlow](#).

Add a new critical process

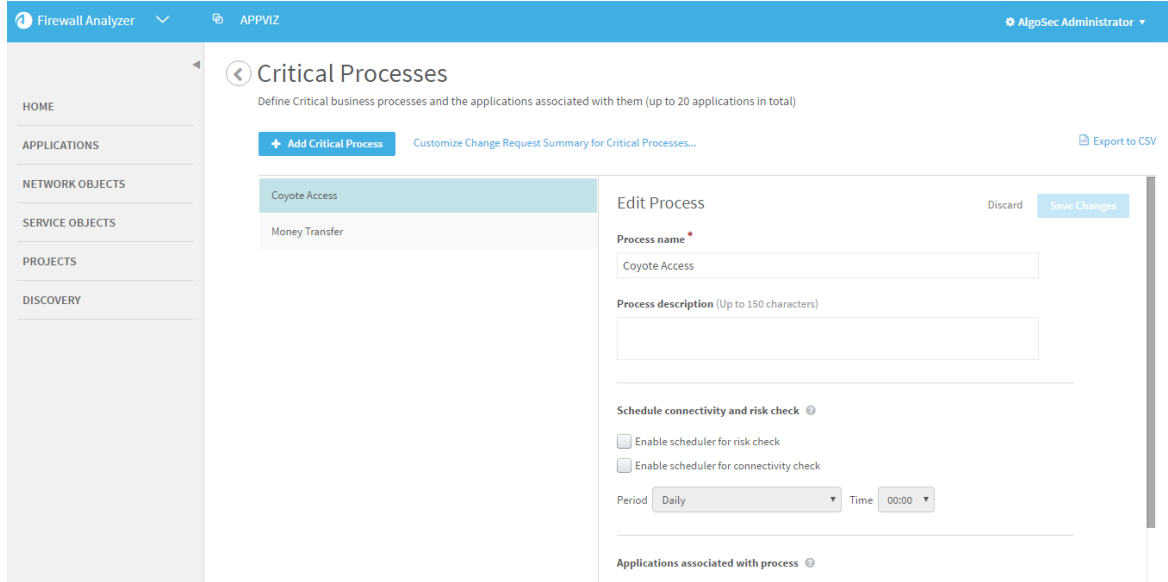
Adding a new Critical Process allows you to define a group of applications that are necessary for a crucial business function. The following occurs for all applications defined as a part of a Critical Process:

- The connectivity and risk checks scheduled for the Critical Process run on the applications' Active revisions.
- Each application is tagged with the Critical Process's system label, which appears in the applications' **Dashboard** tab.
- Any change request opened for the application is created with the default summary for critical applications. For details, see [Customize interactions with AFA and FireFlow](#).

To add a Critical Process:

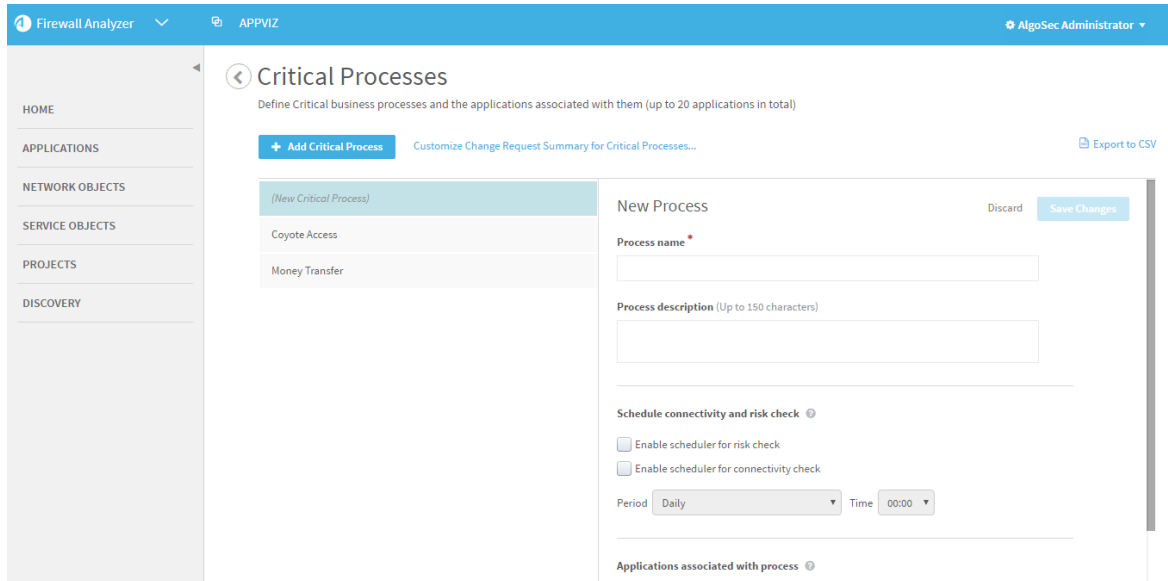
1. In the toolbar, click your username.
A drop-down list appears.
2. In the drop-down list, select **Administration**.
3. Click the **Customization** tab.
4. In the **Critical Processes** area, click **Manage**.

The **Critical Processes** page appears.



5. Click .

The **New Process** area appears.



6. Complete the fields using the information in Critical Process Fields (see [Critical process fields](#)).


Note: If desired, you can customize the default summary for all FireFlow change requests created for an application that is a part of a Critical Process. Click the **Customize Change Request Summary for Critical Processes...** link. For details, see [Customize interactions with AFA and FireFlow](#).

7. Click **Save Changes**.

The Critical Process is created.

Critical process fields

In this field...	Do this...
Process name	Type a name for the process. Each process must have a unique name.
Process description	Type a description of the process.
Schedule connectivity and risk check	Note: The checks are performed on each application's active revision.
Enable scheduler for risk check	Select this check box to enable risk checks performed at the times you specify.
Enable scheduler for connectivity check	Select this check box to enable connectivity checks performed at the times you specify.
Period	Select the frequency to perform checks in the drop-down menu.
Day	If the selected period is weekly, select the day of the week to perform the checks in the drop-down menu.
Time	Select the time of day to perform the checks in the drop-down menu.
Applications associated with process	

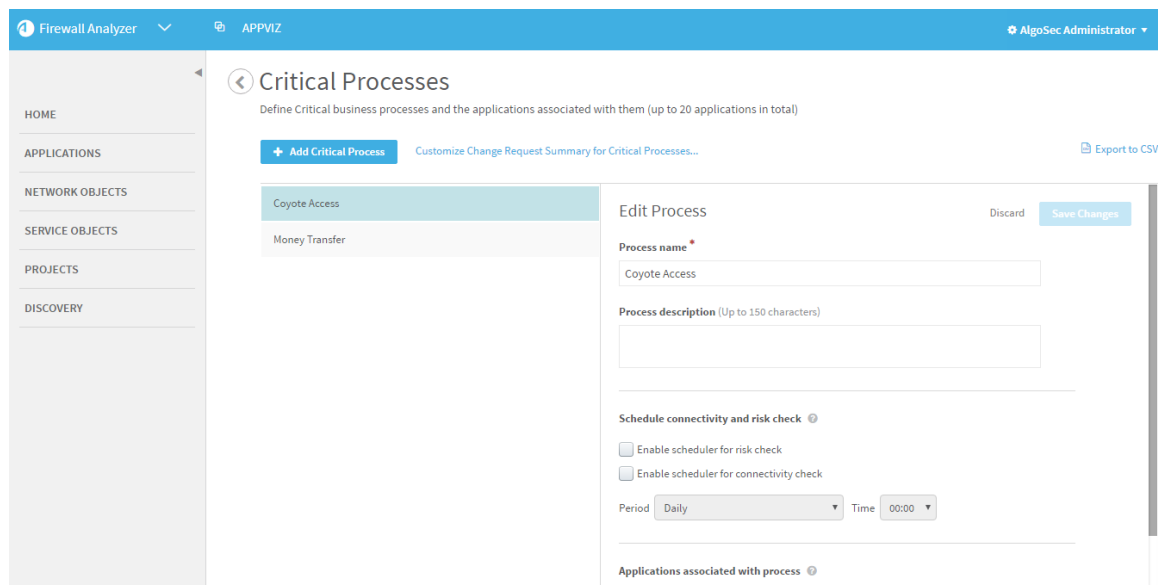
In this field...	Do this...
+ Add Applications	Click this icon to add an application to the Critical Process. For details, see Create an application migration project .
	To remove an application from the process, click this icon next to the desired application.
Remove all	Click this link to remove all the applications associated with the Critical Process.

Edit a critical process

To edit a Critical Process:

1. In the toolbar, click your username.
A drop-down list appears.
2. In the drop-down list, select **Administration**.
3. Click the **Customization** tab.
4. In the **Critical Processes** area, click **Manage**.

The **Critical Processes** page appears, with a list of all Critical Processes on the left.



5. Select the desired Critical Process.

The process's information appears on the right.

6. Edit the fields as needed. For details, see [Critical process fields](#).

Note: If desired, you can customize the default summary for all FireFlow change requests created for an application that is a part of a Critical Process. Click the **Customize Change Request Summary for Critical Processes...** link. For details, see [Customize interactions with AFA and FireFlow](#).

7. Click **Save Changes**.

The Critical Process is saved with the modifications you specified.

Delete a critical process

To delete a Critical Process:

1. In the toolbar, click your username.

A drop-down list appears.

2. In the drop-down list, select **Administration**.

3. Click the **Customization** tab.

4. In the **Critical Processes** area, click **Manage**.

The **Critical Processes** page appears, with a list of all Critical Processes on the left.


5. Hover over the desired Critical Process, and click  .

A confirmation message appears.

6. Click **OK**.


Export all critical processes to CSV

To export all Critical Processes:

1. In the toolbar, click your username.
A drop-down list appears.
2. In the drop-down list, select **Administration**.
3. Click the **Customization** tab.
4. In the **Critical Processes** area, click **Manage**.
The **Critical Processes** page appears.
5. Click  [Export to CSV](#).

Configure applications

This topic describes how AppViz administrators can configure AppViz applications.

 [Decommission an Application](#): Watch to learn how decommission a AppViz application.


Manage application expiration

You may set applications to expire on a particular day and notify all users when the expiration will take place using:

- Email notifications: Additional notifications may be different number of days before expiration than first notification.
- GUI Alerts
- Advance notification - 'Expires in 2 days' is displayed on Dashboard if application is expiring in 2 days.

EXPIRES IN  DAYS

- Notice on day of expiration.



- Alert in Activity Log on day of expiration.

To manage application expiration:

1. Enable expiration date field in applications. See [Enabling Application Expiration](#) (see [Enable application expiration](#)).
2. Set the desired email notifications.

To set default or custom notification settings for all users and applications, or for a specific user (for administrators, only), see [AppViz users, permissions, and roles](#).

Verify that **Application expiration** is selected in the Application Events section, otherwise only notification will be in Activity Log on day of expiration.

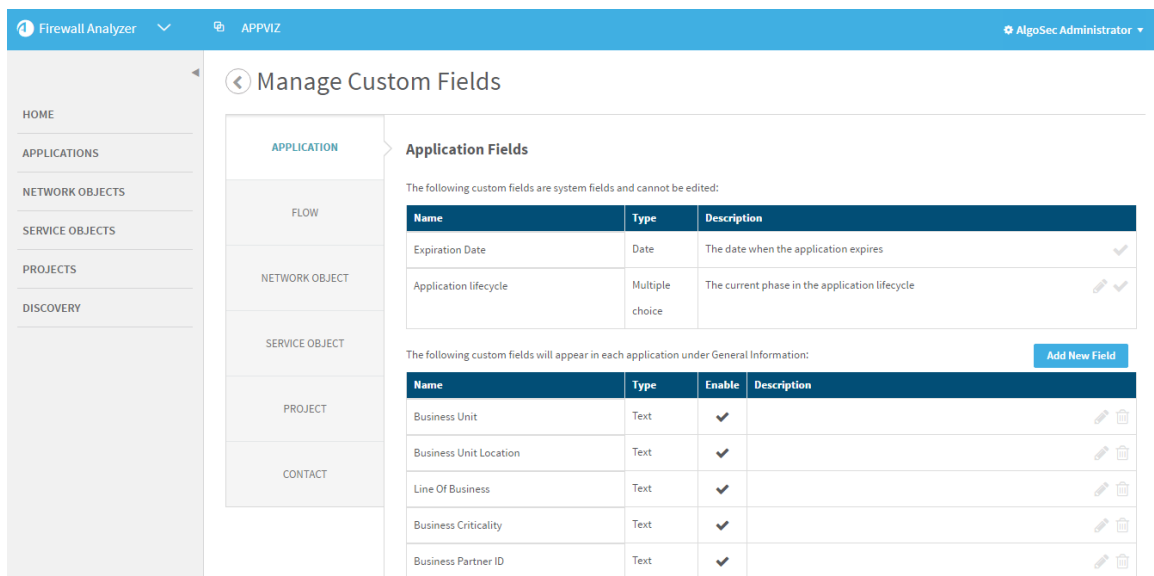
Enable application expiration

The expiration date field is an optional system field. When enabled, the field appears in application screens along. If an application is set to expire within a short time, alerts are presented on relevant screens.

To enable application expirations:

1. Log into AppViz as an administrator.
2. In the toolbar, click your username.
A drop-down list appears.
3. In the drop-down list, select **Administration**.
Click the **Customization** tab.
4. Next to **Custom Fields**, click **Manage**.

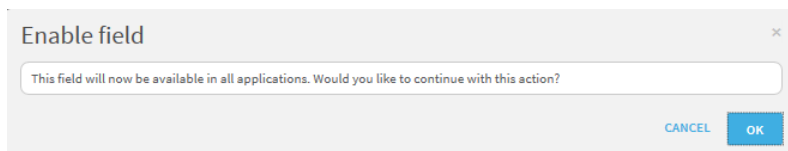
The **Manage Custom Fields** page appears with the **Application fields** area open.



- Enabled fields are marked with ✓.
- Disabled fields are marked with ✕.

5. To enable the **Expiration Date** field, on the right side, click ✕.

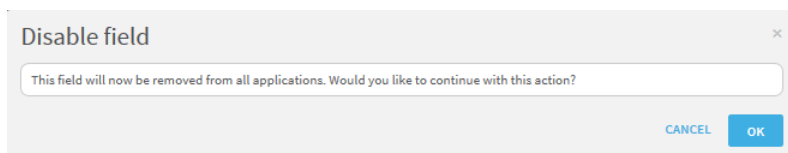
The Enable field confirmation dialog box appears.



a. Click **OK** to enable.

6. To disable the field and remove it from all applications, click ✓.

The Disable field confirmation dialog box appears.



a. Click **OK** to disable.

Manage application labels

AppViz provides two different types of application labels:

- **User-defined labels.** Basic labels that can be created and added to any application as a way of organizing applications in groups.
- **System labels.** Labels that are automatically assigned to an application as the result of a system function. Applications with system labels include critical process applications and PCI applications.

User-defined labels can be managed with the following actions:

- **Add.** Create a label and optionally assign it to one or more applications. See Adding a Label (see [Add a label](#)).
- **Edit.** Modify the name of a label and the assigned applications. See Editing a Label (see [Edit a label](#)).
- **Replace.** Replace a label (for all applications assigned to the label) with a different existing label. See Replacing a Label (see [Replace a label](#)).
- **Delete.** Delete a label from the system and all its associations with applications. See Deleting a Label (see [Delete a label](#)).

The **PCI** label can be edited by modifying the applications assigned to it. See Customizing Applications Assigned to the PCI Label (see [Customize applications assigned to the PCI label](#)).

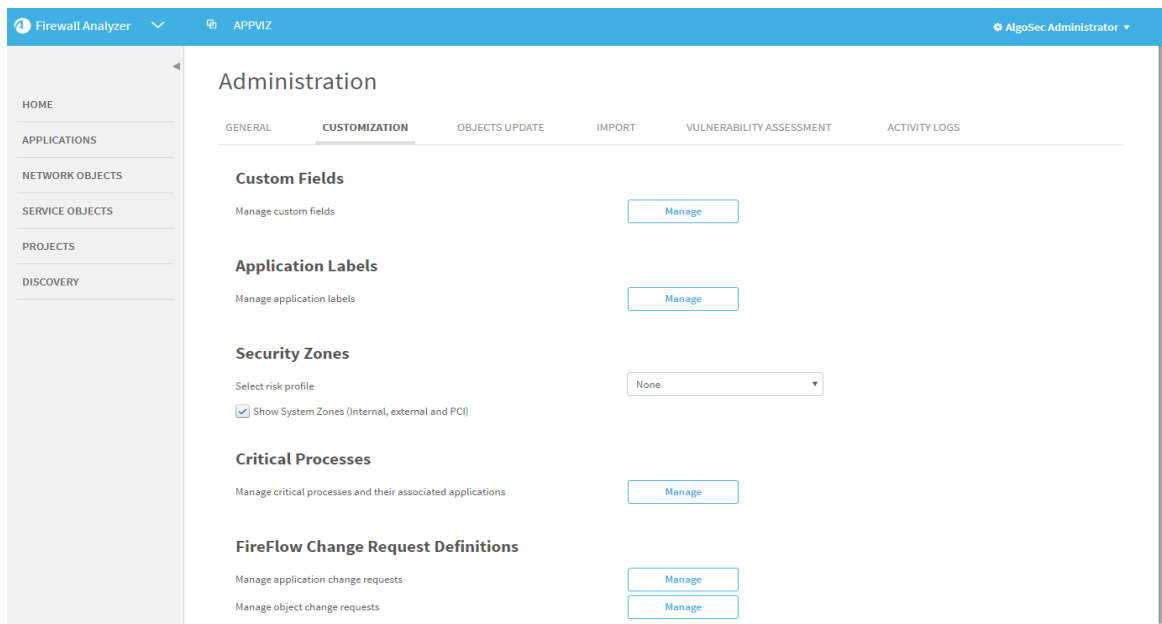
Critical Process labels are managed in the critical process manager. For details, see [Critical processes](#).

Note: Only users with administrative permission can manage application labels. In order to allow users without administrative permissions to create new labels while managing applications, see [AppViz users, permissions, and roles](#). All users can search for applications by label by performing an advanced or simple search in the **Application** area menu.

Add a label

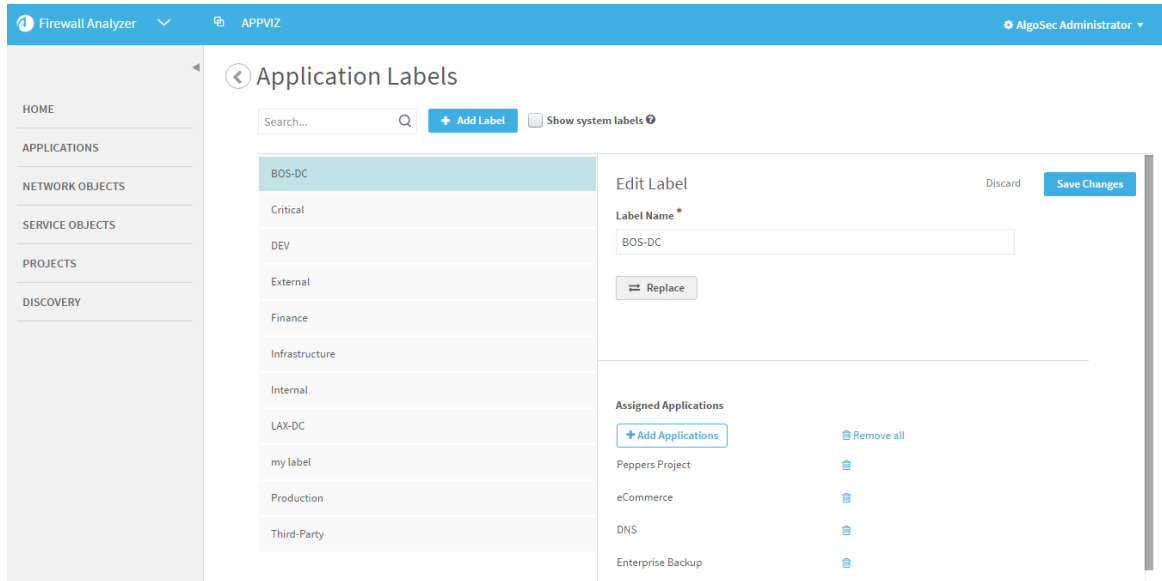
To add a label :

1. In the toolbar, click your username.
A drop-down list appears.
2. In the drop-down list, select **Administration**.
3. Click the **Customization** tab.



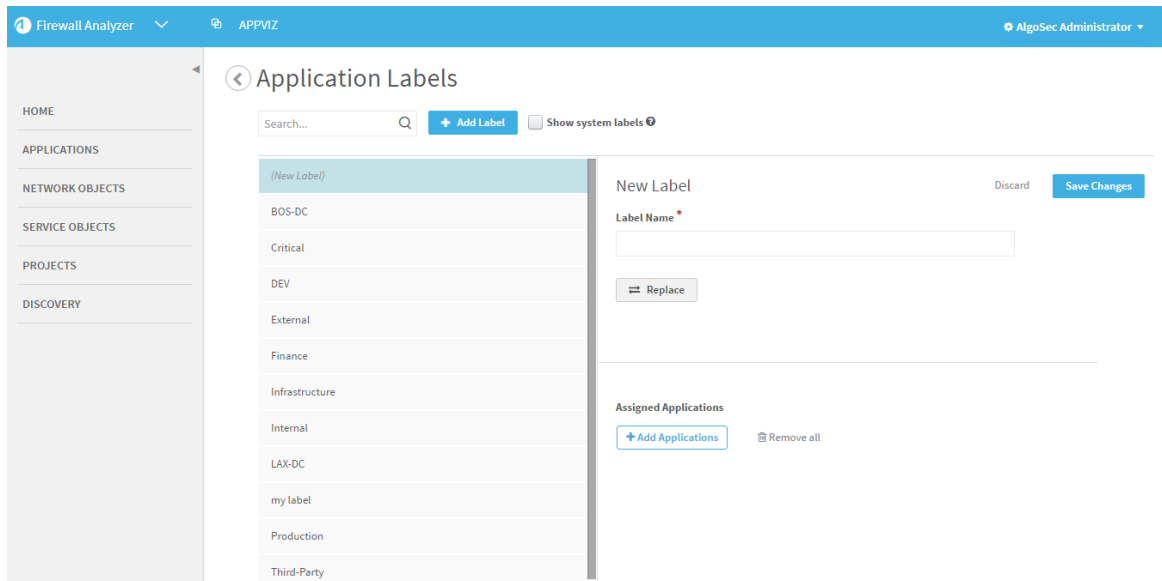
4. In the **Application Labels** area, click **Manage**.

The **Manage Application Labels** page appears.



5. Click **Add Label**.

The **New Label** area appears.



6. In the **Label Name** field, type the name of the label.


7. To assign applications to the label, do the following:

a. Click **+Add Applications**.

The **Add Applications** wizard opens.

- b. Select applications using the information in Using the Add Applications Wizard (see [Use the Add Applications wizard](#)).

The selected applications are added to the list.

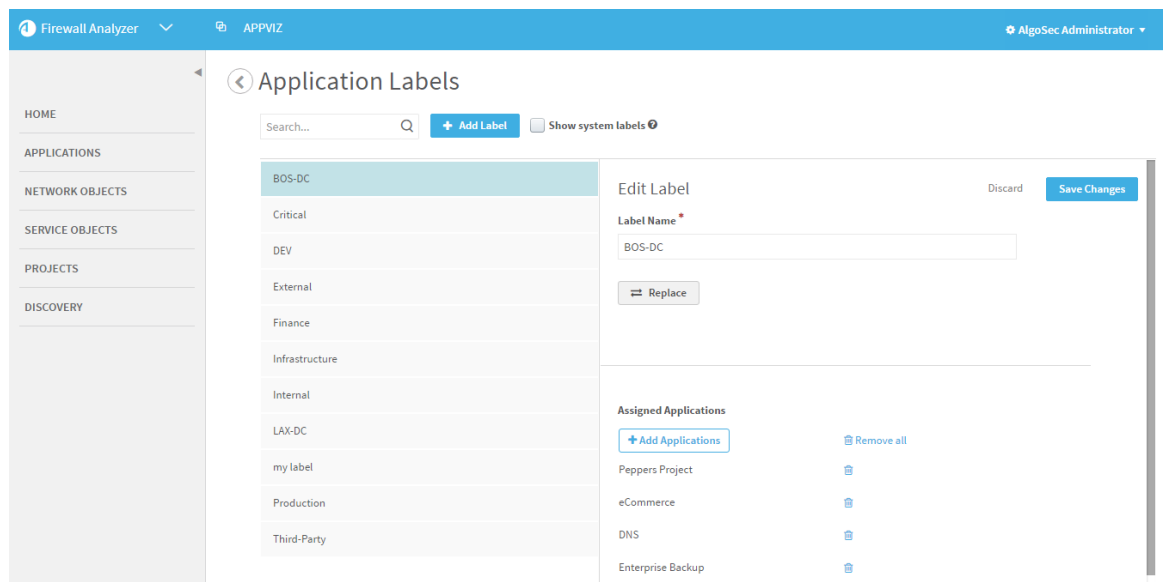
8. To revoke the label from an application, click  next to the application's name in the **Assigned Applications** area.
9. Click **Save Changes**.

Edit a label

To edit labels:


1. In the toolbar, click your username.
A drop-down list appears.
2. In the drop-down list, select **Administration**.
3. Click the **Customization** tab.
4. In the **Application labels** area, click **Manage**.

The **Manage Application Labels** page appears.



The screenshot displays the 'Application Labels' management interface. On the left is a navigation sidebar with categories like HOME, APPLICATIONS, NETWORK OBJECTS, SERVICE OBJECTS, PROJECTS, and DISCOVERY. The main content area is titled 'Application Labels' and includes a search bar, an '+ Add Label' button, and a 'Show system labels' checkbox. A table lists various labels such as BOS-DC, Critical, DEV, External, Finance, Infrastructure, Internal, LAX-DC, my label, Production, and Third-Party. To the right of this table is an 'Edit Label' form with a 'Label Name' field set to 'BOS-DC', a 'Replace' button, and 'Discard' and 'Save Changes' options. Below the form is a section for 'Assigned Applications' with an '+ Add Applications' button and a 'Remove all' link, followed by a list of applications: Peppers Project, eCommerce, DNS, and Enterprise Backup, each with a trash icon.

5. Do one of the following:

- Select the label in the list.
- Search for the desired label by doing the following:
 1. In the search box, type part of the label name.
 2. Click  .
 3. Select the label in the results list.

The label appears with its list of associated applications.

6. To edit the label's name, type the new name in the **Label Name** field.


7. To assign applications to the label, do the following:

a. Click **+Add Applications**.

The **Add Applications** wizard opens.

b. Select applications using the information in Using the Add Applications Wizard (see [Use the Add Applications wizard](#)).

The selected applications are added to the list.

8. To revoke the label from an application, click  next to the application's name in the **Assigned Applications** area.

The label is removed from the selected application *without* confirmation.

9. Click **Save Changes**.

Replace a label

To replace a label:

1. In the toolbar, click your username.

A drop-down list appears.


2. In the drop-down list, select **Administration**.

3. Click the **Customization** tab.

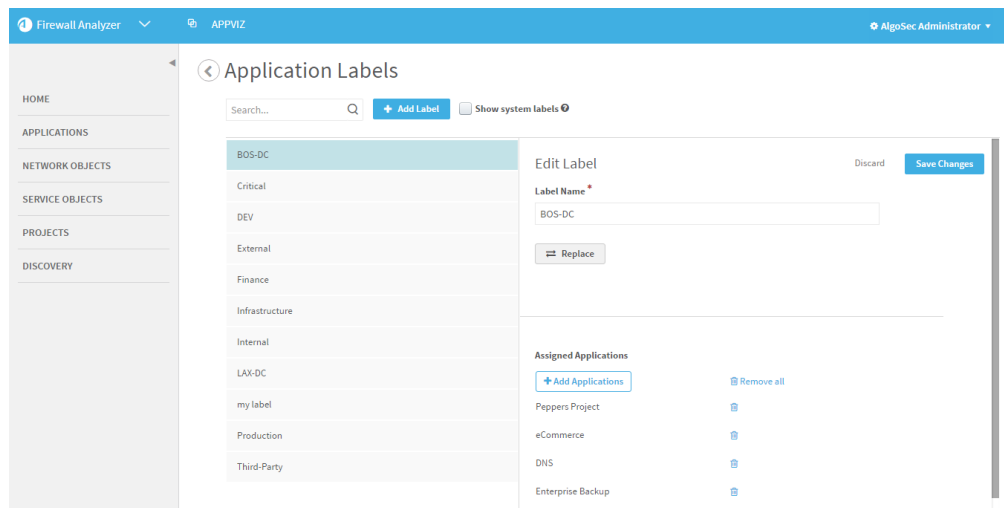
4. In the **Application labels** area, click **Manage**.

The **Manage Application Labels** page appears.

5. Do one of the following:

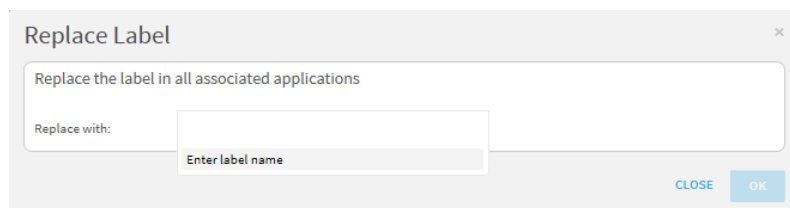
- Select the label in the list.
- Search for the desired label by doing the following:
 1. In the search box, type part of the label name.
 2. Click .
 3. Select the label in the results list.

The label appears with its list of associated applications.



6. Click .

The **Replace Label** dialog box opens.



- a. In the **Replace with** field, start typing the existing label name, and select the label from the drop-down list.
- b. Click **OK**.

The label name is replaced in each assigned application.

Delete a label

To delete a label:

1. In the toolbar, click your username.
A drop-down list appears.
2. In the drop-down list, select **Administration**.
3. Click the **Customization** tab.
4. In the **Application labels** area, click **Manage**.

The **Manage Application Labels** page appears, with a list of labels on the left.

5. In the list of labels, hover over the desired label and click  .

A confirmation message appears.

6. Click **OK**.

Customize applications assigned to the PCI label

All applications that include a network object that intersects the PCI zone are automatically assigned to the **PCI** system label. If desired, you can manually un-assign applications you do not want to be associated with the label. Un-assigning an application does nothing to affect its traffic flows; its network object(s) will still intersect the PCI zone, but the **PCI** label will not appear on the application's dashboard. Unassigned applications will not appear as PCI applications in the AFA PCI regulatory compliance report.

Note: The PCI zone is specified in AFA.

To customize applications assigned to the PCI label:

1. In the toolbar, click your username.

A drop-down list appears.

2. In the drop-down list, select **Administration**.

3. Click the **Customization** tab.

4. In the **Application labels** area, click **Manage**.

The **Manage Application Labels** page appears, displaying all user-defined labels.

5. Select the **Show system labels** check box.

All existing system labels appear at the top of the list.

6. Select the system label with the name **PCI**.

The label appears with its list of associated applications in the **Assigned Applications** list. All applications with an object that intersects the PCI zone are assigned to the label by default.

7. To un-assign an application, click **Un-assign** next to the desired application.

8. To assign an application, click **Assign** next to the desired application.

Only applications that you previously un-assigned appear as options.

9. Click **Save Changes**.

Manage application and user awareness

Note: This procedure is only relevant when AppViz is being used without FireFlow. When AppViz is being used with FireFlow, application and user awareness is controlled by FireFlow.

ASMS supports the **User** and **Application** traffic fields. When a Palo Alto Networks or Check Point device is defined in AFA, user and network application awareness is automatically enabled in AppViz. Both these fields will appear wherever traffic fields

appear and will be considered in all traffic simulation queries, such as connectivity checks. If desired, you can manually enable or disable user and network application awareness in AppViz.

Note: In order to enable validation for the User field when using an LDAP authentication server, see Enabling Validation for the User Field (see [Enable validation for the user field](#)).

To manage application and user awareness:

1. In the toolbar, click your username.

A drop-down list appears.

2. In the drop-down list, select **Administration**.

The administration page appears in the workspace.

3. Click **Customization**.

The **Customization** tab appears.

4. To manage application awareness, do the following:

- To enable application awareness, in the **Application Awareness Support** area, click **Turn On**.
- To disable application awareness, in the **Application Awareness Support** area, click **Turn Off**.

5. To manage user awareness, do the following:

- To enable user awareness, in the **User Awareness Support** area, click **Turn On**.
- To disable user awareness, in the **User Awareness Support** area, click **Turn Off**.

Enable validation for the user field

By default, the value of the **User** field is not validated. If ASMS is fetching data from an LDAP authentication server (enabled in AFA), and user awareness is enabled in AppViz, you can manually enable or disable validation of the **User** field in AppViz.

Note: This procedure is only relevant when **User Awareness Support** is enabled for AppViz and fetching data from an LDAP is enabled in AlgoSec Firewall Analyzer. For more details, see [Manage application and user awareness](#).

To enable validation for the user field:

1. In the toolbar, click your username.

A drop-down list appears.

2. In the drop-down list, select **Administration**.

The administration page appears in the workspace.

3. Click **Customization**.

The **Customization** tab appears.

4. Do one of the following:

- To enable validation for the User field, in the **User Awareness Support** area, next to **User validation via LDAP is currently turned off**, click **Turn On**.
- To disable validation for the User field, in the **User Awareness Support** area, next to **User validation via LDAP is currently on**, click **Turn Off**.

Manage vulnerability assessment scanners

Relevant for AppViz administrators

This section describes how to manage vulnerability assessment scanner information, either by integrating directly with scanners, or importing vulnerabilities manually from files.

Tip: Once you configure vulnerability assessment scanners in AppViz, your AFA reports also include vulnerability data in the **Risky Rules** page. For more details, see the *AlgoSec Firewall Analyzer User Guide*.

Supported vulnerability assessment service providers

AppViz supports the following scanners:

- **Qualys** - QualysGuard (v7.0 and above). QualysGuard licenses must have KB permissions to integrate with AppViz, including API permissions.
- **Rapid 7** - Nexpose
- **Tenable** - Nessus Vulnerability Scanner, versions 6 and above
- **Tenable** - Nessus Manager
- **Tenable** - SecurityCenter

If your vulnerability scanner is not supported, AppViz enables you to import vulnerability data using our API instead. For details, see the *AlgoSecAppViz API Guide*.

Vulnerability scanner configuration prerequisites

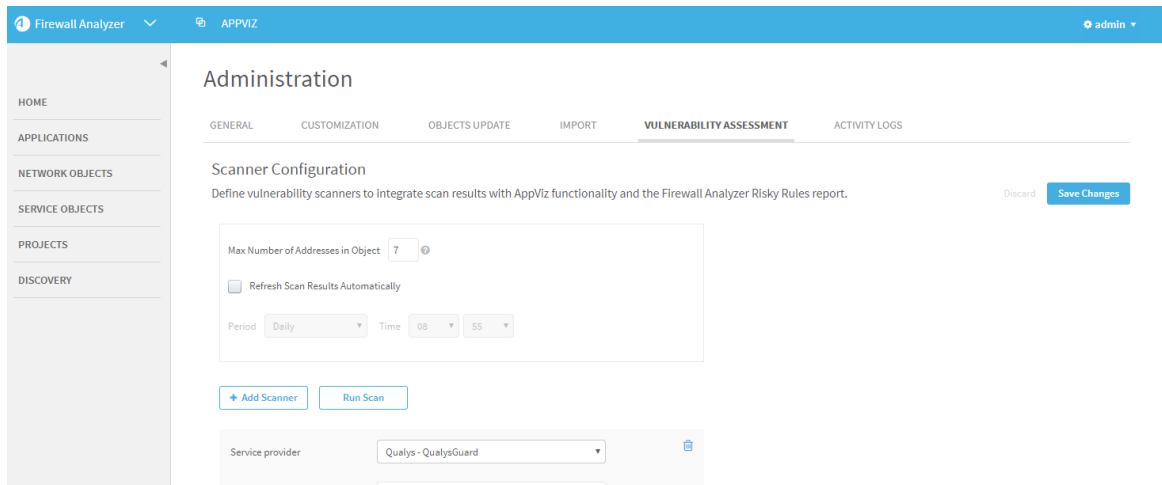
Configuring a vulnerability scanner in AppViz requires the following:

Connections	An open connection between the ASMS and the scanner. Default ports: <ul style="list-style-type: none"> • QualysGuard: 443 • Nessus: 8834 • Rapid Nexpose: 3780
Credentials	Credentials for a user with read permissions for all scans and API access
API address	A full API address for the scanner.

Define general vulnerability assessment settings

Do the following:

1. In the toolbar, click your username, and then select **Administration**.
2. Click the **VULNERABILITY ASSESSMENT** tab. For example:



3. Define the following general vulnerability settings:

<p>Max Number of Addresses in Object</p>	<p>Enter the maximum network object size.</p> <p>Only vulnerability information for network objects with this number of IP addresses or less will appear in ASMS.</p> <p>For example, an object with an IP range of 10.20.0.0/16 includes 65,536 IP addresses. It will therefore be ignored while performing vulnerability queries.</p> <p>Default = 256, Max = 1024</p>
<p>Refresh Scan Results Automatically</p>	<p>Determines whether AppViz refreshes vulnerability data automatically, and if so, how often and when.</p> <p>Default = Enabled, and set to Daily at 00:00.</p>

4. Click **Save Changes**.

Add a vulnerability scanner

Do the following:

1. In the toolbar, click your username, and then select **Administration**.
2. Click the **VULNERABILITY ASSESSMENT** tab.

- To add a new scanner, click **+ Add Scanner**. A new scanner definition area is added towards the bottom of the screen.

Tip: If you already have scanners configured, you may need to scroll down to view the new area.

Populate the fields as follows:

Service provider	Select the scanner type you want to add.
Scanner API address	Enter the scanner's server URL.
Username / Password	Enter the credentials used to access the scanner server.

- Click **Save Changes**.

Your new scanner is added to the grid, and scanning begins. It may take some time until the initial vulnerability scan is complete.

Delete a scanner

To delete a scanner configuration, click the **Delete**  button next to the scanner you want to delete.

Each of the scanners you configure enables you to do the following:

Update	Update vulnerability data from this scanner. This performs a manual refresh for the selected scanner, and is useful if you don't have refresh automatically selected, or if you want to run a manual update in between scheduled refreshes.
Disable	Disable the scanner without losing the scanner configuration data.

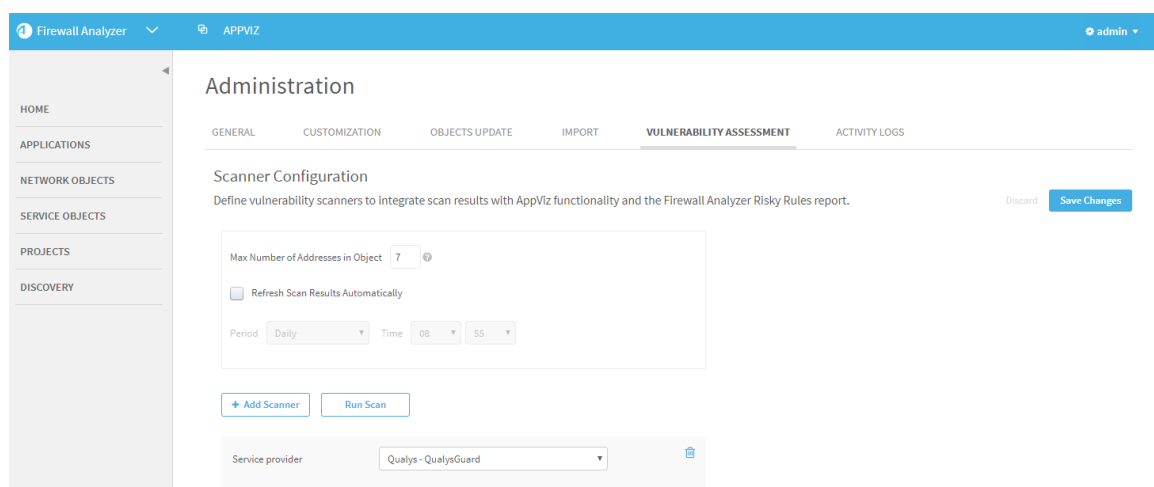
Run a vulnerability scan

This section describes how to run a vulnerability scan from the AppViz **Administration** area.

Before you start, you must have vulnerability scanners configured. For details, see [Add a vulnerability scanner](#).

Do the following:

1. In the toolbar, click your username, and then select **Administration**.
2. Click the **VULNERABILITY ASSESSMENT** tab. For example:



3. Click **Run Scan**. A full scan is run on all vulnerability scanners configured.

Tip: Optionally, enable AppViz to run scans automatically by refreshing scan results periodically. For details, see [Define general vulnerability assessment settings](#).

Import vulnerability assessment information

This section describes how to import your vulnerability data into AppViz from a CSV file using the command line.

Use this process when AppViz does not support integrating directly with your vulnerability scanner, and you do not want to use the API.

Do the following:

- [Prepare your CSV files](#)
- [Import vulnerability data](#)

Note: We do not recommend using this procedure to import vulnerability data, and keep this process documented for backwards compatibility only. Instead, we recommend importing vulnerability data via API. For details, see the *AlgoSecAppViz API Guide*.

Prepare your CSV files

In the `/home/bflow/config/vulnerability_from_file` directory, create the following CSV files:

Vulnerability data	<p>Name the file with a prefix that includes: vulnerability_info. For example: <i>vulnerability_info_dataJun12-19.csv</i></p> <p>Include the following column headers in the file:</p> <p>Mandatory column headers (in this order):</p> <ul style="list-style-type: none"> • Vulnerability ID (String, unique) • Summary (String) • Description (String) • CVSS score (Float) <p>Optional column headers: CVEs (Strings divided by ',')</p>
---------------------------	---

Server-vulnerability mapping	<p>Name the file with a prefix that includes: servers_vulnerability. For example: servers_vulnerability_dataJun12-19.csv</p> <p>Include the following column headers in the file:</p> <p>Mandatory column headers (in this order):</p> <ul style="list-style-type: none"> • IP address (string). Only single IP addresses are supported, not ranges or subnets. • Vulnerability ID (string) <p>Optional column headers: Date (Unix timestamps, in milliseconds). Default is the current date and time.</p> <p>Note: Each entry can contain only one vulnerability. If a single server has more than one vulnerability, the server must be represented on multiple lines.</p>
-------------------------------------	---

Note: Invalid data in either file will fail the entire import operation.

Continue with [Import vulnerability data](#).

Import vulnerability data

Once you have both your vulnerability data and server-vulnerability mapping CSV files ready in the `/home/bflow/config/vulnerability_from_file`, you're ready to import vulnerability data into AppViz.

For more details, see [Prepare your CSV files](#).

Do the following:

Open a terminal and run one of the following:

- Import both vulnerability and server mapping data together:

```
BusinessFlow-CLI.sh -t import_vulnerability_files
```

Note: Use this command if you this is the first time you are importing

vulnerability data.

- Import vulnerability data only:

```
BusinessFlow-CLI.sh -t import_vulnerability_information
```

- Import mapping data only:

```
BusinessFlow-CLI.sh -t import_servers_vulnerability
```


The vulnerabilities are imported.

Note: Vulnerabilities with a CVSS score of 0 are not supported and fail the validation.

Customize interactions with AFA and FireFlow

This topic describes how AppViz administrators can customize how AppViz and AppChange interact with elements in AFA and FireFlow.

For more details, see [AppViz administration](#).

 [Customizing Change Requests from AppViz](#): Watch to learn how to map AppViz custom fields to FireFlow template fields.

Manage application change requests

Use this procedure to customize the traffic change requests that AppChange opens as the result of applying changes to an application.

Note: Whenever a FireFlow change request is opened as the result of a change to a AppViz application, AppChange passes information about the application to FireFlow. The FireFlow change request will include a link to the application, the application's diagram, and details of the changes to the application's flows. The application information in FireFlow will only be visible to users with the required

AppViz permissions.

Do the following:

1. In the toolbar, click your username.

A drop-down list appears.

2. In the drop-down list, select **Administration**.

The administration page appears in the workspace.

3. Click **Customization**.

The **Customization** tab appears.

4. In the **FireFlow Change Request Definitions** area, next to **Manage application change requests**, click **Manage**.

The **FireFlow Application Change Requests** page appears.

The screenshot shows the 'FireFlow Application Change Requests' configuration page. The interface includes a top navigation bar with 'Firewall Analyzer' and 'APPVIZ' tabs, and a user profile 'AlgoSec Administrator'. A left sidebar contains navigation options: HOME, APPLICATIONS, NETWORK OBJECTS, SERVICE OBJECTS, PROJECTS, and DISCOVERY. The main content area is titled 'FireFlow Application Change Requests' and features a 'Cancel' button and a 'Save Changes' button. The configuration fields are as follows:

- Request Template:** A dropdown menu currently showing '150: Parallel-Approval Request'.
- Default Summary:** A text input field containing 'AppViz Change Request for {AppName}'.
- Decommission Default Summary:** A text input field containing 'AppViz Change Request for Decommissioning {AppName}'.
- Default Summary for an application related to a Critical Process:** A text input field containing 'AppViz Change Request for {AppName} which is associated with {CriticalProcessName}'.
- Template Fields:** A section with a list of fields: 'CHANGE REQUEST' (highlighted) and 'AFFECTED FLOWS'. Below the list is a description: 'Map AppViz application custom fields to FireFlow change request custom fields. Add field to begin.' and an '+ Add Field' button.

5. In the **Request Template** drop-down menu, select the FireFlow traffic change request template to use for all application based change requests.
6. Complete the fields using the information below.

In this field...	Do this...
Default Summary	Type the default summary for application based change requests. You can optionally include the variable {AppName} to indicate the relevant application's name.
Decommission Default Summary	Type the default summary for decommission change requests. You can optionally include the variable {AppName} to indicate the relevant application's name. This field is optional. If left blank, the Default Summary is used for all application based change requests (including decommission requests).
Default Summary for an application related to a Critical Process	Type the default summary for any change request opened for an application which is part of a Critical Process. You can optionally include the variable {AppName} to indicate the relevant application's name or the variable {CriticalProcessName} to indicate the critical process's name. This field is optional. If left blank, the Default Summary is used for all application based change requests (including requests related to critical processes).

7. (Optional) To map the values of AppViz fields to FireFlow change request custom fields, continue completing the fields as needed. For details, see [Template fields](#).
8. Click **Save Changes**.

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

Template fields

In this field...	Do this...
+ Add Field	Click this button to add a new field mapping for Applications, Flows, and Objects. Each component has different mapping fields as follows. Note: All custom fields for the selected request template appear as options.

In this field...	Do this...
Change Request	<p>Complete Change Request field mapping as follows:</p> <ul style="list-style-type: none"> • In the Template field drop-down list, select a Template field: Business Criticality, BusinessFlow Application, and Business Partner ID. • In the Application field drop-down list, select a field or value to map to: None, Name, Labels, or one of the listed application custom fields. <p>This field is only relevant for application based change requests.</p> <ul style="list-style-type: none"> • In Default value drop-down list, select None, Template Default, or Default value. If Default value is selected, type a default value in the blank box. <p>When typing a default value, you can optionally type the variable {AppName} to represent the application's name.</p>
Affected Flows	<p>Complete Affected Flows field mapping as follows:</p> <ul style="list-style-type: none"> • In the Template Traffic field drop-down list, select a field. • In the Flow field drop-down list, select a value: None, Name or Comment (Flow fields), or one of the listed application custom fields. • In the Default value drop-down list, select a value: None, Template Default, or Default value. If Default value is selected, type a default value in the blank box.
Network Objects	<p>Complete Network Objects field mapping as follows:</p> <ul style="list-style-type: none"> • In the Template Traffic Item field drop-down list, select a field. • In the Network Object field drop-down list, select a network object: None, Name, Type, or one of the listed Custom Fields. • In the Default value drop-down list, select a value: None, Template Default, or Default value. If Default value is selected, type a default value in the blank box.
	<p>Click this button to delete a field mapping.</p>

Manage object change requests

Use this procedure to customize the traffic change requests that AppChange opens as the result of changing an object used in an application.

Note: If your AppViz environment is configured to open a FireFlow *object change* request to change the definition of device objects on the device(s), this procedure does not apply. For details, see [Edit device objects](#).

Do the following:

1. In the toolbar, click your username.

A drop-down list appears.

2. In the drop-down list, select **Administration**.

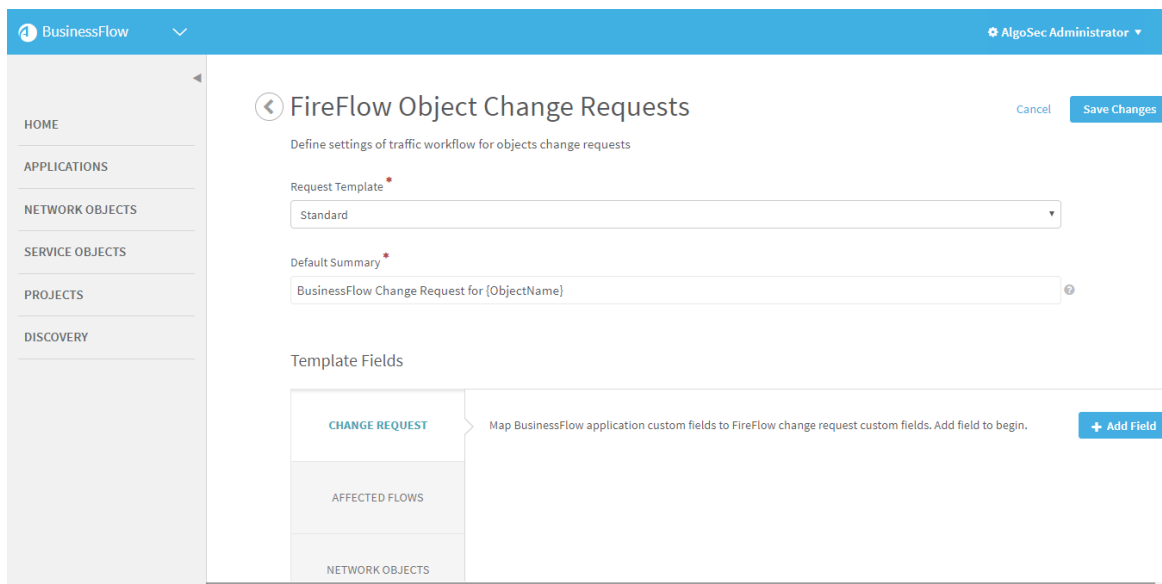
The administration page appears in the workspace.

3. Click **Customization**.

The **Customization** tab appears.

4. In the **FireFlow Change Request Definitions** area, next to **Manage object change requests**, click **Manage**.

The **FireFlow Object Change Requests** page appears.



5. In the **Request Template** drop-down menu, select the FireFlow traffic change request template to use for all object based change requests
6. In the **Object Change Default Summary** field, type the default subject for all object based change requests.


You can optionally include the variable `{ObjectName}` to indicate the relevant object's name.

7. (Optional) To map the values of AppChange fields to FireFlow change request custom fields, continue completing the fields as needed. For details, see [Template fields](#).
8. Click **Save Changes**.
A confirmation message appears.
9. Click **OK**.

Logging and notifications

Relevant for AppViz administrators

This topic describes how to manage AppViz activity logs and notification settings.

 **Setting Up Email Notifications:** Watch to learn how to set up email notifications for events and applications in AppViz.

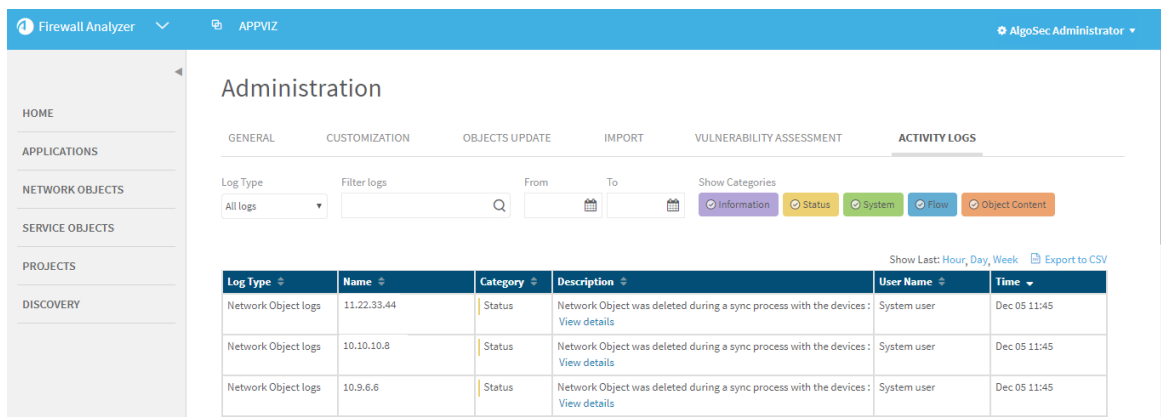
View all activity logs

AppViz provides the ability to view all the activities related to applications and network objects in one place, enabling you to see the different impacts of a single action. The extensive options for filtering the logs enable you to search for the activities you want to view. In addition to tracking current applications and network objects, the logs also document the history of deleted objects and decommissioned applications.

To view activity logs:

1. In the toolbar, click your username.
A drop-down list appears.
2. In the drop-down list, select **Administration**.
3. Click the **Activity Logs** tab.

The **Activity Logs** tab appears, displaying every activity log for every application and every network object.



The screenshot displays the 'Administration' section of the AppViz interface, specifically the 'ACTIVITY LOGS' tab. The page includes a navigation sidebar on the left with options like HOME, APPLICATIONS, NETWORK OBJECTS, SERVICE OBJECTS, PROJECTS, and DISCOVERY. The main content area shows a table of activity logs with the following data:

Log Type	Name	Category	Description	User Name	Time
Network Object logs	11.22.33.44	Status	Network Object was deleted during a sync process with the devices: View details	System user	Dec 05 11:45
Network Object logs	10.10.10.8	Status	Network Object was deleted during a sync process with the devices: View details	System user	Dec 05 11:45
Network Object logs	10.9.6.6	Status	Network Object was deleted during a sync process with the devices: View details	System user	Dec 05 11:45

Column	Description
Log Type	The activity log's type: Application or Object.
Name	The name of the application or network object.
Category	The activity's category: Flow, Information, Status, System or Object Content.
Description	Description of the activity.
User Name	Name of user who performed the activity.
Time	Date and Time the activity occurred.

4. To filter the logs by type, select the desired type in the **Log Type** drop-down menu.
5. To filter the logs by category, time, or a textual search, or to export the logs to a CSV file, see [Application activity log](#).

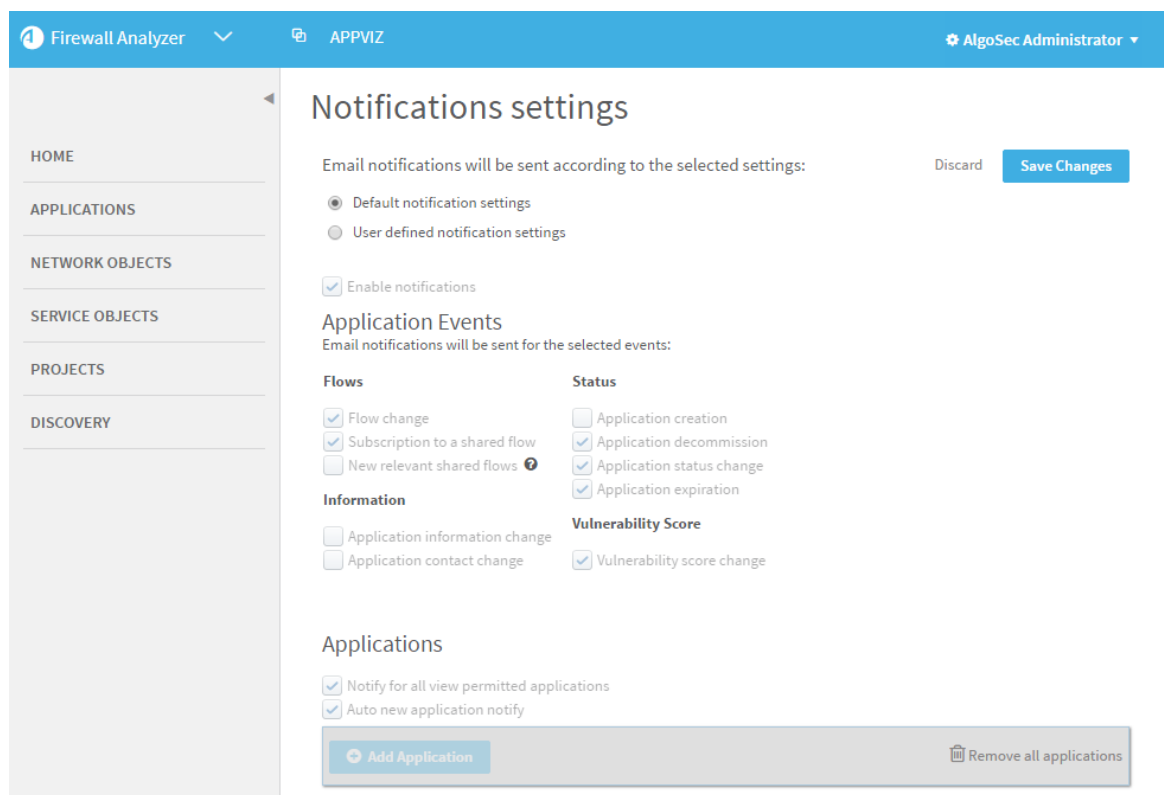
Customize email notifications

If desired, you can specify which application events should trigger sending an email notification to your user. You can specify custom email settings for specific applications or for all applications you have permissions for.

Note: User-specific settings override the default settings for all users and applications. To set the default email notification setting for all users and applications, see [Manage general email settings](#). Only administrators can manage general email settings.

To set custom email notification options:

1. In the toolbar, click your username.
A drop-down list appears.
2. In the drop-down list, select **Notifications Settings**.
The **Notifications settings** page appears in the workspace.



3. Do one of the following:

- To use the default email settings configured by the AppViz administrator, select **Default notification settings**.
- To configure custom notification settings for your user, do the following:
 1. Select **User defined notification settings**.
 2. In the **Application Events** area, select the check boxes for the events for which you want to receive email notifications.
 3. To only receive notifications for specific applications (and not every application you have permissions for), do the following in the **Applications** area:
 - a. Clear the **Notify for all view permitted applications** check box.
 - b. To not automatically receive notifications for new applications, clear the **Auto new application notify** check box.

- c. Click **+Add Applications** and select the desired applications. For details, see [Use the Add Applications wizard](#).

4. Click **Save Changes**.

Manage general email settings

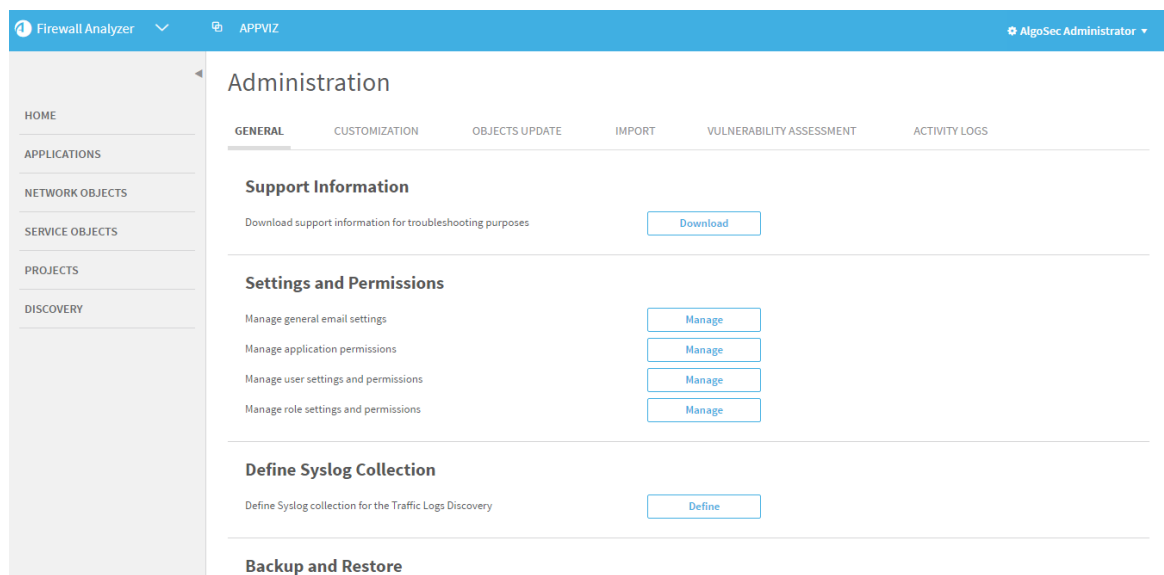
AppViz allows you to define default email notification settings for all users and applications. The general email settings can be overridden by user-specific notification settings. For details, see [Customize email notifications](#).

Note: The general email settings can only be configured by administrators.

To manage general email settings:

1. In the toolbar, click your username.
A drop-down list appears.
2. In the drop-down list, select **Administration**.

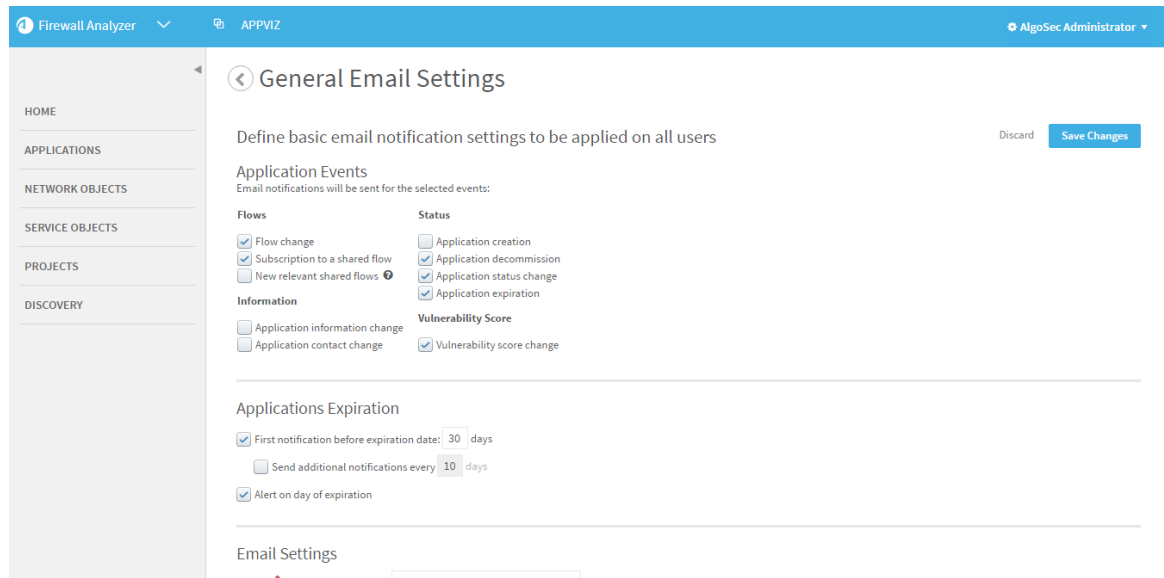
The **Administration** page appears in the workspace.



3. In the **Settings and Permissions** area, next to **Manage general email settings**,

click **Manage**.

The **General Email Settings** page appears.



4. Complete the fields as needed. For details, see [Email settings fields](#).
5. Click **Save Changes**.

Email settings fields

In this Field...	Do this...
Application Events	Select the events that should trigger email notifications.
Applications Expiration	Use this area to set when email notifications should be triggered for applications about to expiry.
First notification before expiration date: <i>n</i> days	To set how many days before expiration the first email notification should be sent, select this check box and type the number of days into the field. Notifications are via email and GUI.
Send additional notifications every <i>n</i> days	To set the period for additional email notifications, select this check box and type the number of days. Notifications are via email and GUI.

In this Field...	Do this...
Alert on day of expiration	Select this check box to create an activity log alert on the day of expiration. No email or GUI notification on day of expiration.
Email Settings	Use this area to customize the email notifications that are sent.
Sender:	Type the sending email address.
Subject Prefix	Type the prefix of the email subject.
Greeting	Type the email greeting.
Signature	Type the email signature.
AppViz URL:	In the box, type the IP address or host name to complete the URL.

Discovery settings

This topic describes how to configure an AlgoSec AutoDiscovery server or a Cisco Tetration server in AppViz.

These both enable you to import flows to AppViz directly from discovered applications in an AutoDiscovery or Tetration system.

For more details, see [Discover applications](#).

Configure an AutoDiscovery server

This procedure describes how to connect an AutoDiscovery server to AppViz, enabling you to use AutoDiscovery to discover business applications and import them in to AppViz.

Do the following:

1. In the AppViz Administration area, click the **Discovery** tab.
2. Click **Connect to AlgoSec AutoDiscovery**, and enter the following details:

AutoDiscovery server URL	The IP address of the AutoDiscovery server.
AutoDiscovery server username	The username used to access the AutoDiscovery server.
AutoDiscovery server password	The password used to access the AutoDiscovery server.

- (Optional) When adding an AutoDiscovery server, configure the additional optional automation options:

Auto-run discovery after every synch with	Select to configure AppViz to run an automatic discovery after each automatic synchronization with AFA. Displayed only when Automatic update is enabled on the OBJECTS UPDATE tab of the AppViz Administration area.
Schedule	Select to schedule a daily or weekly discovery at a specific time. Displayed only when Automatic update is disabled on the OBJECTS UPDATE tab of the AppViz Administration area.

For more details, see [Update all device objects](#).

- Click **Save** at the top-right of the page to save your changes.

Configure a Cisco Tetration server

This procedure describes how to connect a Cisco Tetration server to AppViz, enabling you to use Tetration to discover business applications and import them in to AppViz.

Do the following:

- In the AppViz Administration area, click the **Discovery** tab.
- Click **Connect to Cisco Tetration**, and enter the following details:

Cisco Tetration server URL	The IP address of the Tetration server.
-----------------------------------	---


Cisco Tetration VRF ID	The VRF ID used to access the Tetration server.
Cisco Tetration OpenAPI Key	<p>The OpenAPI key used to access the Tetration server. Click Select a File to browse to and select the OpenAPI key file to upload.</p> <p>Tip: Click Download Example to view a sample json OpenAPI key file.</p>

3. Click **Save** at the top-right of the page to save your changes.

Configure advanced settings

This procedure describes how to access and configure advanced AppViz settings for discovery.

Do the following:

1. In the AppViz **Administration** area, click the **Discovery** tab, and then click  **Advanced Settings**.

2. Configure the settings as follows:

Existing applications	<p>Select one of the following to determine how AppViz handles flows that are discovered with existing AppViz applications:</p> <ul style="list-style-type: none"> • Append flows to existing applications. This prevents duplication and the creation of extra AppViz applications. • Ignore flows that relate to existing applications (create only new applications). Ignore flows that are related to any applications that already exist. Only flows with new applications will be imported.
Optimize traffic flows	<p>Select this option to automatically optimize discovered traffic flows. This helps to organize and manage your applications efficiently.</p> <p>Select Optimize my traffic flows, and then enter a number in the text box to indicate the maximum number of flows per application.</p>
Optimization mapping	<p>Select Enable object mapping to map the discovered IP addresses to specific network objects.</p> <p>If you select this option, then also select or upload a new CSV mapping file to the AppViz server.</p> <p>Click Sample CSV mapping file to download an example of how this file should be configured.</p>


3. Click **Save** to save your changes and close the dialog.

Tip: Additional advanced settings are available via the CLI and the `user.properties` file. For details, see [Configure advanced AppViz properties](#).

AppViz maintenance

Relevant for AppViz administrators

This section describes maintenance procedures that administrators must perform periodically to maintain AppViz.

 [Updating Network Objects](#): Watch to learn how to ensure that your AppViz

network objects are always up to date.

View AppViz product data

You can view information about your AppViz installation, including version and build number.

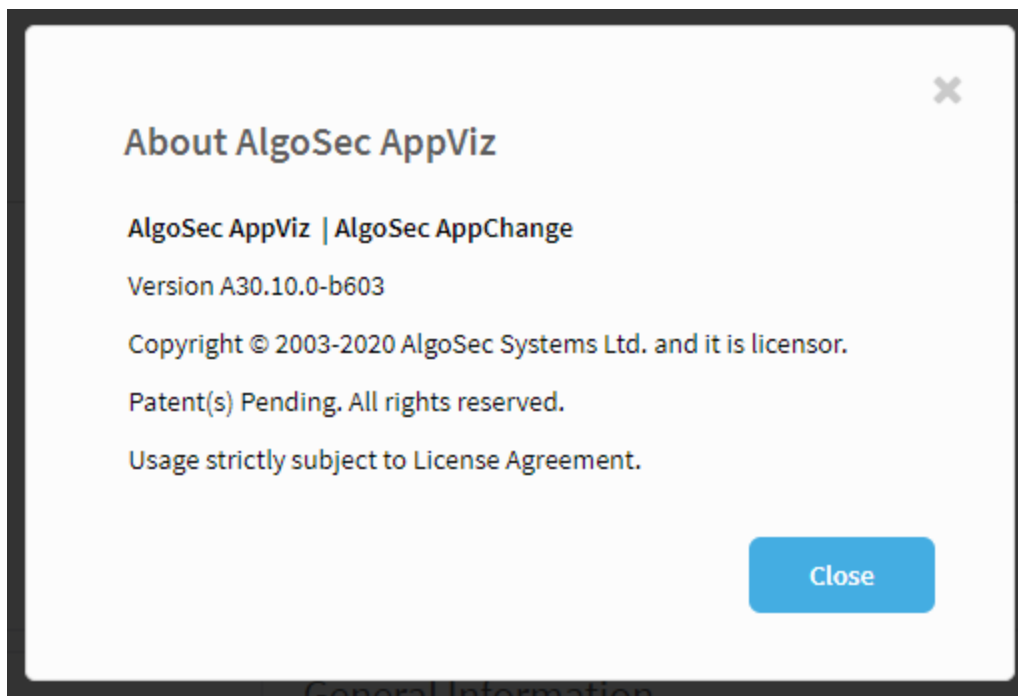
To view information about your AppViz installation:

1. In the toolbar, click your username.

A drop-down list appears.

2. In the drop-down list, select **About**.

The **About AlgoSec AppViz** window appears displaying the version, build, and copyright information.



Download support data

If needed, you can download support information for troubleshooting purposes and send it to AlgoSec technical support.

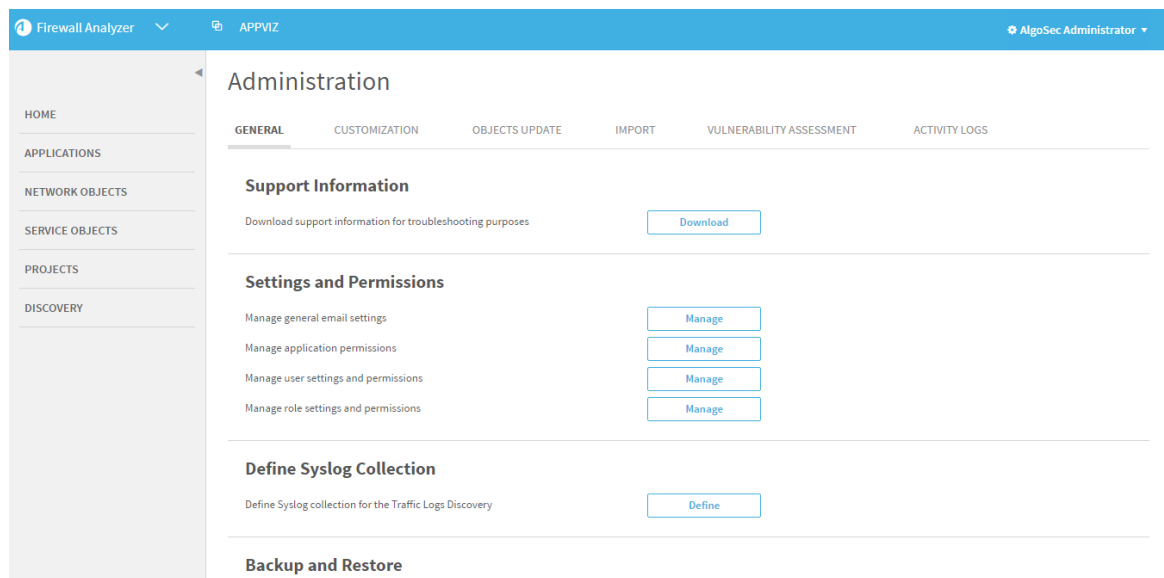
Do the following:

1. In the toolbar, click your username.

A drop-down list appears.

2. In the drop-down list, select **Administration**.

The administration page appears in the workspace.



3. In the **Support Information** area, click **Download**.

A ZIP file called **appviz-support-zip.zip** is downloaded to your computer.

AppViz troubleshooting permissions

AppViz troubleshooting may include steps such as viewing logs, editing configuration files and log configuration files, restarting the AppViz service, and running the CLI tool.

To perform these steps, you must have the following permissions:

- Read **/var/log/bflow**
- Read/write **/home/bflow/config**
- Execute/read **/usr/share/bflow**
- Restart the AppViz service (**/etc/init.d/algosec-ms restart**)

For more details, see [Restart AppViz](#).

Update all rule/application associations for AFA

AppViz applications associated with specific device rules are indicated in AFA for each rule. Run a connectivity check on an AppViz application to update and synchronize the rule details in AFA.

Do the following:

1. Open a terminal.
2. Enter the following command:

```
BusinessFlow-CLI.sh -t update_rule_application_association
```

A connectivity check is run for every application in AppViz and the AFA details are updated for each rule.

Backup and restore AppViz from the CLI

Do the following:

Open a terminal and run one of the following:

Back up AppViz	BusinessFlow-CLI.sh -t backup -o <i>File</i> where <i>File</i> is the full path of the output backup file.
Restore AppViz	BusinessFlow-CLI.sh -t restore -i <i>File</i> where <i>File</i> is the full path of the backup file.

Restart AppViz

Some AppViz configurations require that you restart AppViz.

Do the following:

1. Log in to the AppViz server as user **root**.
2. Run the following command:

```
/usr/share/bflow/restart_businessflow.sh
```

AppViz is restarted.

Update or import AppViz data

Administrators can update or import data into AppViz using files from AFA, CSV files, or a CMDB.

For more details, see:

- [Update data via CSV files](#)
- [Update objects from a CMDB](#)

Tip: Additionally, you can import flow data using an automatic discovery server, or using data exported from AFA. For details, see [Discover applications](#)

Customize AppViz user interface text

You can customize text in the AppViz web interface. This allows you to translate the web interface into a different language or simply edit terminology to suit your needs.

Do the following:

1. Open a terminal and log in using the username "bflow" and the related password.
2. Create a new file at `/home/bflow/config/customization/customized_messages`.
3. Copy the contents of `/data/afa_catalina_base/webapps/BusinessFlow/WEB-INF/classes/messages/messages.properties` into the new file.
4. Search for the phrases you want to edit and change them as needed.

For example, to change the word **Summary** to **Information**, do the following:

- a. Search the file for the word **Summary**. It should appear in the following line:

```
application.stats.revision.header=Revision Summary
```

- b. Edit the line as follows:

```
application.stats.revision.header=Revision Information
```

- c. Continue searching and editing as needed.

Warning: When making changes, do not change the key value, which is the string on the left side of the code.

5. Save the file.
6. Restart AppViz. For details, see [Restart AppViz](#).

Update data via CSV files

This topic describes how to update AppViz data from CSV files from the AppViz**Administration** area or via CLI.

Flows can also be imported from CSV files in the main **Discovery** area. For details, see [Discover applications via AutoDiscovery or Cisco Tetration](#).

Supported import data

AppViz provides the ability to import the following data from CSV files:

- Flows to applications (including discovery search results)
- Applications and custom application fields
- Contacts and custom contacts fields
- Contacts and their roles in applications
- Network Objects and their custom fields

CSV file sources

Some options for acquiring the CSV file include:

- Exporting it from your configuration management database (CMDB).
- Exporting it from AlgoSec Firewall Analyzer. For details, see [Export flows directly from AFA](#).
- Creating it through a AppViz discovery search. For details, see [Discover applications](#).
- Preparing it manually. For details, see [Prepare a CSV file](#).

When you have the data ready, run the update.

For details, see:

- [Import network object CSV data into AppViz](#)
- [Import CSV data into AppViz](#)

Prepare a CSV file

Note: You can download an example of any of the types of CSV files. In the **Import** tab of the **Administration** area you can download examples of the Applications, Contacts, Flows or Application Contacts CSV file. In the **Objects Update** tab of the **Administration** area you can download an example Network Object CSV file.

Prepare a CSV file for importing applications and custom application fields

Do the following:

1. Open a new text file.
2. In the first line of the file, type a list of column headers. The headers must be separated by commas.

Column requirements:

The first column must be the application name. All other column headers are optional, and should contain custom fields for the applications.

3. For each application you want to import, type a new line containing values that

correspond to the column headers. The values must be separated by commas.

For example:

```
Application Name,Business Unit,Geographical Location,Internal app-id  
Application#1,Financial Services,Europe,241154  
AnotherApp,IT,Boston MA,044914
```

4. Save the file.

Prepare a CSV file for importing contacts and custom contact fields

Do the following:

1. Open a new text file.
2. In the first line of the file, type a list of column headers. The headers must be separated by commas.

Column requirements:

The first four columns must be first, middle, last, and email (in that order). All other column headers are optional, and should contain custom fields for the contacts.

3. For each contact you want to import, type a new line containing values that correspond to the column headers. The values must be separated by commas.

For example:

```
First,Middle,Last,Email,Extension,Cell Phone,Number of children  
John,,Smith,smith@company.com,#1234,(614)113-1452,0  
Ned,Nicholas,Networks,ned@company.com,#9999,(614)113-1515,2
```

4. Save the file.

Prepare a CSV file for importing contacts for application contact roles

Importing contacts for application contact roles allows you to specify contacts for the contact roles of many applications. The contact roles and the contacts you specify for an

application can be existing contacts/contact roles or new contacts/contact roles. Any new contacts/contact roles will be automatically created when you run the import.

Do the following:

1. Open a new text file.
2. In the first line of the file, type a list of column headers. The headers must be separated by commas.

Column requirements:

The first column must be the application name. All other column headers should contain contact roles; you can include as many columns as you desire.

3. For each application you want to import contacts for, type a new line containing values that correspond to the column headers. The corresponding value for each contact role should be the email address of the contact you want to assign to the role. The values must be separated by commas.

Note: If you type an email address that does not correspond to an existing contact, a new contact will be created. The new contact's name field and email field will both be the new email address.

For example:

```
Application,Application Owner,IT Support,  
Business RepresentativeNetBackup,ned@company.com,  
netbackup-support@company.com,rob@company.com
```

Importing the above example will cause the following:

- If the contact role's Application Owner, IT Support, or Business Representative do not exist, they will be created.

- If the contacts with the email addresses ned@company.com, netbackup-support@company.com, or rob@company.com do not exist, they will be created.
 - For the application NetBackup, the contact with the email address ned@company.com will be assigned the Application Owner role, the contact with the email address netbackup-support@company.com will be assigned the IT Support role, and the contact with the email address rob@company.com will be assigned the Business Representative role.
4. Save the file.

Prepare a CSV file for importing network objects and custom network object fields

Do the following:

1. Open a new text file.
2. In the first line of the file, type a list of column headers. The headers must be separated by commas.

Column requirements:

The first two columns, in the following order, must be:

- *Network Object Name*. A string.
- *Network Object Contents*. An IP address (Host), a range/CIDR (Range), a comma delimited list of network objects (Group), or empty/no content (Abstract).

All other column headers are optional, and should contain custom fields for the network objects.

Note: There are no requirements for the header names.

In case of different objects with the same name (defined on different devices), you can specify the object name with the device name, separated by a semicolon. For

example, if there is a network object "internal" on device1, and a network object "internal" on device2, you can specify that you intend the network object on device1 by typing `internal;device1`.

3. For each network object you want to import, type a new line containing values that correspond to the column headers. The values must be separated by commas.

For example:

```
Name,AddressesWebFarm1,192.159.221.0/24WebFarm2,192.159.222.0-192.159.222.255WebFarm3,192.159.223.0/24WebFarms,WebFarm1,WebFarm2,WebFarm3,WebFarm4;WebFarmDevice
```

Importing the above example will create four new network objects:

- WebFarm1, which contains 192.169.221.0/24
- WebFarm2, which contains 192.159.222.0-192.159.222.255
- WebFarm3, which contains 192.159.223.0/24
- WebFarms, which contains the 3 new web farm objects as well as `WebFarm4` (which is a device object on the device named `WebFarmDevice`).

4. Save the file.

Prepare a CSV file for importing flows and custom flow fields

Importing flows and custom flow fields allows you to assign flows to many applications. The flow fields you specify can include new custom flow fields. You can import application flows, shared flows and subscribed flows.

Do the following:

1. Open a new text file.
2. In the first line of the file, type a list of column headers. The headers must be separated by commas.

You can optionally download an example CSV file for importing flows and use it as a template by replacing the sample values with your own values. For details, see [Download a flows CSV example](#).

Mandatory Headers:

- *application*. The name of the application, or in the case of a shared flow, the name of the shared application. In case of a subscribed flow, the name of the subscribed application.
- *sources*. A comma separated list of existing network object names and/or IP addresses/ranges. Leave this field empty to specify the source as the placeholder for a shared flow.

Note: Any IP addresses/ranges included in the source or destination of the flow that are not defined as an object will automatically be defined as an object in AppViz.

- *destinations*. A comma separated list of existing network object names and/or IP addresses/ranges. Leave this field empty to specify the destination as the placeholder for a shared flow.
- *services*. A comma separated list of service objects. Leave this field empty for subscribed flows.
- *comment*. A comment for the flow.
- *name*. The name of the flow. For subscribed flows, the name needs to specify the shared application and shared flow name in the following format: **APP:{<shared application>},FLOW:{<shared flow name>}**. If this field is left empty (for shared or application flows), AppViz will generate a sequential name for the flow.

Optional Headers:

- *network applications*. (relevant only when application awareness is enabled)
A comma separated list of network application objects enclosed by quotations.
- *user*. (relevant only when user awareness is enabled) A comma separated list of user names enclosed by quotations.

In case of different objects with the same name (defined on different devices), you can specify the object name with the device name, separated by a semicolon. For example, if there is a network object "internal" on device1, and a network object "internal" on device2, you can specify that you intend the network object on device1 by typing `internal;device1`.

All other column headers are optional, and can contain custom fields for the flows.

3. For each flow you want to import, type a new line containing values that correspond to the column headers. The values must be separated by commas.

For example:

```
Application, Sources, Destinations, Services, Comment, NameNetBackup,
BackupServer, "BackedUpWorkstations, BackedUpServers",
NetBackupServices, NetBackup, "BackedUpWorkstations, BackedUpServers",
BackupServer, NetBackupServices,
```

Note: When you specify multiple objects for a single field, these objects must be in a comma separated list. When viewing the CSV as a spreadsheet, the comma separated list must be in a single cell. When viewing the CSV as text, the comma separated list must be enclosed in quotations.

4. Save the file.

Download a flows CSV example

To download a flows CSV example from the Administration area:

1. In the toolbar, click your username.

A drop-down list appears.

2. In the drop-down list, select **Administration**.

The administration page appears in the workspace.

3. Click the **Import** tab.

The **Import** tab appears.

4. In the **Flows** area, click **Download Example**.

The sample CSV file downloads to your computer.

To download a flows CSV example from the Discovery area:

1. Go to the **Discovery** area. For details, see [Welcome to AppViz](#).

The **Discovery** area appears in the workspace.

2. In the **Import Flows from File** area, click **Download Example**.

The sample CSV file downloads to your computer.

Import CSV data into AppViz

After acquiring the CSV file, you import the data into AppViz.

Note: This procedure is not appropriate for importing network objects. For network objects, [Import network object CSV data into AppViz](#).

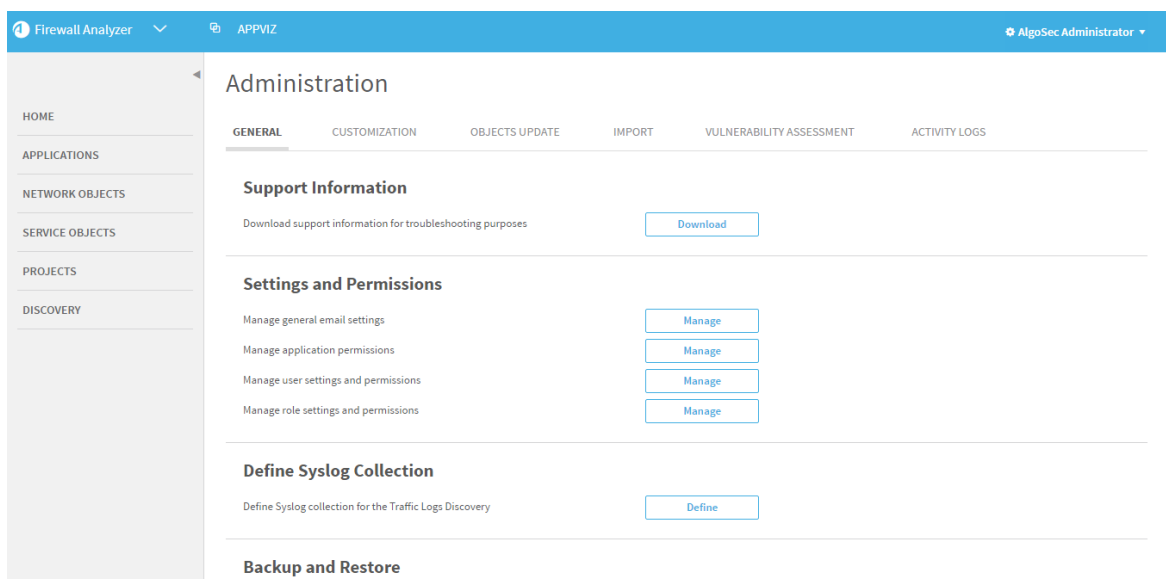
Note: Flows can optionally be imported in the **Discovery** area. For details, see [Update data via CSV files](#).

Note: You can optionally import the files using the CLI. For details, see [Import CSV data into AppViz via CLI](#).

To run the update:

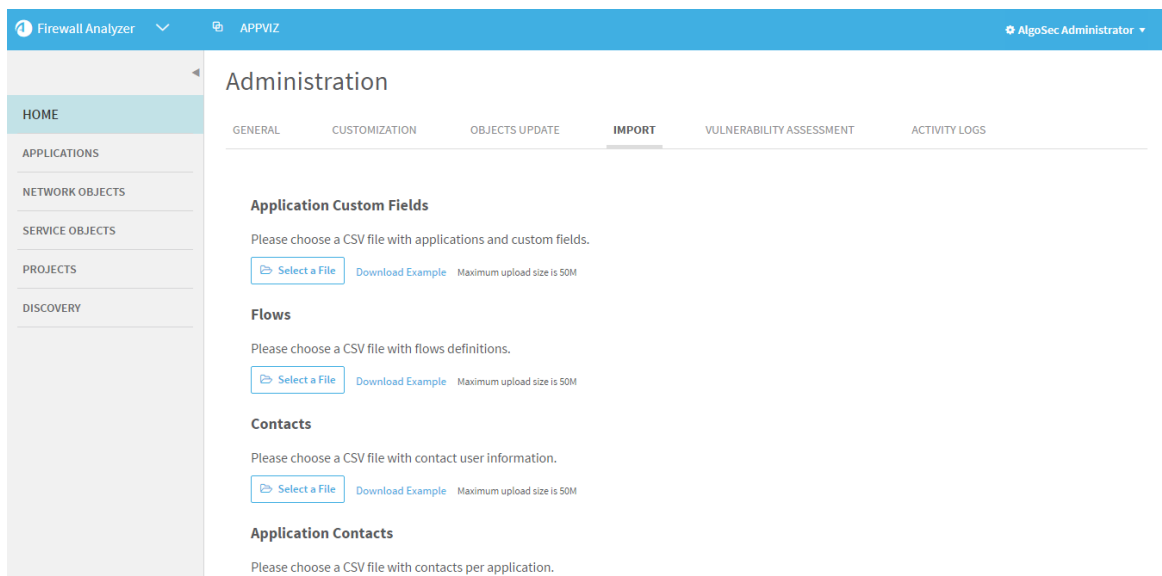
1. In the toolbar, click your username.
A drop-down list appears.
2. In the drop-down list, select **Administration**.

The **Administration** page appears in the workspace.



3. Click the **Import** tab.

The **Import** tab appears.



4. In the area relevant to the type of data you are importing, click **Select a File**.

5. Select the desired CSV file.

The selected file appears in the Web Interface.

6. Click **Import**.

The file is imported, and a success message appears with information about the import.

Import network object CSV data into AppViz

After acquiring the CSV file, you import the data into AppViz. You can import the CSV files manually or schedule automatic updates from the AppViz database.

Additionally, you can review the results of the last import. For details, see [Update objects from a CMDB](#).

Note: You can optionally import network objects using the CLI. For details, see [Import CSV data into AppViz via CLI](#).

To run the update for network objects:

1. In the toolbar, click your username.

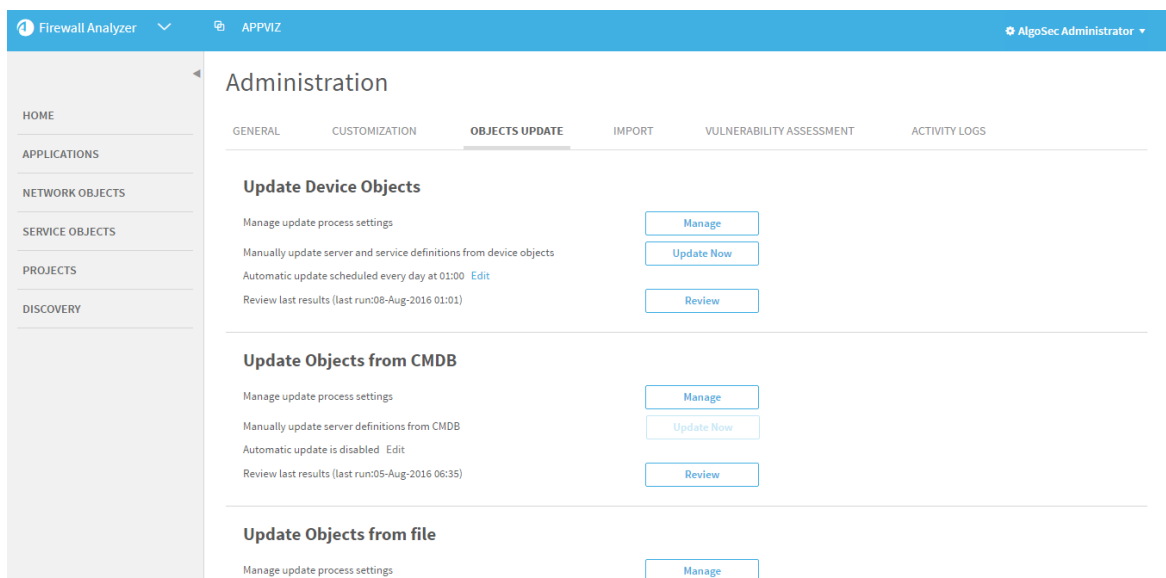
A drop-down list appears.

2. In the drop-down list, select **Administration**.

The **Administration** page appears in the workspace.

3. Click the **Objects Update** tab.

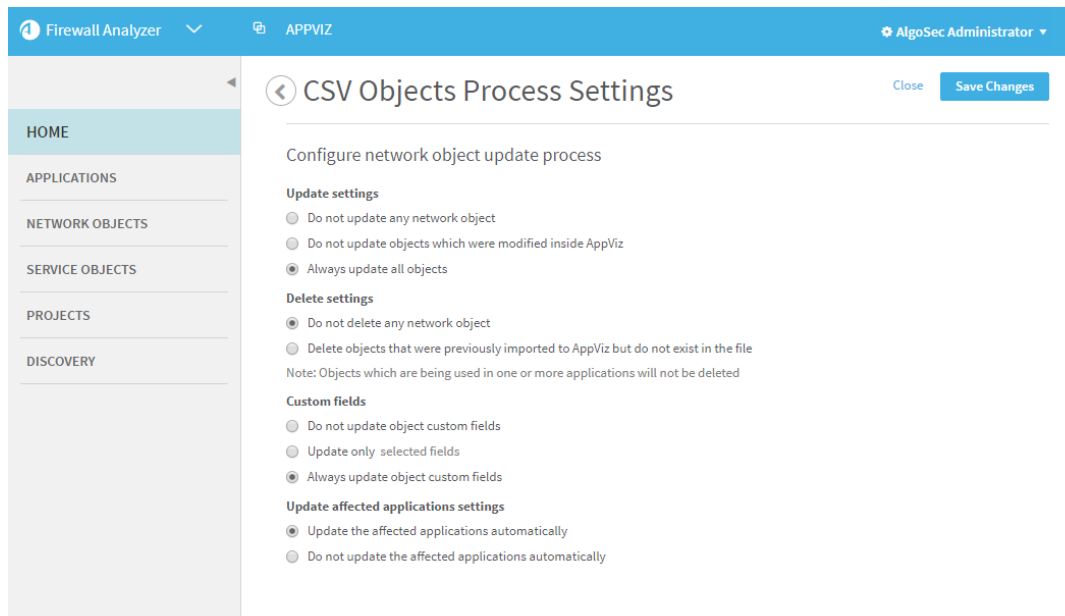
The **Objects Update** tab appears.



4. Configure the behavior of the import, by doing the following:

- a. In the **Update Objects from file** area, click **Manage**.

The **CSV Objects Process Settings** page appears.



b. Select the desired options as needed. For details, see [Update objects from a CMDB](#).

c. Click **Save Changes**.

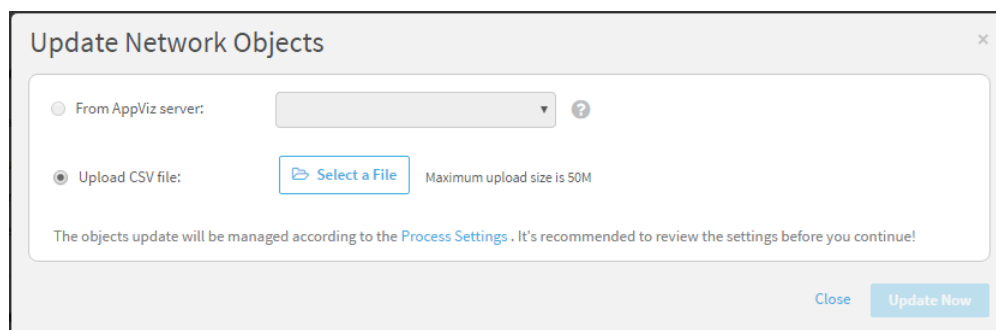
A confirmation message appears at the top of the workspace.

5. In the **Update Objects from file** area, do one of the following:

- To manually update objects, do the following:

1. Click **Update Now**.

The **Update Network Objects** dialog box appears.



2. Do one of the following:

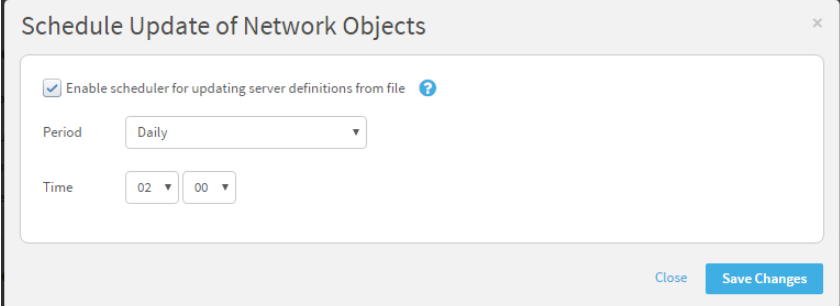
- To select a file from the AppViz server (*/home/bflow/config/discovery_from_logs*), do the following:
 1. Select **From AppViz server**.
 2. In the drop-down menu, select the CSV file.
- To select a CSV file from any location, do the following:
 1. Select **Upload CSV file**.
 2. Click **Select a File**.
 3. Select the desired CSV file.

3. Click **Update Now**.

The objects are updated, and a success message appears with information about the import.

- To schedule automatic updates, do the following:
 1. Click **Edit**.

The **Schedule Update of Network Objects** dialog box appears.



Screenshot of the "Schedule Update of Network Objects" dialog box. The dialog contains a checked checkbox labeled "Enable scheduler for updating server definitions from file" with a help icon. Below this, there is a "Period" dropdown menu set to "Daily" and a "Time" section with two dropdown menus set to "02" and "00". At the bottom right, there are "Close" and "Save Changes" buttons.

2. Complete the fields as needed. For details, see [Update objects from a CMDB](#).

Note: If many files accumulate between scheduled

updates and are consequently all imported at once, the oldest file is imported first. Conversely, in the case where the update is configured to delete objects that are not present in the file, objects will only be deleted if they do not appear in any of the files.

3. Click **Save Changes**.
4. Save the file you want to use for the update to the AppViz server:

```
/home/bflow/config/objects_update.
```

The automatic updates are scheduled, and will run off of the file you specified.

Import CSV data into AppViz via CLI

To run an import for a CSV file from the CLI:

1. Open a terminal.
2. Enter the following command:

```
BusinessFlow-CLI.sh -t Task -i CSVFile
```

where *Task* is one of the following tasks:

- **import_applications**. Imports applications and custom application fields to the AppViz database.
- **import_contacts**. Imports contacts and custom contact fields to the AppViz database.
- **import_app_contacts**. Imports contacts and their roles to applications.
- **import_objects**. Imports network objects.
- **import_flows**. Imports flows definitions to applications.

and, *CSVFile* is the full path to the CSV file.

The data in the CSV file is imported.

Update objects from a CMDB

Related for AppViz administrators

This topic explains how to import data into AppViz from a configuration management database (CMDB).

For more details, see:

- [Export flows directly from AFA](#)

CMDB import support

AppViz supports importing network objects directly from a CMDB. You can update your objects from the CMDB manually, or schedule automatic updates.

Additionally, you can review the results of the last import. See [Reviewing the last object update](#).

Note: If AppViz does not support the CMDB you use, you can export your data from your CMDB as a CSV file and then import it into AppViz. See [Update data via CSV files](#).

HPE Universal CMDB (UCMDB)

AppViz supports the **HP Universal CMDB (UCMDB)** for IPv4 IP addresses only.

For UCMDB, AppViz imports computer CIs. When a CI has more than one IP address, AppViz creates an object for each IP address, and The object names are created by concatenating the IP address to the name.

For example, if a computer called **TEST** has 2 IP addresses, **1.1.1.1** and **2.2.2.2**, AppViz will create 2 objects: **TEST_1.1.1.1** and **TEST_2.2.2.2**.

If one of the IP addresses changes and the object is used in an application flow, the object will be marked as deleted in the application.

To update objects from a CMDB:

1. In the toolbar, click your username.

A drop-down list appears.

2. In the drop-down list, select **Administration**.

The **Administration** page appears in the workspace.

3. Click the **Objects Update** tab.

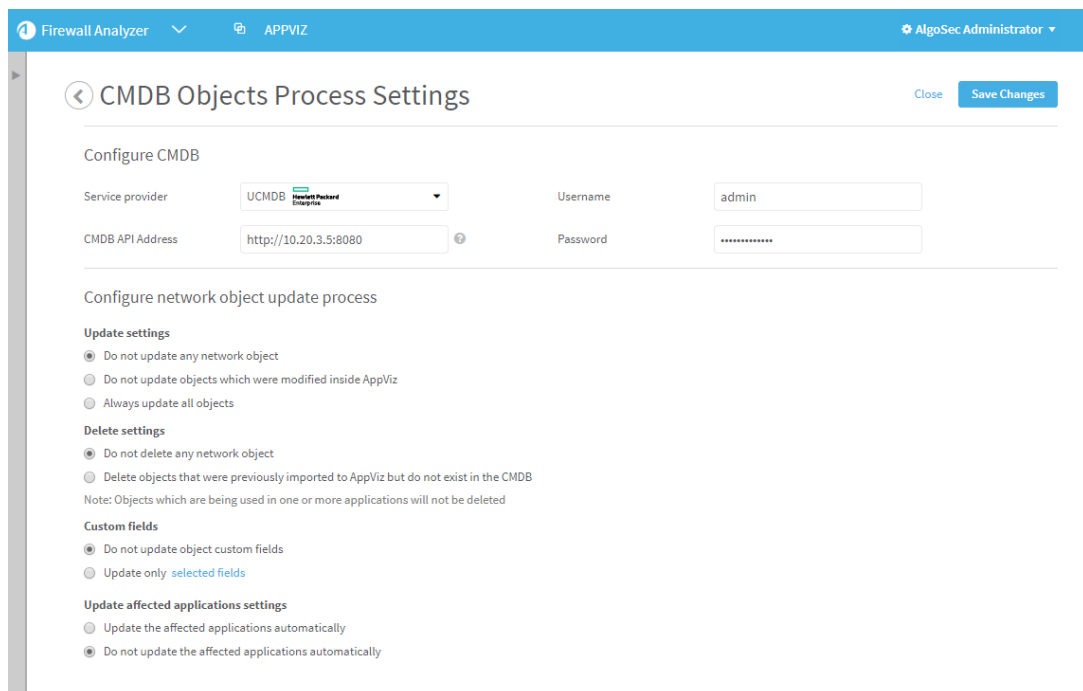
The **Objects Update** tab appears.

The screenshot shows the AppViz Administration interface. The top navigation bar includes 'Firewall Analyzer', 'APPVIZ', and 'AlgoSec Administrator'. The left sidebar lists navigation options: HOME, APPLICATIONS, NETWORK OBJECTS, SERVICE OBJECTS, PROJECTS, and DISCOVERY. The main content area is titled 'Administration' and has tabs for GENERAL, CUSTOMIZATION, OBJECTS UPDATE (selected), IMPORT, VULNERABILITY ASSESSMENT, and ACTIVITY LOGS. Under the 'OBJECTS UPDATE' tab, there are three sections: 'Update Device Objects', 'Update Objects from CMDB', and 'Update Objects from file'. Each section contains update process settings and buttons for 'Manage', 'Update Now', and 'Review'.

4. Configure the behavior of the import, by doing the following:

- a. In the **Update Objects from CMDB** area, click **Manage**.

The **CMDB Objects Update Settings** page appears.



- b. Configure the CMDB by completing the fields as needed. For details, see [CMDB configuration fields](#).
- c. Select the desired options as needed. For details, see [CSV/CMDB objects update settings options](#).
- d. Click **Save Changes**.

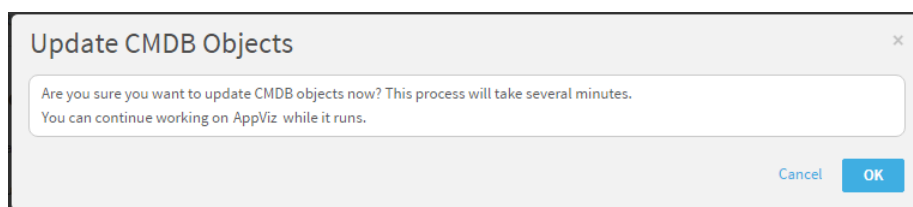
A confirmation message appears at the top of the workspace.

5. In the **Update Objects from CMDB** area, do one of the following:

- To manually update objects, do the following:

Click **Update Now**.

The **Update CMDB Objects** dialog box appears.



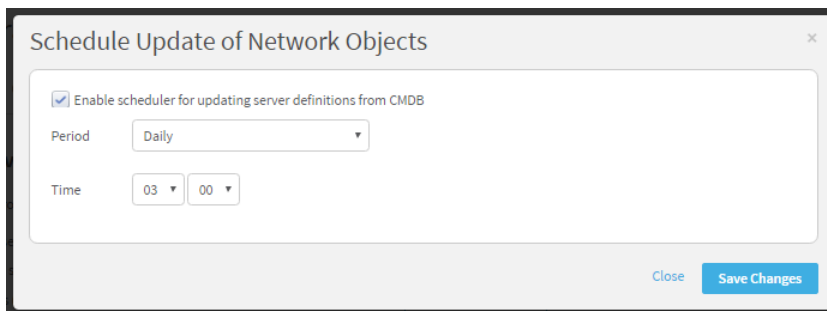
Click **OK**.

The network objects are updated.

- To schedule automatic updates, do the following:

Click **Edit**.

The **Schedule Update of Network Objects** dialog box appears.



Complete the fields as needed [Schedule update of network objects fields](#).

Click **Save Changes**.

The automatic updates are scheduled, and will run off of the file you specified.



CMDB configuration fields

In this field...	Do this...
Service provider	Select the CMDB service provider in the drop-down menu.
CMDB API Address	Type the CMDB server URL and port. For example, http://192.168.0.101:8080
Username	Type the username to access the CMDB.
Password	Type the password associated with the username.

CSV/CMDB objects update settings options

For this setting...	Do this...
Update settings	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Do not update any network object. Choose this option to indicate you do not want to update the definitions of any objects already in AppViz when the file/CMDB contains a different definition. This is the default behavior. • Do not update objects which were modified inside AppViz. Choose this option to indicate you only want to update the definitions of objects which have not been modified in AppViz. • Always update all objects. Choose this option to indicate you want to update all objects in AppViz with the definitions in the file/CMDB. <p>This option is relevant for CMDB updates, or when the CSV file is a comprehensive list of all current object definitions.</p>
Delete settings	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Do not delete any network object. Choose this option to indicate you do not want to delete an object from AppViz when it does not appear in the file/CMDB. This is the default behavior. • Delete objects that were previously imported to AppViz but do not exist in the file. Choose this option to indicate you want to delete all objects from AppViz that do not appear in the file/CMDB. <p>This is relevant for CMDB updates, or when the CSV file contains a comprehensive list of all the objects you want in AppViz.</p> <div style="background-color: #e0f2f7; padding: 10px; border: 1px solid #ccc;"> <p>Note: Objects in the current revision of an application will not be deleted. Additionally, for CSV file updates, if many files accumulate between scheduled updates and are consequently all imported at once, objects will only be deleted if they are not present in any of the files.</p> </div>

For this setting...	Do this...
Custom fields	<p>Select one of the following:</p> <ul style="list-style-type: none"> <p>Do not update object custom fields. Choose this option to indicate you do not want to update custom fields or their values already in AppViz with the custom fields and values in the file/CMDB.</p> <p>This is the default behavior.</p> <p>Update only selected fields. Choose this option to indicate you only want to update the custom fields you specify.</p> <p>To specify the fields you want to update, see Select specific custom fields to import.</p> <p>Always update object custom fields. Choose this option to indicate you always want custom fields and their values in the file to be imported into AppViz.</p> <p>This option is not available when updating objects directly from a CMDB.</p> <p>This option is relevant when the file contains a comprehensive list of all the custom fields you want in AppViz.</p> <p>Note: Objects with the status In Change Process or Rejected will never be updated.</p>

For this setting...	Do this...
Update Affected Applications settings	<p>Select one of the following:</p> <ul style="list-style-type: none"> <p>Update the affected applications automatically. Choose this option to indicate you want AppViz to automatically update all affected applications.</p> <p>This option will automatically create a change request in FireFlow to allow/drop any traffic that is required as a result of the object update.</p> <p>This is the default behavior.</p> <p>Do not update the affected applications automatically. Choose this option to indicate you do not want AppViz to automatically update affected applications.</p> <p>If you select this option, the revision of the object in use for the affected applications is designated as outdated. When this is the case,  Some applications are not updated with this object's last revision appears in the upper right corner of the object's page. Additionally,  appears on the object's icon in any application flows or projects using the outdated revision. After running the import, AppViz provides the option to update outdated definitions for all an object's applications. For more details, see Business applications.</p>

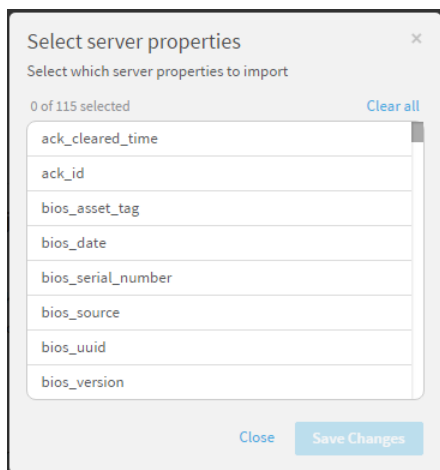
Select specific custom fields to import

Use this procedure while managing the import settings for an object update from a CSV file or CMDB.

To select specific custom fields to import:

1. In the **Custom fields** area, click **selected fields**.

Depending on whether you are managing settings for CSV file updates or updates directly from a CMDB, either the **Select custom fields** or **Select server properties** dialog box appears.



2. Select the custom fields or server properties to import as custom fields.
3. Click **Save Changes**.

Reviewing the last object update

You can view the results of the last update of device objects, objects from a file, or objects directly from a CMDB.

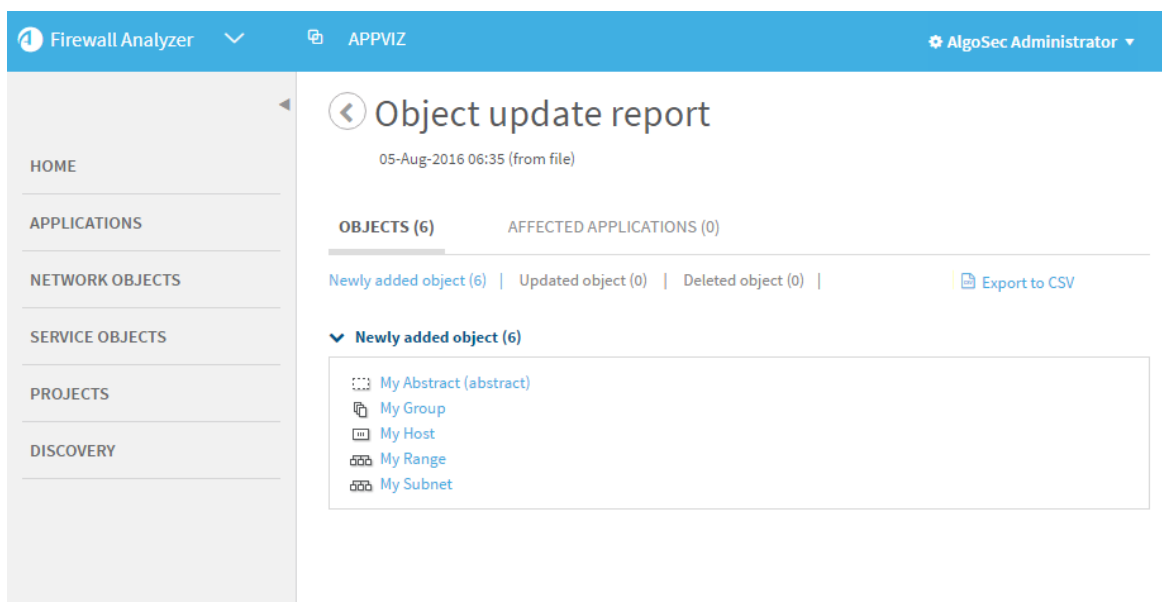
Note: These results contain information only for network objects, not service objects.

To review the last object update:

1. In the toolbar, click your username.
A drop-down list appears.
2. In the drop-down list, select **Administration**.
The **Administration** page appears in the workspace.
3. Click the **Objects Update** tab.
The **Objects Update** tab appears.
4. Do one of the following:
 - To view the last report for device objects, in the **Update Device Objects** area, click **Review**.

- To view the last report for objects from a file, in the **Update Objects from file** area, click **Review**.
- To view the last report for objects imported directly from a CMDB, in the **Update Objects from CMDB** area, click **Review**.

The **Object update report** appears displaying the **Objects** tab.



Note: The relevance of the objects or applications in each tab is dependent on the update settings. For example, if affected applications are not updated automatically, no applications will appear in the affected applications tab.

Note: Some or all of the sub tabs may appear, depending on the settings configured for the update.

Within the **Objects** tab, all of the objects are sorted into the following sub-tabs:

- **Newly added object.** This tab includes all objects that were added to AppViz as a result of the update.

- **Updated object.** This tab includes all objects whose definition changed as a result of the update.
- **Deleted object.** This tab includes all objects that were deleted from AppViz as a result of the update.
- **Could not be deleted.** This tab includes objects that the import attempted to delete from AppViz, but could not delete because they are used in the current revision of at least one application.
- **Could not be updated due to object status.** This tab includes objects that the import attempted to update, but could not update because of the object's change status.
- **Were not updated due to current settings.** This tab includes objects that were not updated because of the settings you specified before the update.

Clicking on any object brings you to the object's AppViz page.

5. To view a list of applications which were affected by the object import, click the **Affected Applications** tab.

Clicking on any application brings you to the application's AppViz page.

6. To export the report as a CSV file, click  [Export to CSV](#).

Schedule update of network objects fields

In this field...	Do this...
Enable scheduler for updating server definitions	Check this check box to enable scheduling updates.
Period	In the drop-down menu, select either Daily or Weekly as the period for the updates.
Time	Using the two drop-down menus, specify the time of day on the 24 hour clock for the updates.

Configure advanced AppViz properties

This topic describes the advanced configuration available for AppViz in the `user.properties` file on the AppViz server.

Access and edit the `user.properties` file

The `user.properties` AppViz configuration file is located on the AppViz server, at `/home/bflow/config/user.properties`.

Do the following:

1. Open a terminal and log in to the AppViz server as user `root`.
2. Browse to an open `/home/bflow/config/user.properties` for editing.
3. Add or edit configuration parameters as needed. If the parameter is missing, add the parameter name and value on a new line.

For details, see [Advanced AppViz property reference](#).

4. When you're finished, save the file and restart AppViz. For more details, see [Restart AppViz](#).

Advanced AppViz property reference

This section describes the advanced AppViz properties available for editing in the `user.properties` file.

For details, see:

- [advanced-search.results.page_size](#). Defines the number of impact analysis results shown by default.
- [application.recent.page_size](#). Defines the number of recent applications displayed in the applications menu.
- [change_requests.disable](#). Determines whether AppViz is disabled from handling change requests, including all change request creations and all change request-related tabs.

- [changerequest.status.resolved](#). Defines the FireFlow change request statuses for which you want to trigger AppViz status changes.
- [connectivity.enable](#). Determines whether application status is constantly refreshed.
- [discovery.max_flows_per_application](#). Determines the maximum number of flows combined per application during a discovery process.
- [discovery.minimum_density](#). Defines the minimum percentage of the IP addresses found in a specific CIDR, for the CIDR to be suggested as a source/destination value.
- [fireflow.objects.add_firewall_suffix](#). Determines whether AppViz opens change requests in FireFlow for specific device objects by adding the device name to the object in the source/destination value.
- [fireflow.objects.always_pass_content](#). Determines whether AppViz passes the names or content of the network objects when opening change requests in FireFlow.
- [fireflow.services.always_pass_content](#). Determines whether AppViz passes the names or content of the service objects when opening change requests in FireFlow.
- [flow.connectivity.display_unprotected](#). Determines whether AppViz differentiates between traffic that is explicitly allowed by a rule and traffic that is allowed because it is unprotected or unfiltered.
- [flow.connectivity.export](#). Determines whether flow connectivity data is exported together with an application's flows.
- [import.delimiter](#). Determines the delimiter used in CSV import files.
- [import.encoding](#). Defines the encoding used for imported files.
- [network_entity.origin.order](#). Determines the order of preference used when optimizing network objects from different sources.

- [object_workflow.enabled](#). Determines whether AppViz is enabled to define device object definitions on the device using AppChange.
- [permissions.initial](#). Determines the permissions granted by default to all AppViz users.
- [permissions.initial.afa_user](#). Determines the permissions granted by default to AFA-only users.
- [risk.enable](#). Determines whether risk checks are run automatically when a pending revision becomes active.
- [security_zones.default_internal_network_ranges](#). Defines the internal/private zone networks.
- [shared_flows.subscription.actions_ownership](#). Determines ownership of shared flows, which are general or partial flows that may be relevant to many applications.
- [upload.max_size](#). Determines the maximum upload size, in MB.

upload.max_size

Integer. Determines the maximum upload size, in MB.

For example:

```
upload.max_size=100
```

connectivity.enable

Determines whether application status is constantly refreshed.

- **True.** (Default) Enables constant application refreshes.
- **False.** Disables constant application refreshes.

Tip: Use together with [risk.enable](#) to enable automatic data refreshes.

risk.enable

Determines whether risk checks are run automatically when a pending revision

becomes active.

- **True.** (Default) Enables automatic risk checks.
- **False.** Disables automatic risk checks.

Tip: Use together with [connectivity.enable](#) to enable automatic data refreshes.

permissions.initial

String. Determines the permissions granted by default to all AppViz users.

Separate multiple values with commas.

For example, the following sets the initial permissions for all users to create applications and view all applications:

```
permissions.initial=ROLE_CREATE_APPLICATION,ROLE_VIEW_ALL_APPLICATION
```

For more details, see [AppViz permission reference](#).

Default values:

All users	Default permissions for all users include: <ul style="list-style-type: none"> • Create applications • Update vulnerability • Edit network objects • Edit service objects
Privileged users	Privileged users have additional permissions to update risk information by default.
Administrators	Administrator users receive all permissions by default.

permissions.initial.afa_user

Determines the permissions granted by default to AFA-only users.

For example, the following sets the initial permissions for AFA users to view risk information and update vulnerability information:

```
permissions.initial.afa_user=ROLE_VIEW_RISK,ROLE_UPDATE_VULNERABILITY
```

For more details, see [AppViz permission reference](#).

AppViz permission reference

Permission name	Permission to...
ROLE_CREATE_APPLICATION	Create new applications.
ROLE_UPDATE_VULNERABILITY	Update vulnerability
ROLE_EDIT_NETWORK_OBJECTS	Edit network objects.
ROLE_EDIT_SERVICE_OBJECTS	Edit service objects.
ROLE_VIEW_ALL_APPLICATION	View all applications.
ROLE_EDIT_ALL_APPLICATION	Edit all applications.
ROLE_EDIT_APPLICATION_INFORMATION	Edit application custom fields, labels, and contacts.
ROLE_CREATE_APPLICATION	Create a new application.
ROLE_VIEW_CONNECTIVITY	View connectivity.
ROLE_UPDATE_CONNECTIVITY	Update connectivity.
ROLE_VIEW_VULNERABILITY	View vulnerability information for applications.

Permission name	Permission to...
ROLE_VIEW_ACTIVITY_LOG	View activity log information for applications and network objects.
ROLE_VIEW_CHANGE_REQUESTS	View change request information for applications, network objects, and service objects.
ROLE_CREATE_LABELS	Create labels.
ROLE_UPDATE_VULNERABILITY	Update vulnerability information.
ROLE_APPLY_DRAFT	Apply application drafts.
ROLE_CREATE_SHARED_FLOWS	Create a shared flow.
ROLE_UPDATE_RISK	Update risk information.
ROLE_VIEW_RISK	View risk information.
ROLE_SYNC_OBJECT	Run an update process for a device object.

discovery.max_flows_per_application

Integer. Determines the maximum number of flows combined per application during a discovery process.

Default: 50

For example, the following sets the default value to 60 flows:

```
discovery.max_flows_per_application=60
```

Tip: The larger the number of maximum flows per application, the more specific each flow will be. The smaller the maximum number of flows per application, the more AppViz will optimize and combine flows.

network_entity.origin.order

String. Determines the order of preference used when optimizing network objects from

different sources.

During discovery, if more than one network object is found with the same name, AppViz selects the object to use based on origin preference configured.

Supported values	Source values include: <ul style="list-style-type: none"> • BusinessFlow. Objects created in AppViz • Imported. Objects imported from a discovery server or a CSV file. • Device. Objects from an AFA device.
Default value	Imported, BusinessFlow, Device

For example, the following sets the priority sequence to BusinessFlow, Imported, Device :

```
network_entity.origin.order=BusinessFlow,Imported,Device
```

Note: Network objects that originate from the same place cannot have the same name, except for device objects. If two device objects with the same name (but different content) exist, the CSV file validation will fail.

If two device objects defined on different devices have the same name and the same content, AppViz will treat them as one object and validation will succeed.

discovery.minimum_density

String. Defines the minimum percentage of the IP addresses found in a specific CIDR, for the CIDR to be suggested as a source/destination value.

This is relevant for the optimization process performed during discovery from traffic logs.

Supported values	<p>Supported values include:</p> <ul style="list-style-type: none"> • Integer between 0 and 1. Indicates a static minimum percentage. For example, .4 sets the minimum density to a static 40%, regardless of CIDR size. • auto. Determines that AppViz determines the optimum density automatically, depending on the size of the CIDR. Larger CIDRs require less density.
Default value	<p>0.3</p> <p>This value determines that by default, the IP addresses in the traffic logs must be at least 30% of the CIDR to be suggested as a source/destination value.</p>

flow.connectivity.export

Boolean. Determines whether flow connectivity data is exported together with an application's flows.

- **True.** Connectivity data is exported together with the flows.
- **False.** (Default) No connectivity data is exported.

When configured , exported connectivity data includes any of the following values:

- **Allowed**
- **Blocked**
- **Partially blocked**
- **No connectivity information**
- **Unprotected.**

Note: **Unprotected** appears only when AppViz is configured to detect unprotected flows.

Otherwise, all allowed traffic is assigned the **Allowed** value. For details, see [flow.connectivity.display_unprotected](#).

import.encoding

String. Defines the encoding used for imported files.

Default value: **UTF-8**

import.delimiter

String. Determines the delimiter used in CSV import files.

Default value: , (comma)

For example, change this to a colon if needed:

```
import.delimiter=:
```

flow.connectivity.display_unprotected

Boolean. Determines whether AppViz differentiates between traffic that is explicitly allowed by a rule and traffic that is allowed because it is unprotected or unfiltered.

Supported values:

- **True.** AppViz differentiates between explicitly allowed traffic and unprotected/unfiltered traffic.
- **False.** (Default). AppViz does not differentiate between allowed traffic types.

For example, you may want to enable this feature when using micro-management within subnets.

```
flow.connectivity.display_unprotected=true
```

When configured, AppViz indicates this in the **FLOWS** tab as follows:

- All allowed flows appear with a green connectivity indicator.
- All unprotected flows appear with a striped indicator.

For example:



Additionally, this information is available in:

<p>Flow exports / API responses</p>	<p>When AppViz provides connectivity information about flows, the values will specify whether the flow is "allowed" (protected) or "unprotected".</p> <p>Note: By default, AppViz does not include connectivity information in flow exports.</p> <p>For details, see flow.connectivity.export and Export flows directly from AFA.</p>
<p>Application search abilities</p>	<p>When performing an advanced search for applications By Connectivity, you will have the option to specify whether to search for applications with allowed flows that are protected or allowed flows that are unprotected.</p> <p>For more details, see Business applications.</p> <p>Note: Unprotected flow detection has no impact on <i>application</i> connectivity status, only <i>flow</i> connectivity status.</p> <p>An application whose flows are all allowed (protected or unprotected) will always have the connectivity status Allowed.</p>

shared_flows.subscription.actions_ownership

String. Determines ownership of shared flows, which are general or partial flows that may be relevant to many applications.

Note: Shared flows specify only a source or destination, leaving the remaining field

only with a placeholder value. When an application subscribes to another application's shared flows, the subscribing application specifies a value for the placeholder.

Supported values include:

sharingApplication (Default)	<p>Determines that the application with the shared flows is defined as the flow owner.</p> <p>Editing a shared flow or a subscribed flow creates an application draft for the application with the shared flow.</p>
combined	<p>Determines that ownership is shared across several applications.</p> <ul style="list-style-type: none"> • Editing a shared flow creates a draft for the application with the shared flow. • Editing a subscribed flow's placeholder value creates a draft for the subscribed flow. <p>The application with the shared flow and the application with the subscribed flow will both reflect the risks, connectivity, etc., derived from the subscribed flow.</p> <p>Note: When a change is pending for traffic relevant to a shared or subscribed flow, the flows cannot be edited, deleted or added in any application.</p>

For more details, see [Application flows](#).

security_zones.default_internal_network_ranges

A semi-colon delimited list of networks, in CIDR format. Defines the internal/private zone networks.

Default value: 10.0.0.0/8;172.16.0.0/12;92.168.0.0/16

For example, the following sets the internal zone to 172.16.0.0/12 and 92.168.0.0/16:

```
security_zones.default_internal_network_ranges=172.16.0.0/12;192.168.0.0/16
```

application.recent.page_size

Integer. Defines the number of recent applications displayed in the applications menu.

Default value: 10

advanced-search.results.page_size

Integer. Defines the number of impact analysis results shown by default. Click **Load more applications....** to view more.

For example, the following sets the number of applications to display in the impact analysis results to 15:

```
advanced-search.results.page_size=15
```

changerequest.status.resolved

Comma-separated list. Defines the FireFlow change request statuses for which you want to trigger AppViz status changes.

By default, pending statuses for objects and applications in AppViz transition to their next status once FireFlow change requests reach the **reconcile**, **pending match**, or **resolved** statuses.

For example, the following sets the AppViz status to change when the FireFlow change request reaches the **pending match**, **matched** or **resolved** status:

```
changerequest.status.resolved=pending match,matched,resolved
```

change_requests.disable

Boolean. Determines whether AppChange is disabled from handling change requests, including all change request creations and all change request-related tabs.

Supported values:

- **True.** Change requests are disabled from AppChange
- **False.** Change requests are enabled in AppChange

fireflow.objects.add_firewall_suffix

Boolean. Determines whether AppChange opens change requests in FireFlow for specific device objects by adding the device name to the object in the source/destination value.

Supported values:

- **True.** AppChange appends the device name to the object in the source/destination.
- **False.** AppChange does not append the device name to the object.

Note: This feature must be used together with the **Set (\$StoreFirewallSuffixInHostGroup, '1')**FireFlow command.

fireflow.objects.always_pass_content

Boolean. Determines whether AppChange passes the names or content of the network objects when opening change requests in FireFlow.

Supported values:

- **True.** AppChange passes the content of the network objects.
- **False.** (Default) AppChange passes the network object name.

fireflow.services.always_pass_content

Boolean. Determines whether AppChange passes the names or content of the service objects when opening change requests in FireFlow.

Supported values:

- **True.** AppChange passes the content of the service objects.
- **False.** (Default) AppChange passes the service object name.

object_workflow.enabled

Boolean. Determines whether AppViz is enabled to define device object definitions on the device using AppChange.

Supported values:

- **True.** Enables AppViz to define device object definitions on the device.
- **False.** Disables the ability for AppViz to define device object definitions on the device.

Device objects

By default, AppViz does not change device object definitions on the device. When you edit a network or service object that is a part of an application's flows, regardless of whether the object originated from AppViz, an import, or a device, AppViz initiates a *traffic change* request to adjust the traffic that is required for the application as a result of the object's new definition in AppViz. When an object that is not used in an active application is edited in AppViz, no change request opens. Additionally, AppViz will not permit deleting a device object, even when it is not used in an application.

Manage device objects in AppViz

If desired, you can enable AppViz to manage device network object definitions on the device via the AppChange plugin. This will allow you to edit and delete device network objects directly from AppViz. AppChange initiates FireFlow *object change* request (using the Multi Device Object Change Request workflow) whenever a device network object is edited or deleted.

Note: This feature is only for *network* objects, not service objects. When this feature is configured, network objects will be changed on the device using an object change request, but service objects will still be changed using a traffic change request.

Enabling this feature has no affect on service objects at all.

Note: This feature does not affect AppViz's handling of objects which originated in AppViz, objects which originated from a CSV or CMDB import, or objects that originated on a device but are no longer defined on a device.

When this feature is enabled, the following occurs:

- AppChange will open a FireFlow object change request to change the definition of the object on the device every time a device object is edited, regardless of whether the object is being used in an application's flows.

- AppChange will allow deleting device objects and will open a FireFlow object change request to delete the objects from their device(s).
- AppChange will not allow adding invalid members to device groups.
- If you attempt to add a member to a group object where the member is defined on some, but not every device the group is defined on, AppViz provides the following options:
 - Creating the member object on the device(s) on which only the group is defined and then adding the member to the group.
 - Splitting the group into two groups in AppViz. AppChange will add the new member to the group on the devices on which the member is defined. For devices on which the member is not defined, the group will maintain its original definition (without the new member).
- If you attempt to add a member to a group object where the group is defined on some, but not every device the member is defined on, AppChange will only modify the group on the devices where the group is defined. The devices where only the member is defined will not be modified.

For more details, see:

- [Edit device objects](#)
- [Update all device objects](#)
- [Configure advanced AppViz properties](#)

Edit device objects

This topic describes how editing device objects from AppViz.

Device editing process

When AppViz is configured to change device objects on the device via AppChange, the following occurs when a device object is edited:


- An object change request opens in FireFlow to modify the object(s). Multiple objects may be added or created when editing a group object.
- The object's change status becomes **In Change Process**. For information, see Device Object Change Statuses (see [Device object change statuses](#)).
- The applications using the object are automatically and immediately updated with the new object value. AppChange immediately uses the new definition without waiting for the change request to be resolved.
- If the change request is resolved in FireFlow, the object leaves the **In Change Process** change status.
- If the change request is rejected in FireFlow, the object leaves the **In Change Process** change status and the object's change status becomes **Rejected**.

Note: The applications using the object stay active throughout the whole process. No new application revisions are created; only the object's status changes.

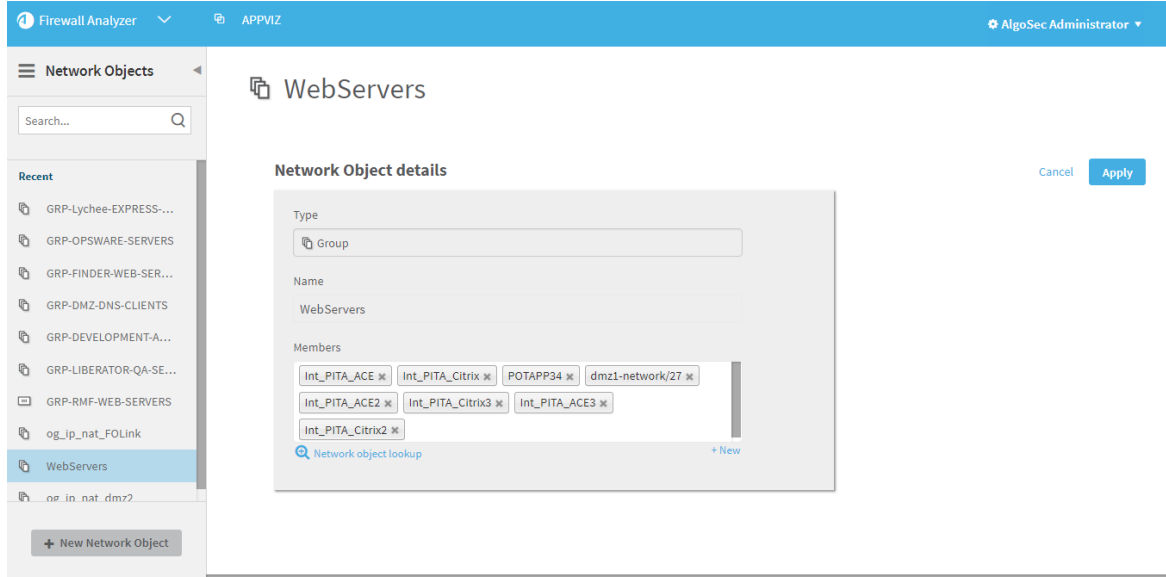
Note: You cannot edit objects which you do not have permission to edit. Additionally, the following objects cannot be edited by anyone:

- Objects that are in use by an application for which you do not have permissions
- Objects that are involved in a pending application. For example if you change an application to include a new object, and the application is now pending implementation, you cannot edit that object.
- Objects that are part of a group that currently has the **In Change Process** status.

Edit a device object from AppViz

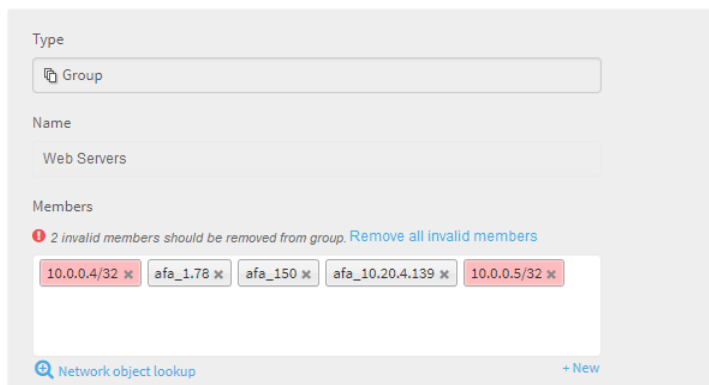
1. View the object you want to edit. For details, see [View a network object](#).
2. In the **Actions** area of the **Dashboard** tab, click .

The **Object details**, and if relevant, the **Affected Applications** appear.



The **Affected Applications** area lists the applications that contain the object. You can view the affected flows by clicking [➤](#).

If the object you are editing is a group object with invalid members, all invalid members appear in red.



3. Edit the fields you desire. For details, see [Add and edit network objects](#).

Note: If a device group contains invalid members, you must delete these members before applying a change to the object. For details, see [Manage](#)

[groups with invalid members.](#)

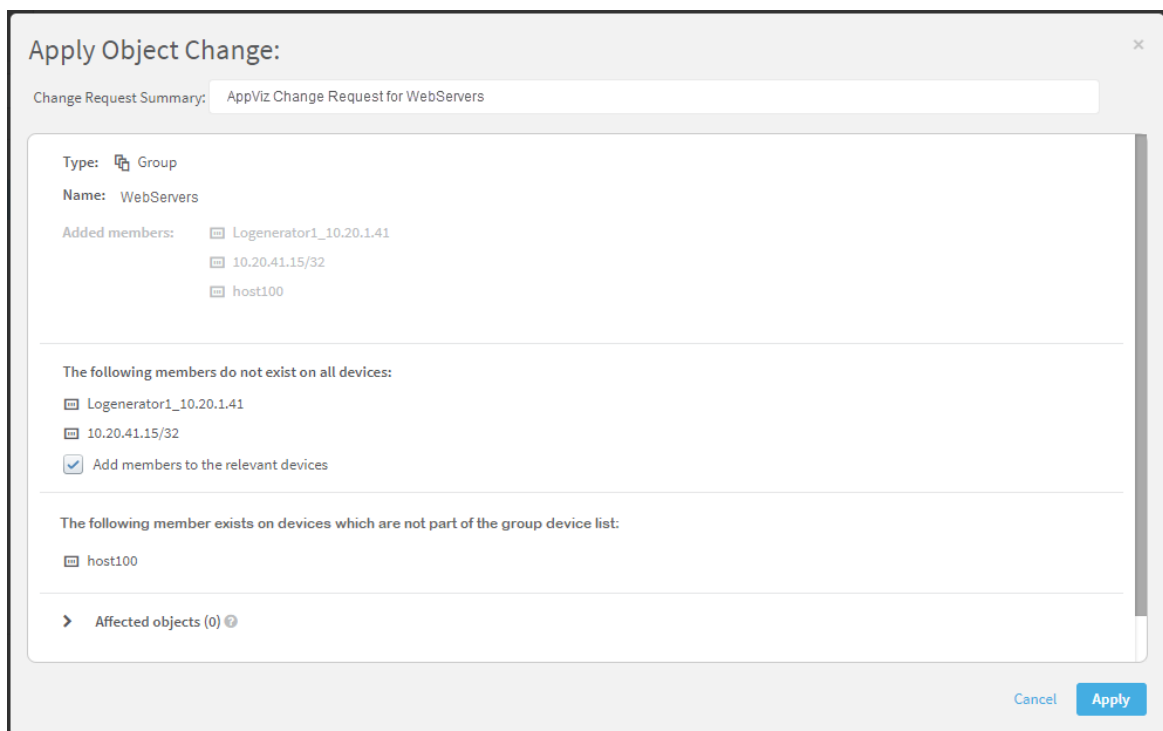
Note: You cannot edit the name.

Note: If you are adding a new network object as a member of a group, the change request that modifies the object you are editing will also create the new object on the device. For details, see [Manage objects pending creation](#).

Note: You can only add an object as a member of a device group when the object is a device object whose device list intersects the device list of the group.

4. Click **Apply**.

The **Apply Change** dialog box appears.



The dialog box displays the type, name, definition, and former definition of the device object. The affected applications and affected objects appear at the bottom. Affected objects include any object that contains the object being edited or contain an object containing the object being edited.

If one or many members you added to a group do not exist on all the devices on which the group is defined, these members are listed in the dialog box and the **Add Members to Relevant Devices** check box appears.

If one or more members you added to a group exist on devices on which the group is not defined (members that are not a part of the group's device list), the dialog box lists the objects. This list is simply informational; none of these devices will be modified.

5. If the **Add Members to Relevant Devices** check box appears, do one of the following:
 - Leave the check box marked to indicate you want to define the member object(s) on the device(s) on which only the group is defined and then add them to the group.
 - Clear the check box to indicate you do not want to define the members on the devices on which only the group is defined. AppChange will add the new member(s) to the group on the device(s) on which the member(s) are defined. For devices on which the member(s) are not defined, the group will maintain its original definition, without the new member(s).

6. Click **Apply**.

The object change request editing the object(s) is created, the object(s) are updated by AppChange.

Synchronize device object definitions


Updating a device object will synchronize the definition of the object in AppViz with the definition on the device. The object, its members, and its containing objects will all be updated.

This action will appear as an option when the following are true:

- The object is a device object which is currently defined on a device.
- The object does not have a change status (**Rejected**, **In Change Process**, etc.).
- The user has permission to edit the object and permission to update objects from the device. For details, see [AppViz users, permissions, and roles](#).

Note: You can optionally update all of AppViz 's device objects at once. For details, see [Update all device objects](#).

To update device objects:

1. View the object you want to edit. For details, see [View a network object](#) or [Service objects](#).
2. In the **Actions** area of the **Dashboard** tab, click .

The object is updated.

Delete a device object

When AppChange is configured to change device objects on the device, you can delete device network objects.

Note: You cannot delete objects that are currently in use in an application, a member of a group object, or in use in a project with the status **In Progress**. Additionally, you must have permission to edit the object.

The following occurs when a device object is deleted:

- An object change request opens in FireFlow to delete the object.
- The object's change status becomes **Pending Deletion**. For details, see [Device object change statuses](#).
- If the change request is resolved, the object will be deleted from its devices and


from AppViz. The object's history will still be visible in the activity logs in the administration area. For more details, see [Application activity log](#).

Note: Be careful to not resolve the change request in FireFlow until the change on the device is actually implemented. As soon as the change request is resolved, AppViz deletes the object. If the object is actually still defined on the device, the next device object update will automatically re-create the device object in AppViz.

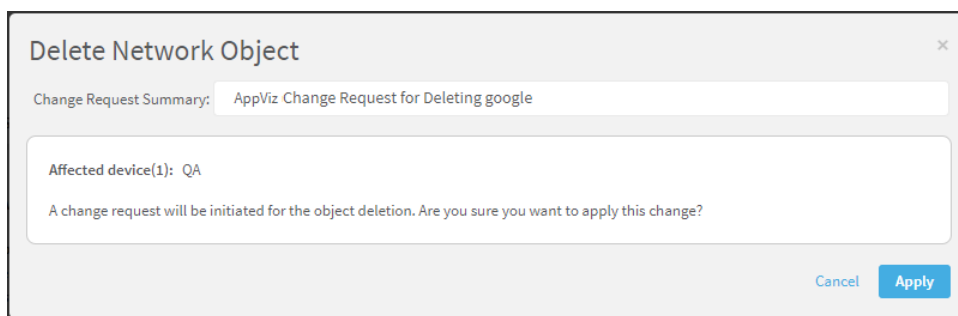
- If the change request is rejected, the object leaves the **Pending Deletion** change status and the object's change status becomes **Rejected**.

Note: If the object is already deleted from the device, there is no need to complete this procedure. Updating AppViz with the current device object information will automatically remove the device from AppViz. If you try to use this procedure to delete an object that is already deleted on the device, change request creation will fail. For more details, see [Update all device objects](#).

To delete a device object:

1. View the object you want to delete. For details, see [View a network object](#).
2. In the **Actions** area of the **Dashboard** tab, click .

The **Delete Network Object** dialog box appears.



The dialog box displays the affected devices.



3. Click **Apply**.

The object change request deleting the object is created and the object's status changes to **Pending Deletion**.

Device object change statuses



When AppChange is configured to manage device objects on their devices, device network objects may have one of the following change statuses:

- **In Change Process.** The object's definition in AppViz has been updated, and the FireFlow object change request to modify the object is pending.

When an object has this change status,  appears in the upper right corner of its page. Additionally,  appears on the object's icon in any application flows, projects, or discovery processes.



Objects in change process cannot be edited, used in projects or included in discovery from traffic logs. They can be used in flows.

- **Pending Deletion.** The **Delete** action has been performed on the object, and the FireFlow object change request to delete the object is pending.

When an object has this change status,  appears in the upper right corner of its page. Additionally, the object appears grayed out and with  on its icon in any projects or discovery processes.

Objects pending deletion cannot be edited, added as members of group objects, added to application flows, added to projects, or added to a discovery process.


- **Rejected.** The object was in change process, and its FireFlow change request was rejected.

When an object has this change status,  appears in the upper right corner of its page. Additionally,  appears on the object's icon in any application flows, projects, or discovery processes.

If the object change request for an object **Pending Deletion** is rejected, the object will not be given the **Rejected** change status. The **Pending Deletion** change status will simply be removed from the object, leaving the object with no change status.





Objects with the **Rejected** change status cannot be edited, used in projects, included in discovery from traffic logs or used in flows.

- **Pending Creation.** The object has been created in AppViz, and the FireFlow object change request to create the object is pending.

When an object has this change status,  appears in the upper right corner of its page. Additionally, the dashboard will include the **Status Details** tab, which specifies the details of the object's creation and its relationships with other objects.

Objects in this change status are the result of adding a member to a group network object that does not yet exist. For more information, see [Managing Objects Pending Creation](#) (see [Manage objects pending creation](#)).

Some objects may have a notification that is not related to change status, but because it is in one of the following problematic scenarios:

- Group objects with invalid members. When this is the case,  appears in the upper right corner of its page and  appears next to the problematic member in the dashboard. For more details, see [Manage groups with invalid members](#).
- Objects with outdated revisions being used in applications. When this is the case,  appears in the upper right corner of its page and  appears on the object's icon in any application flows or projects using the outdated revision. This situation can only occur as the result of an import when the **Do not update the affected applications automatically** option is chosen. For more details, see [AppViz maintenance](#) and [Business applications](#).

Note: Objects with a change status are not affected by AppChange device object updates.

Note: For information about the standard network object change statuses, see [Network object dashboard](#). When AppViz manages objects with its default setting, these statuses are relevant to all network objects. When AppChange is configured to manage device objects on their devices, the standard statuses are relevant to network objects created in or imported into AppViz (not device objects).

Customize FireFlow object change requests

Use this procedure to customize the change requests opened as the result of editing an object in AppViz when AppChange is configured to change the definition of device objects on the device. This includes the following types of change requests:

- Traffic change requests opened as the result of changing an object in AppViz that is not defined on a device.
- Object change requests opened as the result of changing a device object in AppViz.

Note: To customize traffic change requests that are opened as the result of changing an application, see [Customize interactions with AFA and FireFlow](#).

To manage object change request behavior:

1. In the toolbar, click your username.
A drop-down list appears.
2. In the drop-down list, select **Administration**.
The administration page appears in the workspace.

3. Click **Customization**.

The **Customization** tab appears.

4. In the **FireFlow Change Request Definitions** area, next to **Manage object change requests**, click **Manage**.

The **FireFlow Object Change Requests** page appears, displaying the **OBJECT WORKFLOW** tab.

The screenshot shows the 'FireFlow Object Change Requests' configuration page. The page has a blue header with 'Firewall Analyzer' and 'APPVIZ' on the left, and 'Admin admin' on the right. A left sidebar contains navigation options: HOME, APPLICATIONS, NETWORK OBJECTS, SERVICE OBJECTS, PROJECTS, and DISCOVERY. The main content area is titled 'FireFlow Object Change Requests' and includes a 'Cancel' button and a 'Save Changes' button. Below the title, there is a note: 'Object workflow functionality is currently on. Define device object settings in the object workflow tab, and non-device objects settings in the traffic workflow tab.' There are two tabs: 'OBJECT WORKFLOW' (selected) and 'TRAFFIC WORKFLOW'. Under the 'OBJECT WORKFLOW' tab, there are three input fields: 'Request Template' (a dropdown menu showing '135: Object Change Multi Device Request'), 'Object Change Default Summary' (a text field containing 'BusinessFlow Change Request for {ObjectName}'), and 'Object Delete Default Summary' (a text field containing 'BusinessFlow Change Request for Deleting {ObjectName}'). Below these fields is a 'Template Fields' section with a 'CHANGE REQUEST' field and a note: 'Set default values to FireFlow change request custom fields. Add field to begin.' There is an 'Add Field' button to the right of the note.

5. To customize object change requests opened for device objects (using an object change workflow), do the following:


- a. In the **Request Template** drop-down menu, select the FireFlow traffic change request template to use.
- b. In the **Object Change Default Summary** field, type the default subject to use. You can optionally include the variable `{ObjectName}` to indicate the relevant object's name.
- c. In the **Object Delete Default Summary** field, type the default subject to use. You can optionally include the variable `{ObjectName}` to indicate the relevant object's name.

- d. (Optional) To map the values of AppViz fields to FireFlow change request custom fields, continue completing the fields. For details, see [Customize interactions with AFA and FireFlow](#).
6. To customize object change requests opened for objects that are not defined on a device but are used in applications (using a traffic change workflow), do the following:
 - a. Click the **TRAFFIC WORKFLOW** tab.
 - b. In the **Request Template** drop-down menu, select the FireFlow traffic change request template to use.
 - c. In the **Object Change Default Summary** field, type the default subject to use.
You can optionally include the variable `{ObjectName}` to indicate the relevant object's name.
 - d. (Optional) To map the values of AppChange fields to FireFlow change request custom fields, continue completing the fields. For details, see [Customize interactions with AFA and FireFlow](#).
7. Click **Save Changes**.
A confirmation message appears.
8. Click **OK**.

Manage groups with invalid members

When AppChange is configured to manage device objects on the devices on which they are defined, the following objects are invalid as members of device groups:

- An object that originated from AppViz, originated from a CSV/CMDB import, or is otherwise not defined on any device.
- A device object that is not defined on any of the same devices as the group device object.

If you added any of these objects to device groups while AppViz was configured to adjust for object changes by modifying the *traffic* required for applications (the default behavior), some groups will have invalid members once you enable managing device objects on the device(s). Group objects with invalid members are indicated with **Invalid Group Members** in the upper right corner of their page. Additionally,  appears next to the problematic member in the dashboard.

Once you enable managing device objects on their devices, AppViz requires you to remove invalid members before you can apply a change to the object. When you edit an object with invalid members, all invalid object members appear in red.



Note: Removing invalid members from a group will not trigger or impact a change request as these changes were never implemented on the device.

Manage objects pending creation

When you add a new network object as a member of a group, the change request that modifies the object you are editing will also create the new object on the device. The new object will automatically be created in AppViz and will be assigned the **Object Pending Creation on the Device** status.

Note: For more information about device object statuses and how they are indicated in the Web Interface, see [Device objects](#).

AppViz handles these objects in the following ways:

- While the object is pending creation, it cannot be used in an application flow. Additionally, like all objects with outstanding change requests, it cannot be edited, used in a project, or used in a discovery search from traffic logs.
- If the change request creating the object is resolved, the object becomes a normal device object in AppViz.
- If the change request creating the object is rejected, you have the option to re-apply the object or discard it (like all rejected applications). Additionally, like all other rejected objects, it cannot be used in an application, project, or discovery search from traffic logs.
- If the object is discarded, it is deleted completely from AppViz. The object's only purpose was to be a member of the group for which it was created.

Update all device objects

You can update all device objects in AppViz with the current information from AFA. This includes all network objects, service objects, and network applications for every device in AFA. You can do this manually or schedule updates to occur periodically.

Additionally, you can review the results of the last update. For details, see [Edit device objects](#).

Note: Only device objects without a change status are affected by AppViz device object updates. Objects that are in change process, pending deletion, pending creation or rejected are not affected by an update.

Note: You can optionally update device objects from the CLI. For details, see [Update all device objects from \(CLI\)](#).

Update all device objects (GUI)

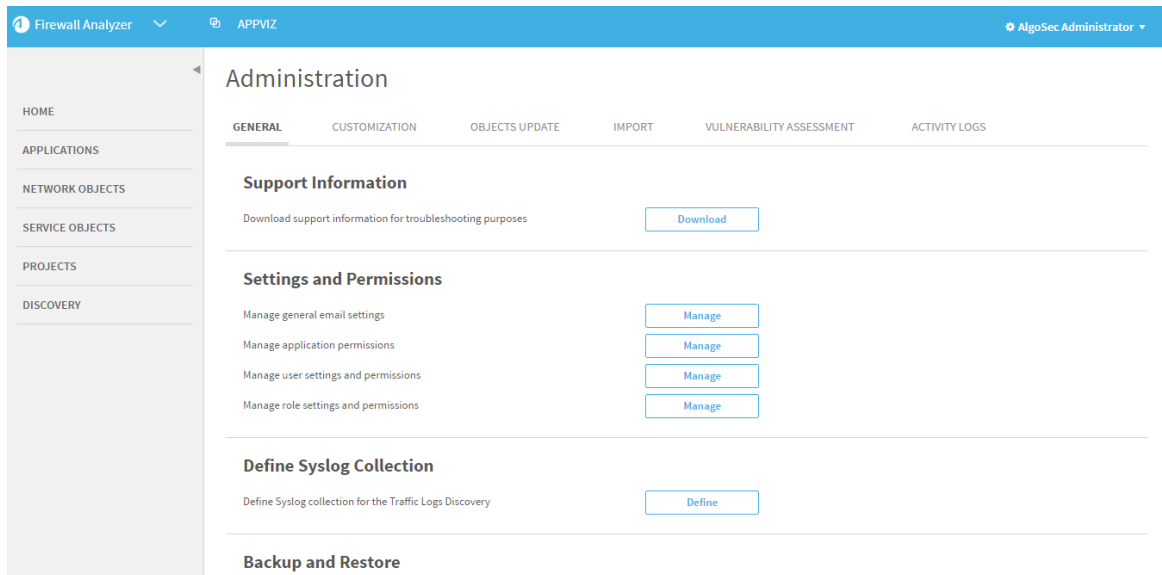
Do the following:

1. In the toolbar, click your username.

A drop-down list appears.

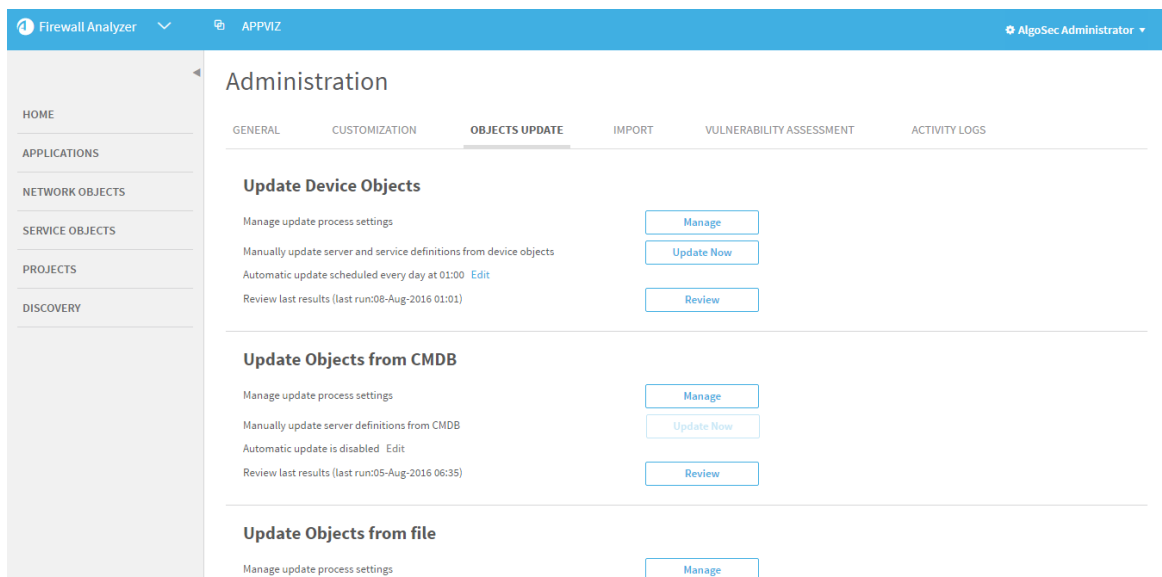
2. In the drop-down list, select **Administration**.

The **Administration** page appears in the workspace.



3. Click the **Objects Update** tab.

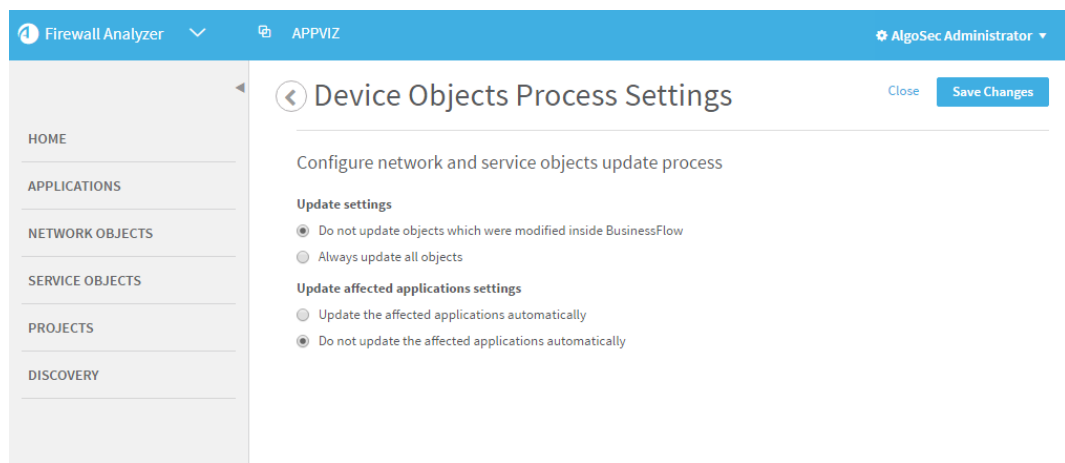
The **Objects Update** tab appears.



4. To configure the behavior of the update, do the following:

- a. In the **Update Device Objects** area, click **Manage**.

The **Device Objects Update Settings** page appears.



- b. Under **Update settings**, select one of the following options:

- **Do not update objects which were modified inside AppViz.** Choose this option if you do not want the changes users have made to device objects in AppViz to be overwritten with the update.

This is the default behavior.

- **Always update all objects.** Choose this option if you want all device objects in AppViz to be updated to the current definition in AFA.

- c. Under **Update Affected Applications settings**, select one of the following options:



- **Update the affected applications automatically.** Choose this option if you want all applications containing flow with device objects to be updated with the new device object values.

This is the default behavior.

This option will automatically create a change request in FireFlow to modify any traffic affected by the object update.

- **Do not update the affected applications automatically.** Choose this option if you do not want to automatically update any applications containing device objects whose values have been updated.

If you select this option, the revision of the object in use for the affected applications is designated as outdated. When this is the case,

 appears in the upper right corner of the object's page. Additionally,  appears on the object's icon in any application flows or projects using the outdated revision. After running the import, AppViz provides the option to update outdated definitions for all an object's applications. For more details, see [Business applications](#).

- d. Click **Save Changes**.

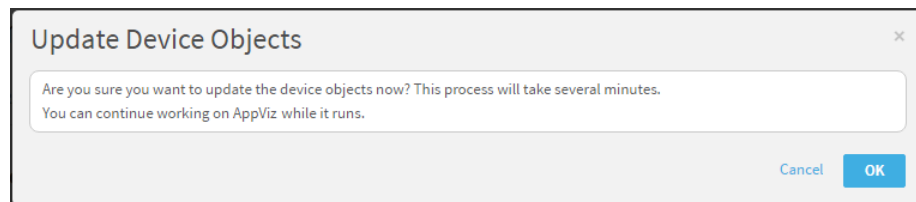
A confirmation message appears at the top of the workspace.

Note: Regardless of the configuration, objects that are in change process or rejected will not be updated.

5. In the **Update Device Objects** area, do one of the following:

- To manually update device objects, do the following:
 1. Click **Update Now**.

The **Update Device Objects** dialog box appears.



2. Click **OK**.

The device objects are updated.

- To schedule automatic updates, do the following:

1. Click **Edit**.

The **Schedule Update of Device Objects** dialog box appears.



2. Complete the fields using the information in [Scheduled update of device object fields](#).
3. Click **Save Changes**.

The automatic updates are scheduled.

Scheduled update of device object fields

In this field...	Do this...
Enable scheduler for updating server and service definitions from the devices	Check this check box to enable scheduling updates.
Period	In the drop-down menu, select either Daily or Weekly as the period for the updates.
Time	Using the two drop-down menus, specify the time of day on the 24 hour clock for the updates.

Update all device objects from (CLI)

You can update all device objects in AppViz with the current information from AFA from the CLI. This includes network objects, service objects, and network applications for

every device in AFA. You can update every object or specify to update only a specific type of object (for example, only service objects).

To update device objects from the CLI:

1. Open a terminal.
2. To update the list of AFA devices and every object from each device, enter the following command:

```
BusinessFlow-CLI.sh -t import_afa_objects
```

3. To update the list of AFA devices, enter the following command:

```
BusinessFlow-CLI.sh -t import_afa_devices
```

Note: If you run the network object, service object, or network application object update listed below without updating the list of devices, only the objects from devices included in AppViz's existing AFA device list will be imported. If a new device was added to AFA since the last device list update, the new device's objects will not be imported.

4. To update network objects, enter the following command:

```
BusinessFlow-CLI.sh -t import_afa_hosts
```

5. To update service objects, enter the following command:

```
BusinessFlow-CLI.sh -t import_afa_services
```

6. To update network applications, enter the following command:

```
BusinessFlow-CLI.sh -t import_afa_applications
```

Send us feedback

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

Email us at: techdocs@algosec.com

Note: For more details not included in this guide, see the online [ASMS Tech Docs](#).