FortiInsight - Administration Guide

Version 6.2.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

July 15, 2020
FortiInsight 6.2.0 Administration Guide
52-600-543474-20190801

TABLE OF CONTENTS

Change log

Date	Change description
2020-07-15	FortiInsight 6.2.0 document release
2020-04-21	FortiInsight 6.0.0 document release.
2020-02-13	FortiInsight 5.6.0 document release.
2019-11-01	FortiInsight version 5.2.0 document release.
2019-11-18	Added FortiInsight Cloud deployment and activation section

Introduction

FortiInsight is a unique data security and threat detection solution that delivers advanced threat hunting to help you detect, respond to, and manage risky behaviors that put your organization's business-critical data at risk. FortiInsight combines powerful and flexible machine learning with detailed forensics around user actions to provide complete visibility of activities around your organization's data. By monitoring user behavior and data movement both on and off your organization's network, and instantly alerting you to anomalous activities, FortiInsight helps you strengthen your security posture, protect your sensitive information, and support regulatory compliance.

What's new in FortiInsight version 6.2.0

The following table lists new features and enhancements in FortiInsight version 6.2.0:

Feature	Description
Increased storage of events	Due to architecture, and system improvements FortiInsight will now default to storing 30 days worth of live events, and 12 months of Archive events. • Previously only 7 days live, and 2 months of archive events were able to be stored. This has now seen a 4 x improvement on Live events, and a 6 x improvement for Archive events.
FortiInsight-VM initial pre-release	Support for running FortiInsight on-prem with provided distributions on MS Hyper-V, VMWare ESXI, and Linux KVM. Full release coming mid-Q3.
Command Line arguments	Command Line arguments integrated throughout the FortiInsight pipeline. This requires endpoint > 5.2 to begin to collect this new information. • Command-line arguments are now present on all “new process created” events where applicable. • You can now use these to craft policies targeting command line arguments
Support for file printed events	File printed events are now fully supported on the FortiInsight pipeline, and now contain additional meta-information such as: • Number of pages printed • Bytes printed • Name of the printer used • All the new meta-information fields are supported on policy creation, and AI will begin to learn behaviors associated with them.

Feature	Description
Added table setting save	All table settings have been moved to behind a settings button. Here you can check/uncheck which columns you want to show, and how many rows you want to display on the table.
Event information	All policy and ai alerts will now contain all event information for the event that triggered them, including command-line arguments, and file printed information.
Date Time picker improvements	• Added search-ability on pressing enter. • Restyling to show a much clearer error indication.
Update to search bar errors	Errors will no longer be visible in line, breaking the display of the search bar. They now have their own section.

System requirements

To successfully install and use FortiInsight version 6.2.0, your system must meet the following requirements.

Component	Requirements
Endpoint agent support	FortiInsight provides endpoint agents for the following platforms: • Windows 7 and later (32-bit and 64-bit) • Windows Server 2008 and later (32-bit and 64-bit)
Endpoint computers	• 1.0 GHz CPU - x86 or x64 (agent uses 0.1% to 5%) • 1 GB RAM (agent uses 10 to 30 MB) • 20 MB free disk space (more space is needed to store compressed and encrypted offline events)
Browser	• Google Chrome (recommended) • Chromium • Mozilla Firefox • Apple Safari Other web browsers may work correctly, but FortInsight does not support them.
Input devices	The FortiInsight UI is not optimized to use with touch devices. We recommend using a keyboard and mouse as the input devices for interacting with the UI.

Related resources

The following resources provide more information about FortiInsight:

- FortiInsight Documentation
- Fortinet Knowledge Base

- Fortinet Support website
- Fortinet NSE Institute

How FortiInsight works

FortiInsight monitors endpoint activity in the form of events. It provides automated inspection and alerts against these events in the form of policy and Augmented intelligence (AI) based inspections, as well as extensive search capabilities across the record of endpoint events for the past seven days.

Solution architecture

The FortiInsight solution consists of the following components:

- Endpoint agents
- Events
- FortiInsight Cloud service

You install agents on endpoints, which are Windows desktop computers and servers. The agents collect activity data on the endpoints and send the data, in the form of events, as they happen in real time on the endpoints, to the FortiInsight Cloud service. The FortiInsight Cloud service then stores and analyzes the data.

Endpoint agents

Endpoint agents use HTTPS to send data to the FortiInsight Cloud service. FortiInsight agents are lightweight, and typically run using less than 1% CPU and 50 MB of memory. The result is that FortiInsight is able to capture event data without slowing down endpoint devices.

When a device is offline, the endpoint agent continues to collect and store data locally on the device. When the device reconnects to the network, the agent sends the stored data to the FortiInsight Cloud service.

FortiInsight automatically authenticates and registers new endpoints that are deployed on your organization's network. All you need to do is push the agent out.

Events

Events are system-level activities that occur on your network. For example, when a file is created, a user logs on, or a process is stopped. FortiInsight captures event information from endpoints, such as:

- Network events, such as file upload or download activities.
- User events, such as a user login or a file read in Excel.

Each FortiInsight event contains the following elements:

Element	Description
User	The user account carrying out the activity.
Endpoint	The machine that the activity took place on.

Element	Description
Activity	The activity type, such as 'file uploaded' and 'file read'.
Application or process	The name of the application or process. For example, explorer.exe and winword.exe.
Resource	This is typically the path, filename, and file type involved in the activity.
Network destination and origin	For events on the **Network** page (**Threat Hunting > Network**), the network locations where the activity started and ended, including the port number that was used for the transfer.

Because there is a large volume of event data streaming in through FortiInsight, events are compacted after a certain threshold to optimize backend storage.

Secure storage

Data at rest

The data that the FortiInsight solution collects is stored securely.

For hosted deployments, all data at rest is encrypted. The FortiInsight solution is not a multi-tenant system, therefore no segregation is required since each set of backend servers, including the database, is dedicated to a particular client. Access to a client's system is locked down to the public IP address provided by the client (and Fortinet for administration purposes).

Stored passwords

FortiInsight UI passwords are stored securely. The passwords are salted and hashed, and are not stored in plaintext.

FortiInsight Cloud deployment and activation

Deploying FortiInsight Cloud

To deploy FortiInsight Cloud, complete the following steps:

1. Register the FortiInsight Cloud subscription license contract for management by FortiInsight Cloud:
   a. On the Customer Service & Support site, go to **Asset > Register/Activate**
   b. In the **Specify Registration Code** field, enter your license activation code and select **Next** to continue registering the product.
   c. Enter your details in the other fields and complete the registration.

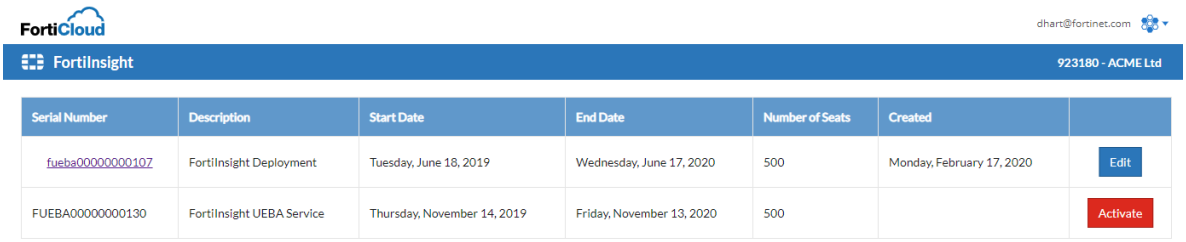
   You may need to wait a few minutes for the registration to complete before you can proceed to step 2.

2. Access FortiInsight Cloud in one of the following ways:
   a. Access FortiInsight Cloud from the Customer Service & Support site.
   b. Access FortiInsight Cloud from the FortiInsight Cloud portal:
      i. In a browser, go to the FortiInsight Cloud portal.
      ii. Log in with your FortiCloud credentials.

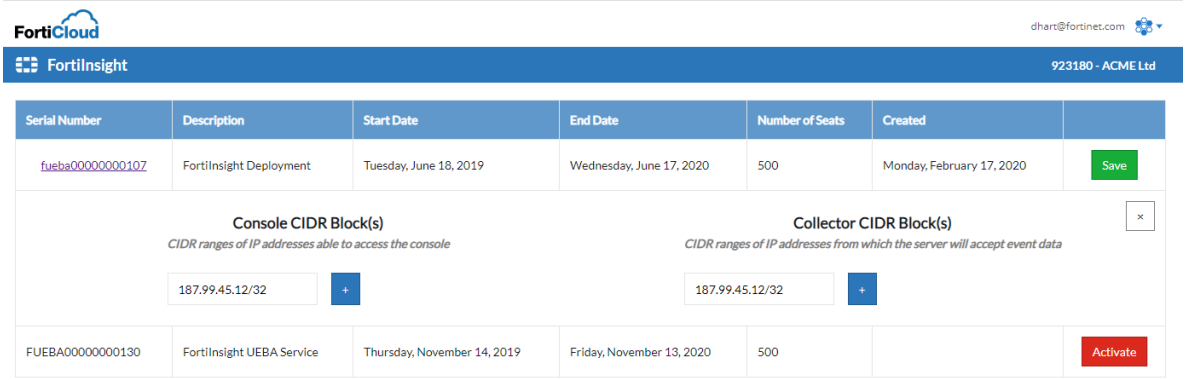
Activating FortiInsight Cloud entitlement

To activate an entitlement of FortiInsight on FortiCloud, complete the following steps:

1. In a browser, go to the FortiInsight Cloud portal.
2. Select **Login** and log in to your FortiCloud account, or register if you do not yet have one.
3. Select **Activate** for an entitlement that has not yet been deployed.



4. Fill out the following information and then click **Activate**.



Do not lose the administrator username or password, as you cannot reset them if forgotten. Customer Support is required to reset these credentials for you if a reset is necessary.

a. administrator account name and unique password

b. CIDR range of IP addresses able to access the console

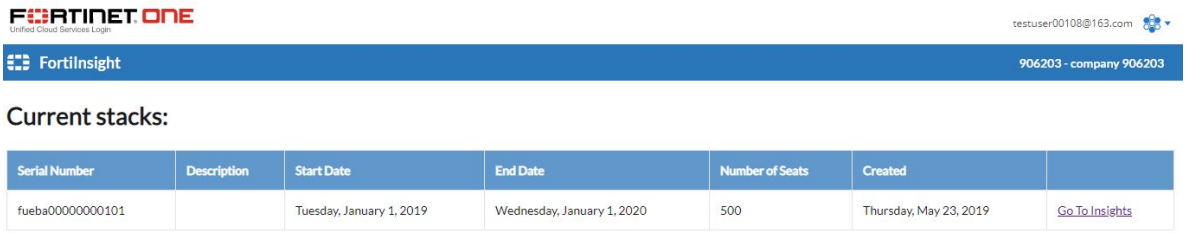
c. CIDR range of IP addresses from which the server accept event data

Note: You can add multiple CIDR blocks by clicking the plus + icon. We have prefilled your public IP address for your convenience.

Activation may take up to an hour to complete.

Only IPv4 is currently supported.

5. Once initialized, click **Go To Insights** to access your entitlement and FortiInsight will launch in a new browser tab



FortiInsight agent installation

Follow these procedures to install the FortiInsight agent for Windows.

Prerequisites

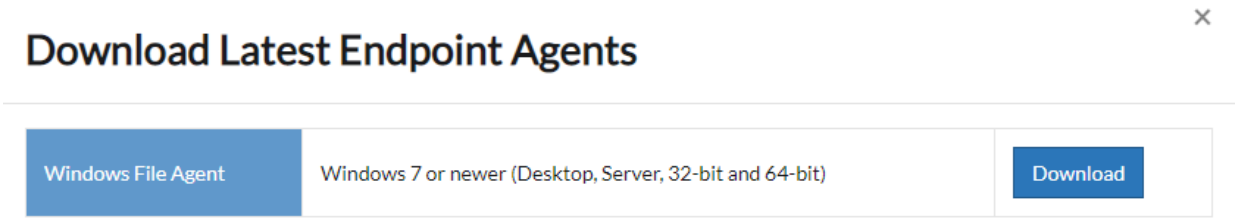
- Configure firewall rules to allow a network route between the FortiInsight agent and the FortiInsight Cloud service. The default port is TCP 8080 (HTTPS). You can do this either during or after installation.

Downloading the endpoint agent installer

You download FortiInsight agent installation software from the FortiInsight UI.

1. Go to **Admin > Endpoints**.
2. Click **Get Latest Endpoint Installers**.
3. Download the **Windows File Agent** (`cms_v<version>.msi` file).

The following image shows an example of the endpoint agent download window.

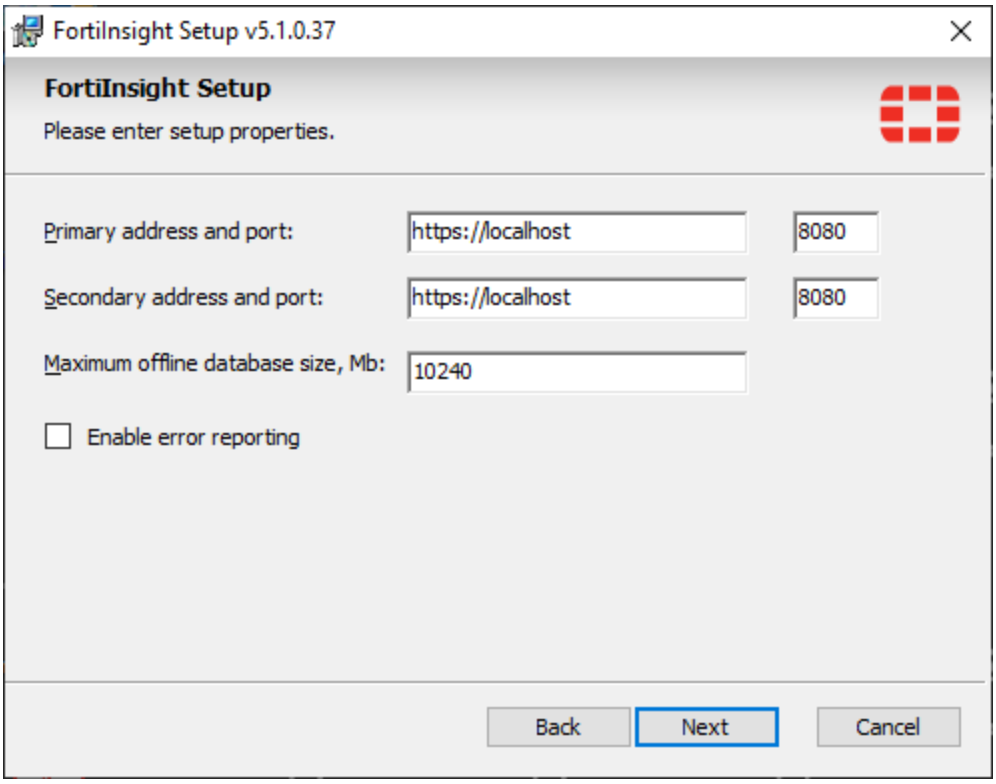


Installing the FortiInsight agent

Follow these steps to install and run the FortiInsight agent. By default, the FortiInsight agent installer installs the software in the `<Windows drive>:\Program Files (x86)\Fortinet\FortiInsight\` or `<Windows drive>:\Program Files\Fortinet\FortiInsight\` directory.

1. Double-click the FortiInsight agent installer and follow the instructions in the installation wizard.
2. In the **Primary address and port** field, enter the address and port information for your primary FortiInsight Cloud service.
3. In the **Secondary address and port** field, enter the address and port information for your secondary FortiInsight Cloud service. If you do not have a secondary FortiInsight Cloud service, it is recommended that you add the primary FortiInsight Cloud service settings to these fields instead.

4. In the **Maximum offline database size** field, enter a limit. This setting is useful for virtualized deployments when the user profile is copied on and off the machine to a remote location.
5. If you want the agent to automatically submit crash dump and text logs data to Fortinet (using HTTPS), select the **Enable error reporting** checkbox.



6. Click **Next**, and then **Install**.
7. To complete the installation, click **Finish**.

Verifying that the agent is reporting to the FortiInsight Cloud service

Follow these steps to verify that the FortiInsight agent is reporting to the FortiInsight Cloud service.

1. Log in to the FortiInsight UI as an administrator.
2. Go to **Admin > Endpoints**.

   By default, all agents are listed in the table. Agent details include both the registered time and information about the last activity. To sort the list to display new agents first, click the **Registered (UTC)** heading.

If an agent does not appear within 10 minutes, see Troubleshooting on page 17 for more information about steps that you can take to determine why the agent is unable to send data correctly.

Package management installation

The following instructions are intended for system administrators who can use package management software to push the FortiInsight agent out to endpoints.

Installing or updating the agent using MsiExec

To install the FortiInsight agent using MsiExec, use the MSI package that is provided. You must also set some additional parameters. To run the MSI package, a user requires elevated privileges such as the ones granted by the administrators group.

You can also use the MSI installer to update the agent. To update the agent, run the command again with a new version of the FortiInsight agent and the installer will find and replace the product.

1. Install the agent using one of the following options:
   - To install the agent without logging, use the following command:
     ```
     msiexec /i cms.msi /norestart /qn CS_ADDRESS=https://<primary_server>
     CS_ADDRESS_PORT=<primary_port> CS_ADDRESS_
     SECONDARY=https://<secondary_server> CS_ADDRESS_PORT_
     SECONDARY=<secondary_port> ERROR_REPORTING=1 OFFLINE_DB_SIZE_MB=<db_
     limit>
     ```
   - To install the agent with logging, use the following command:
     ```
     msiexec /i cms.msi /norestart /qn CS_ADDRESS= https://<primary_server>
     CS_ADDRESS_PORT=<primary_port> CS_ADDRESS_SECONDARY=
     https://<secondary_server> CS_ADDRESS_PORT_SECONDARY=<secondary_port>
     ERROR_REPORTING=1 OFFLINE_DB_SIZE_MB=<db_limit> /L*Vx <log_filename>
     ```

   where:

Parameter	Description
`<primary_server>`	The address of the primary FortiInsight Cloud service.
`<primary_port>`	The port number of the primary FortiInsight Cloud service (for example, 8080).
`<secondary_server>`	The address of the secondary FortiInsight Cloud service.
`<secondary_port>`	The port number of the secondary FortiInsight Cloud service.

   If required, you can specify the following optional parameters:

Parameter	Description
`ERROR_REPORTING=1`	Turn on agent error reporting, which creates and uploads error reports to Fortinet.
`<db_limit>`	Specify a limit for the offline database (for example, 10280). The offline database will not grow beyond the maximum size that you specify.

Parameter	Description
`/L*Vx <log_filename>`	Write verbose output to the log file that you specify (for example, install.log).
`REBOOT=ReallySuppress`	Prevent soft reboots.
`INSTALLFOLDER=<folder_location>`	Specify an alternate installation folder (for example, T:\ZF).

Uninstalling using MsiExec

To uninstall the FortiInsight agent, use the following command. To run the MSI package, a user requires elevated privileges such as the ones granted by the administrators group.

```
msiexec /x cms.msi /norestart /qn /L*Vx uninstall.log
```

Troubleshooting

How to whitelist files if antivirus software interferes with FortiInsight

If antivirus software interferes with FortiInsight, you can consider whitelisting the following files on the endpoint. This is useful if the antivirus software uses application sandboxing heuristics that wrap around any new applications. This can result in high CPU and memory usage and can significantly slow down the machine.

x64

- <Windows drive>:\Program Files (x86)\Fortinet\FortiInsight\end.col.man.exe
- <Windows drive>:\Program Files (x86)\Fortinet\FortiInsight\end.col.man.xml
- <Windows drive>:\Program Files (x86)\Fortinet\FortiInsight*.tmp
- <Windows drive>:\Program Files (x86)\Fortinet\FortiInsight\data\agentID.bin
- <Windows drive>:\Program Files (x86)\Fortinet\FortiInsight\data\agentSettings.xml
- <Windows drive>:\Program Files (x86)\Fortinet\FortiInsight\data\offline.sqlite
- <Windows drive>:\Program Files (x86)\Fortinet\FortiInsight\logs\cms*.log
- <Windows drive>:\Windows\System32\drivers\KernelAgent32.sys
- %appdata%\Fortinet\FortiInsight*

x86

- <Windows drive>:\Program Files\Fortinet\FortiInsight\end.col.man.exe
- <Windows drive>:\Program Files\Fortinet\FortiInsight\end.col.man.xml
- <Windows drive>:\Program Files\Fortinet\FortiInsight*.tmp
- <Windows drive>:\Program Files\Fortinet\FortiInsight\data\agentID.bin
- <Windows drive>:\Program Files\Fortinet\FortiInsight\data\agentSettings.xml
- <Windows drive>:\Program Files\Fortinet\FortiInsight\data\offline.sqlite
- <Windows drive>:\Program Files\Fortinet\FortiInsight\logs\cms*.log

- <Windows drive>:\Windows\System32\drivers\KernelAgent32.sys
- %appdata%\Fortinet\FortiInsight*

How to verify FortiInsight Cloud service details in the config files

1. Navigate to the directory where the FortiInsight agent is installed. By default, FortiInsight installs the agent software in the `<Windows drive>:\Program Files (x86)\Fortinet\FortiInsight` directory.
2. Open the `end.col.man.xml` config file.
3. Confirm that the **Host** and **Port** values are correct for your FortiInsight server installation. If the entries are wrong, edit the file and enter the correct values. Save the file, and the configuration changes automatically take effect.

How to verify that the host computer can reach the FortiInsight Cloud service

1. In a web browser, visit **https://<ip_address>:<port_number>** (insert the appropriate IP address or HTTPS IP address from your config file or Customer Specific Information document).
   You should see an XML document with version numbers similar to the following:

```
{
   "Version": "4.0.14.0",
   "ApiVersions": [
      "1.0",
      "1.1",
      "1.2",
      "1.3",
      "1.4",
      "2.0",
      "2.8"
   ]
}
```

How to gather data for a Fortinet Support request

If you need to contact Fortinet Support for help, gather the following data and have the `cms.log` file ready to share with Fortinet Support.

1. Navigate to the directory where the FortiInsight agent is installed. By default, FortiInsight installs the agent software in the `<Windows drive>:\Program Files (x86)\Fortinet\FortiInsight` directory.
2. Open the `end.col.man.xml` config file.
3. Change the `LogLevel` value from 4 to 2, and save the file.
4. Wait 5 minutes to allow for data to be gathered.
5. Open the `end.col.man.xml` config file.
6. Change the `LogLevel` value from 2 to 4, and save the file.
7. Navigate to the logs folder in the agent installation folder and locate the `cms.log` file. Have the file ready to share with Fortinet Support.

Searching

The search bar is universal across the FortiInsight user interface, and works the same way on each page.

Modes

There are two modes for the search bar: Design and Plain Text. Design mode is flexible UI approach, where you can move pills around, whereas Plain Text removes these UI elements.

Toggle between the two by switching the mode on or off. The following image shows Plain Text mode.

Design

Search pills

You conduct searches on individual fields in the data that FortiInsight stores. Each search consists of the following three pieces of criteria, which combine to form a search pill:

1. Field to search
2. Type of comparison to make
3. Value to search for

The following table describes the criteria options for search pills:

Criteria	Options	Description
Field to search	The list of available search fields varies according to the type of data that you are searching for.	Select the field that you want to search.
Type of comparison to make	• **Less Than** • **Greater Than** • **Greater Than or Equal To**	Matches values that fall within the comparison type that you specify. For example, **Less Than** matches values that are less than the value that you enter. You can use these search types for numerical comparisons, such as searching based on port number or severity. You can also use these search types for alphabetical comparison, such as finding results that appear alphabetically later than the entered value.

Criteria	Options	Description
	• **Less Than or Equal To**	
Value to search for		The value that you want to search for. You can enter more than one value by separating the values with commas.
	Terms	This is a text-based search. The search pill defaults to this type of search. You can use the following special characters for additional search control: • Asterisk (*): Use as a wildcard to represent one or more unknown characters. • Question mark (?): Use as a wildcard for a single unknown character.
	Regular Expression	For advanced users, the search pill supports regular expression searches. For more information about regular expression searches, see https://www.elastic.co/guide/en/elasticsearch/reference/5.6/query-dsl-query-string-query.html#_regular_expressions

The following image shows an example of search pills.:

The following image shows an example of a comma separated list.

Creating search pills

1. Click in the search bar.
2. Select a field to search from the options in the drop-down list. You can also begin typing and FortiInsight narrows the options to a list of available fields.
3. If you do not want to do a terms search, select an alternate type of comparison from the drop-down list.
4. Enter a value to search for and press **Enter**.
5. Optionally, add one or more additional search pills and modify the concatenators. (See Logical operators on page 21)
   The search results table updates to show the results to your search query.

You can also use values that appear in the tables on the FortiInsight UI pages to add criteria to the search bar. To add a value in the table to the search bar, right-click the value and click **Add to Search**. To exclude a value in the table from the search, right-click the value and click **Exclude from Search**.

Logical operators

FortiInsight search pills support the use of logical operators, which include concatenators and modifiers.Concatenators are used to join search pills together in the search bar. Modifiers are used to modify an existing search pill, and can be used in combination with concatenators.

The following operators can be used in your searches:

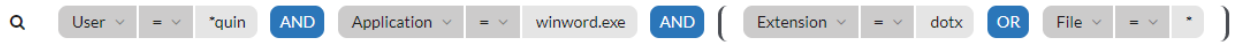
- **AND**: Both search pills joined with this concatenator must evaluate as true in order for a search result to be returned.
- **OR**: Either of the search pills joined with this concatenator can evaluate as true in order for a result to be returned. To use the OR concatenator, either type OR and press Enter between search pills or click on an existing concatenator to cycle between AND and OR concatenators.
- **NOT**: Exclude values from the search by preceding the search pill with a NOT modifier. To use the NOT modifier, before you enter a pill, type NOT and press Enter.

The following image shows an example of the AND and NOT operators:

Grouping search pills

You can use parentheses to group search pills and specify operator precedence to construct complex queries. To group search pills, type an open parenthesis, enter the search pills, and type a close parenthesis. If you do not enter parentheses, the search bar intelligently adds brackets behind the scenes to interpret your query.

The following image shows an example of grouping search pills.



Plain text

Plain text mode allows you to build your search without using the Searchbar Pills. In this raw format, plain text removes all the UI elements from the searchbar - including things like draggable pills, in pill replacements.

Plain text operators are the same as those of design search. See above.

Limiting searches to a specific date range

By default, FortiInsight carries out the searches over an open period of time, searching all the data that is held within its index. **Policy Alert** and **AI Alert** pages are the exception, where the default search is performed over the current week only. You can limit searches to begin at a specific date, end at a specific date, or search within a date range.

- To have the search begin at a specific date, specify the start date in the **From** date range box.
- To have the search end at a specific date, specify the end date in the **To** date range box.
- To search within a specific date range, specify a start and end date in the date range boxes.

The following image shows the date range boxes.

Copying and pasting search queries

You can copy and paste search bar entries across the FortiInsight UI. This means that you can use the same search query in different areas of the FortiInsight UI without having to re-type it. For example, you can copy a query from a new Policy being created and past it to the **Threat Hunting** page without having to retype the search criteria. This helps to save time when you use large, complex search queries.

The search bar copy and paste function intelligently recognizes the fields that are supported by the area of the tool, and will warn you if any fields are not supported within the pasted section of FortiInsight.

1. Click the copy icon in the search bar.

   The following image shows the **Copy Search** icon:
2. Navigate to the screen that you want to move the search query to.
3. Click the paste icon in the search bar.

   The following image shows the **Paste Search** icon:

Deleting a search pill

To delete a search pill, place your cursor to the right of the search pill, and press **Backspace**.

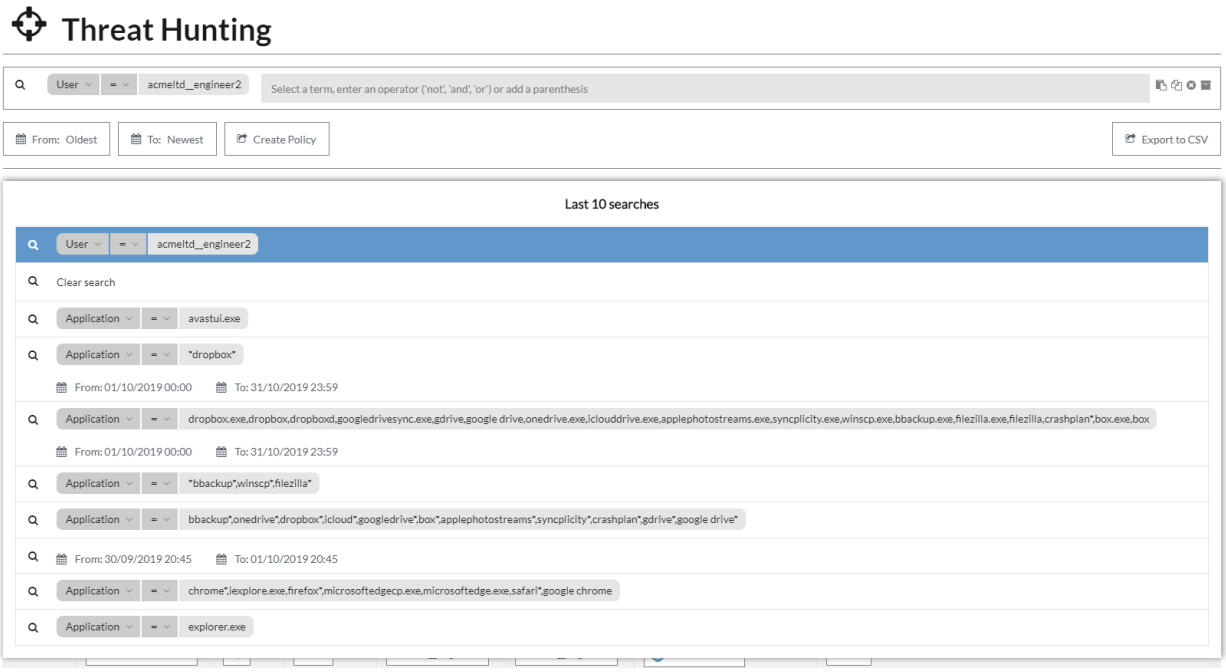
Clearing a search

To clear your current search, click the **x** icon at the end of the search bar.

Last searches

Access a list of your ten latest searches by clicking the Last Searches icon at the end of the search bar. Select a search from the list to run that search again.

The following image shows an example of a list of Last 10 searches:



Sticky searches

In the FortiInsight UI, searches are sticky within a particular data type. This means that when you search events, the search bar on other UI pages that search events autopopulate with the last search that you entered.

Searches are sticky across FortiInsight sessions. This means that the search bar autopopulates with the last search that you entered from the previous session.

To clear a prefilled search from the search bar, click the **x** at the end of the search bar.

Finding related events

To help you explore events that may be connected, and potentially provide further information and context, you can see events that occurred around the same time as a specific event.

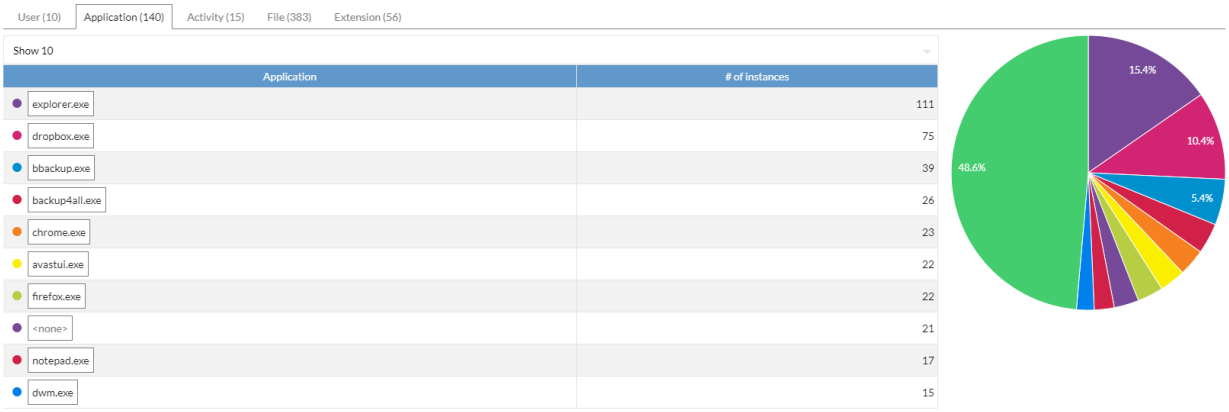
1. Right-click on the timestamp of an event.
2. Select **Find Items Around This Time**.

FortiInsight narrows the list to events that occurred within a five minute radius (five minutes before to five minutes after) of the event that you selected.

Summary tables

Summary tabs and tables are available on some pages in the FortiInsight UI and provide an overview of your search results. You can reveal summary tables below the search bar on the **Alerts** and **Threat Hunting** pages.

The following image shows an example of the summary tabs.



Converting a threat hunting search into a policy

When you perform a search on the **Threat Hunting** page, you can convert your search into a policy for automatic alerting on the criteria in the future. To convert a threat hunting search into a policy that will generate future alerts, click **Create Policy**.

Table settings

To configure tables, select the table settings icon  located to the top right of the table.

The settings allows you to configure the table to show default number of rows per page (10, 50, 100, 250 or 500) and which columns should show by default, the image below is for the Live event table. These settings will be remembered across your logged in sessions on FortiInsight.


Configure table
Rows per page:
100
Columns to display:
Time (UTC)
Endpoint
Endpoint Name
User
User Name
Application
Resource
Activity
File
Extension
Folder
Port Name
Printer
Pages Printed
Bytes Printed
Command Line Arguments

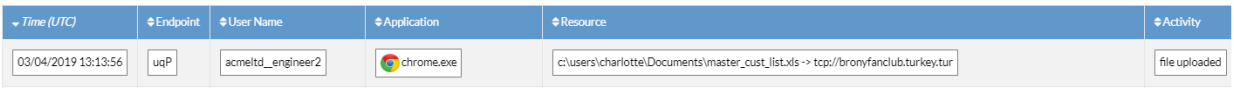
Threat hunting

Threat hunting is your view of all the events that FortiInsight captures. This is where you get access to the record of events that are streaming in from endpoints. Search events using the search bar, refine the time span of events with the date picker, and use summary tables to find more detailed information about events.

Build complex searches to find the events that you are interested in, and add search results to collections.

To see events, navigate to the **Threat Hunting** pages. The events are categorized as **Live** and **compacted**; you can also search for events in the usual way.

The following image shows an example event on the **Live** events page.



The following image shows an example event on the **Compacted** events page.

By default, the **Threat Hunting** pages show all events, which is likely to be a large number. Refine data by searching events in the **Threat Hunting** pages. Sort and order columns, and choose columns that you want to include and exclude. Use filters to pick a time and date range for the data that you want to see.

Collections

A collection is a way of taking a snapshot of a particular search at a particular time so that you can perform further analysis on the results. For example, if you think an event or group of events is unusual, you can add it to a collection and inspect it later on.

Creating a collection

Create a collection by clicking **Collection** beside the search bar.

You can do this with any search. You can create collections based on Policy alerts, AI alerts, and Live events. You can also use collections as a way of saving a search that you want to perform regularly.

Refreshing a collection

If a collection contains a search that you want to perform regularly, such as a daily, weekly, or monthly search, you can refresh the collection to perform the search again by clicking **Refresh Collection**.

This takes the original search that you used as the basis for the collection and updates it by re-running the search with current data.

Taking snapshots of searches

To see all data within a snapshot, click on a collection. The **Collection Definition** shows the original search terms that were used. To further refine the data, you can search within a collection.

To export a collection or a subset of a collection, as a CSV file, click **Export to CSV**.

Policies

FortiInsight policies inspect incoming events in real time as they arrive from endpoints. A policy has a set of criteria that FortiInsight compares to incoming events and raises an alert if an event matches the criteria.

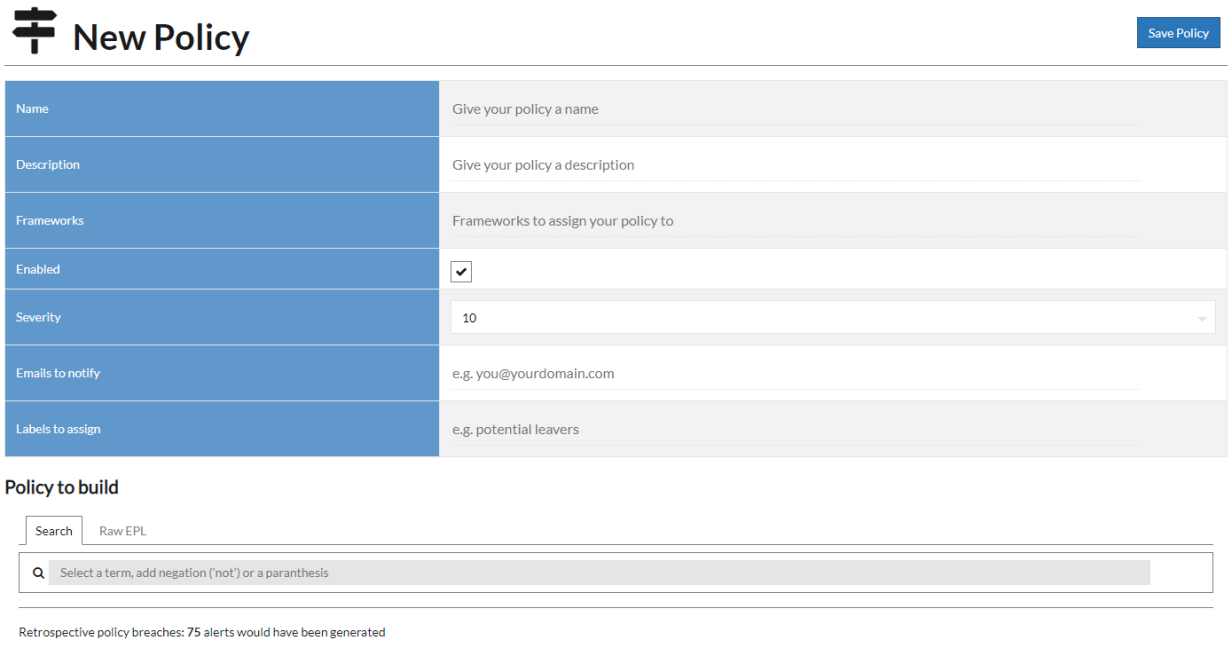
You can set up policies to tell FortiInsight when you want to be notified about particular activities. The alerts page shows you all alerts that have been generated based on policies that you have built.

You can create an unlimited number of policies. You can see the status of policies (active or inactive) in the policy list without having to view the details of each policy.

Creating a policy

1. Go to **Policy > Settings**.
2. Click **New**.
3. Set a policy name, description, and severity level.
4. In the **Policy to build** section, enter criteria for the policy.
5. If you require immediate notifications about the policy, enter an email address in the **Emails to notify** field.

The following image shows the **New Policy** screen.



Editing a policy

1. Click on a policy.
2. Edit the search criteria that apply to the policy.
3. To save your changes, click **Update Policy**.

Retrospective policy breaches

At the bottom of a policy page, FortiInsight shows the number of previous alerts that would have been triggered by the policy rules, based on your FortiInsight data to date.

To see the events that would have triggered alerts, navigate to a **Threat Hunting** page, where the policy details are prefilled in the search bar.

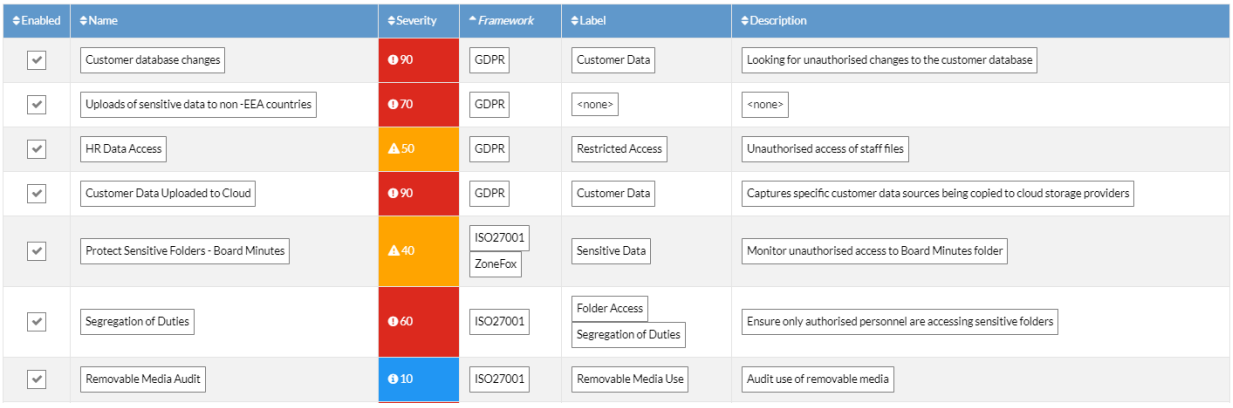
The following image shows an example of the retrospective policy breaches message:

Frameworks and labels

If a policy is relevant to one or more compliance frameworks, you can assign compliance frameworks to the policy when you create it.

The **Framework** column shows all of the compliance frameworks that are associated with a policy. You can use labels in a similar way to mark particular types of activity. The **Label** column shows all labels that are associated with a policy.

The following image shows an example of the **Framework** and **Label** columns.



Out-of-the-box policies

FortiInsight comes with several policies. You can use these policies as they are, modify them to suit your requirements, or use them as a base for creating your own policies.

The following image shows the policies that FortiInsight comes with:

Name	Severity	Framework	Label	Description
AV Not Started Symantec	10	FortiInsight	<none>	Alerts on Symantec Anti Virus service not being started during OS boot sequence
AV Stopped Symantec	10	FortiInsight	<none>	Alerts on Symantec Anti Virus service being stopped while an endpoint is still running
Customer Data Uploaded to Cloud	40	GDPR	Customer Data	Captures specific customer data sources being copied to cloud storage providers
File Written to Removable	10	FortiInsight	<none>	Alerts on files being written from an endpoint to external devices such as flash drives or removable media
Financial Data Breach	90	ISO27001	Restricted Access	Policy to alert on unauthorised access to Sage accounting system
HR Data Access	50	GDPR	Restricted Access	Unauthorised access of staff files
Monitor Command Line Usage	10	FortiInsight	<none>	Alerts on the usage of command line tools
Monitor Suspicious Application Usage	10	FortiInsight	<none>	Alerts on the usage of any application which could constitute a security threat
Protect Sensitive Folders - Board Minutes	40	ISO27001	Sensitive Data	Monitor unauthorised access to Board Minutes folder
Segregation of Duties	60	ISO27001	Folder Access, Segregation of Duties	Ensure only authorised personnel are accessing sensitive folders
Software Install	10	FortiInsight	<none>	Alerts on installation of software on Windows endpoints
Source Code Copied to Removable Media	90	<none>	IP Data, Source Code	Looks for source code files being copied to removable media
Torrent Client Usage	10	FortiInsight	<none>	Alerts on the usage of known torrent clients or the presence of torrent files on an endpoint
Uploads of sensitive data to non EEA countries	70	GDPR	Sensitive Data	Alerts on the upload of files containing sensitive data to no EEA countries
User Login Out of Hours	10	FortiInsight	<none>	Alerts on users logging into an endpoint outside of the defined hours UTC
VPN Usage	10	FortiInsight	<none>	Alerts on known VPN clients being executed on an endpoint
Windows OS Tampering	10	FortiInsight	<none>	Alerts on activity that is indicative of tampering with the Windows operating system

Note that the following out-of-the-box policies from FortiInsight 5.2.0 have moved from Policies and are now part of the default collections on the Threat Hunting page (**Threat Hunting** > **Collections**):

- Browser Download
- Browser Upload
- Files Backed up to Cloud
- Outlook Upload
- Outlook Download

Alerts

FortiInsight generates two types of alerts: Policy and AI alerts. You can view both types of alerts on the **Alerts** pages in the FortiInsight UI.

Policy alerts

The **Policy Alerts** page shows alerts that FortiInsight generates based on policy settings. FortiInsight generates an alert if an event meets conditions that you defined in policies. For example, you can set up an alert that notifies you if a user accesses a sensitive file on a network drive.

To see policy alerts, go to **Policy > Alerts**.

AI alerts

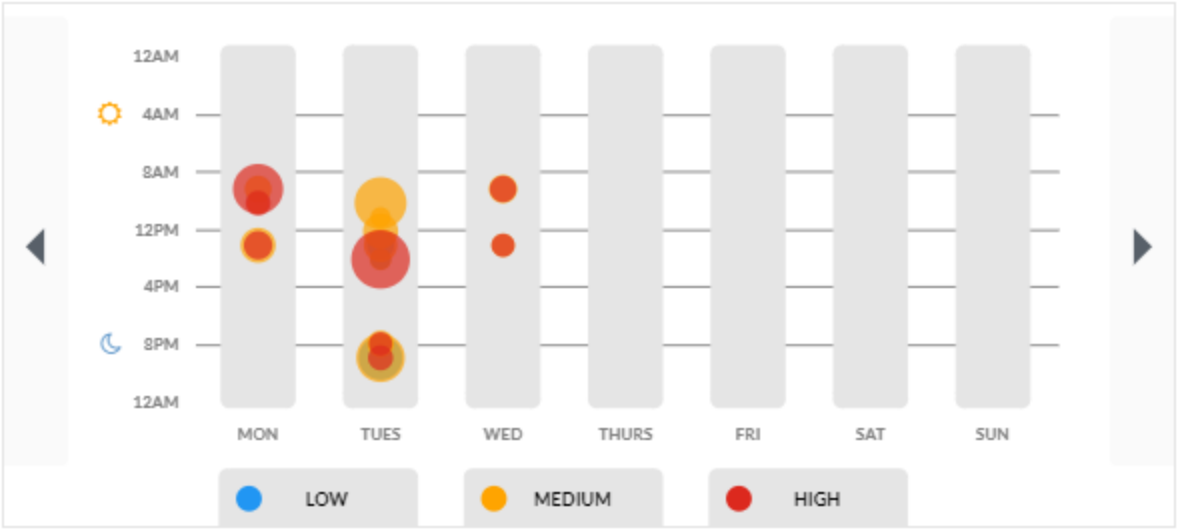
The **AI Alerts** page shows alerts that FortiInsight AI generates. If there are alerts on this page, it means that FortiInsight AI detected some anomalous behavior based on one or more events, as well as any tags that you defined.

To see AI alerts, go to **AI > Alerts**.

Timeline

The timeline provides a weekly view of alerts, categorized by severity (low, medium, and high). The quantity of alerts is represented by the size of the dots.

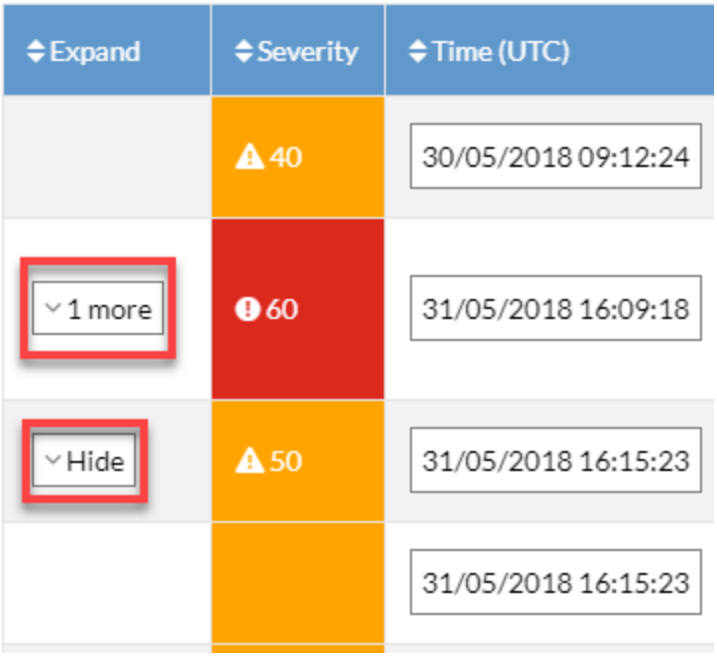
The following image shows an example timeline.



Searching alerts

The search bar allows you to narrow down the alerts displayed on either the **Policy Alerts** or **AI Alerts** pages. To sort and order alerts, click the column headings and use the checkboxes to choose the columns that you want to see.

Similar alerts that occur around the same time are grouped together to reduce noise. Click **more** to see all of the related events, and click **Hide** to re-group them. The following image shows the grouping options in the **Expand** column.



Finding related alerts

To help you explore alerts that may be connected, and potentially provide further information and context, you can see alerts that occurred around the same time as a specific alert.

1. Right-click the timestamp of an alert.
2. Select **Find Items Around This Time**.

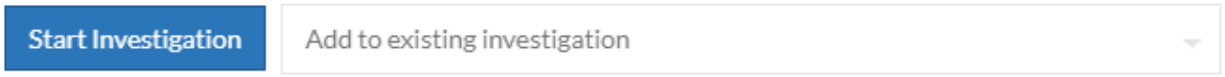
FortiInsight narrows the list to alerts that occurred within a five minute radius (five minutes before to five minutes after) of the alert that you selected.

Alert details

To drill down into further details about alerts, click on an alert. You can see a high-level overview of the alert. You can see more details about the individual events that make up the alert under **Events within this Alert**.

From here, you can choose to start an investigation based on this alert, or add the alert to an existing investigation.

The following image shows the investigation options.



To get more context on an alert, right-click an element of an alert and select **Threat Hunt**. This action takes you to the **Threat Hunting** page where you can view more information.

To export alerts, click **Export to CSV**.

AI

FortiInsight Augmented intelligence (AI) adds context, risks, and ratings to activities on your network to find a wide range of threats. It learns general facts about normal behavior in order to identify when anomalous behavior occurs.

FortiInsight AI uses risk scoring to decide how anomalous an event is. For example, a development team is likely to access and edit different files and applications than a marketing or sales team does. By learning what usual behavior patterns are, AI can help identify when abnormal events occur.

AI scoring

The severity score is a combination of risk and anomalism. FortiInsight decides how risky an activity is, and then how unusual it is for that user. If an activity is high risk and unusual, the score will be high. If an activity is low risk and determined not to be especially unusual for that user, the score will be low.

The machine learning models of FortiInsight automatically generate AI alerts. The AI alerts are scored on a combination of the following factors:

- **Anomalism**: The amount of deviation from normal behavior that the event represents.
- **Risk**: A static score, according to the type of program, data, or activity that the event represents. For example, a cloud backup program is medium risk.

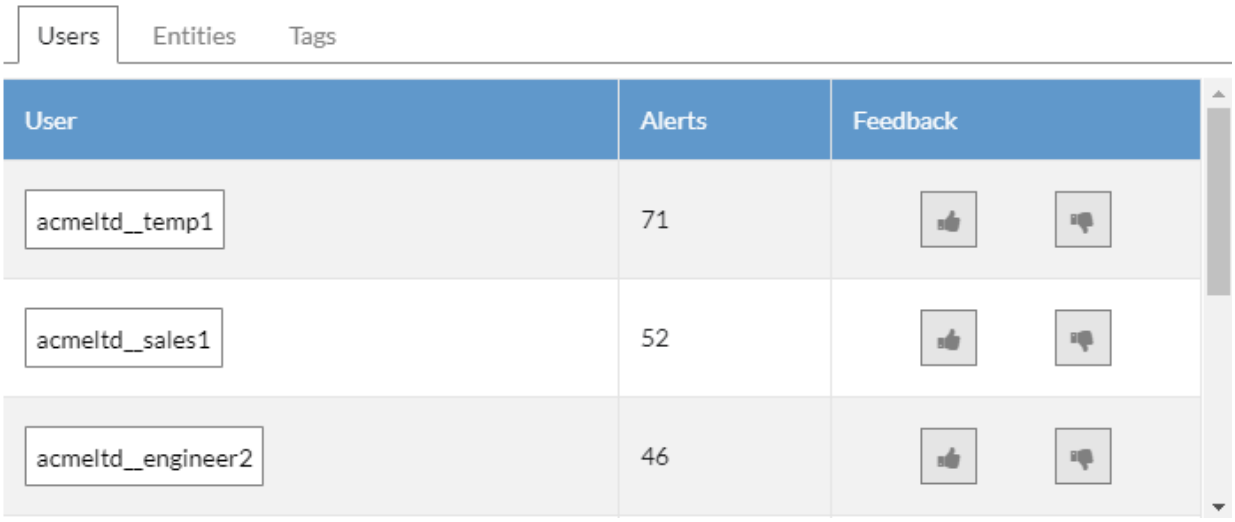
The risk category for each alert (low, medium, or high) is the same for both AI and policy-based alerts:

- **Low**: 0 to 39
- **Medium**: 40 to 69
- **High**: 70 to 100

Feedback

To provide AI with information about alerts, use the **Feedback** column on the **AI Alerts** page (**Alerts > AI**). If AI has identified an event that you think is anomalous, click the thumbs-up icon to give positive feedback. If AI has identified an event that you do not think is a threat, click the thumbs-down icon. AI will learn based on your responses.

The following image shows and example of the **Feedback** column.



AI tags

As FortiInsight AI inspects incoming events for anomalism, it also attempts to categorize anomalous events using tags. AI inspects the events for specific characteristics, as defined in the AI tag definitions, and applies the appropriate tags to events that match. For example, AI applies the **Potential Leaver** tag to an event that involves a user writing a CV file, and the **Malicious File** tag to events that display common characteristics of ransomware.

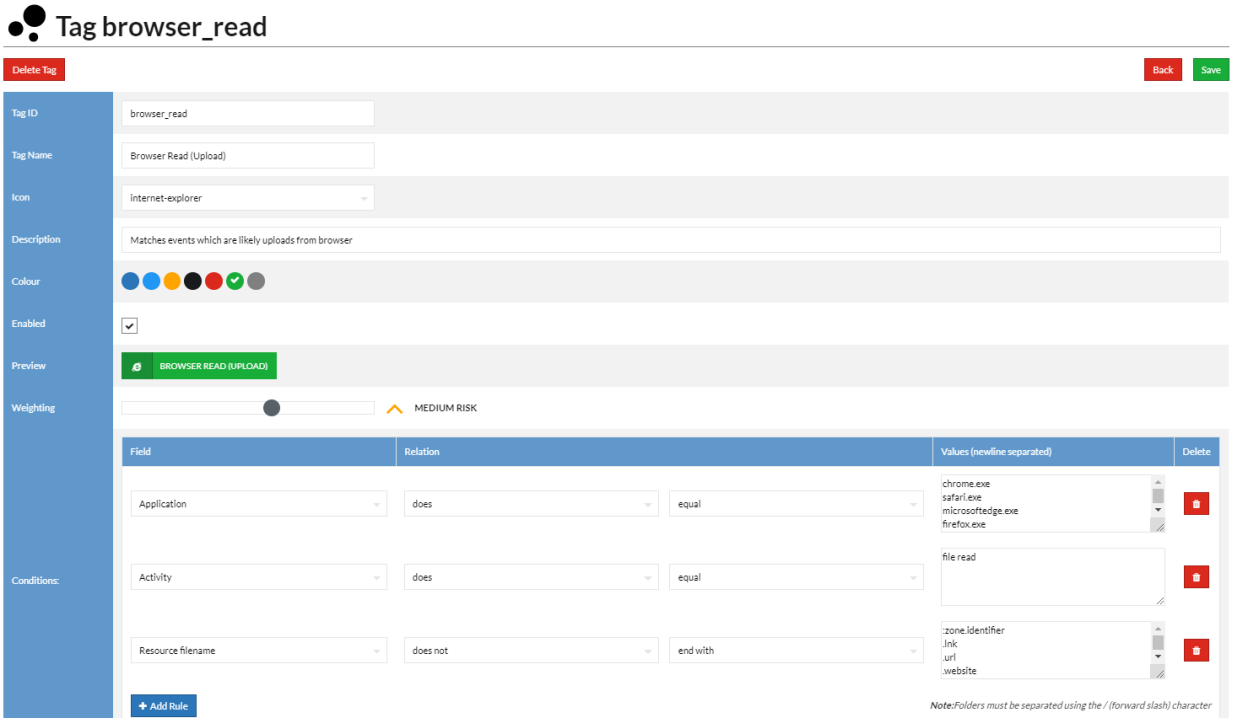
The **AI Alerts** page shows the most commonly detected tags in the summary table, and allows you to search the list of alerts for particular tags.

Using AI tags

You can sort AI tags by risk and other columns. This sorting makes it easier for you to find the tags that you are looking for. You can also search for tags within a table.

Navigate to the **AI > Tags** tab. Click on any tag to edit color codes and icons.

The following image shows an example of an AI tag.



Change tag risk setting

The risk slider on the **Tag** page allows you to quickly change the risk rating of your tags.

The following image shows the risk slider.

AI training

AI takes two weeks to learn what normal behavior looks like and form an effective baseline. After this, AI will automatically switch from learning mode to anomalous detection mode and will begin to identify anomalies.

AI settings

This section allows you to define file types, folders, and users that you think are high risk. FortiInsight AI then attaches a higher risk to anomalous events that include these elements.

Once these settings have been added you must enable, risky_user, risky_filetypes and risky_filepath to allow the AI module to learn these and start to alert on their anomalous behaviours.

Dashboards

The FortiInsight dashboards provide an overview of the activity happening across your organization's environment over various time ranges.These dashboards are accessed through the **Dashboards** drop-down menu. There are five dashboards: one configurable **Custom** dashboard and four built-in dashboards (**Forensic Activity**, **Alerts**, **Data Flow**, and **Applications**).

Each dashboard contains a variety of widgets that provide information about events, users, and alerts. Click on the arrow icon on the widget headings to go to the linked page containg more detailed information relevant to the widget. Click on the bars within bar chart widgets to drill down to see more in-depth data.

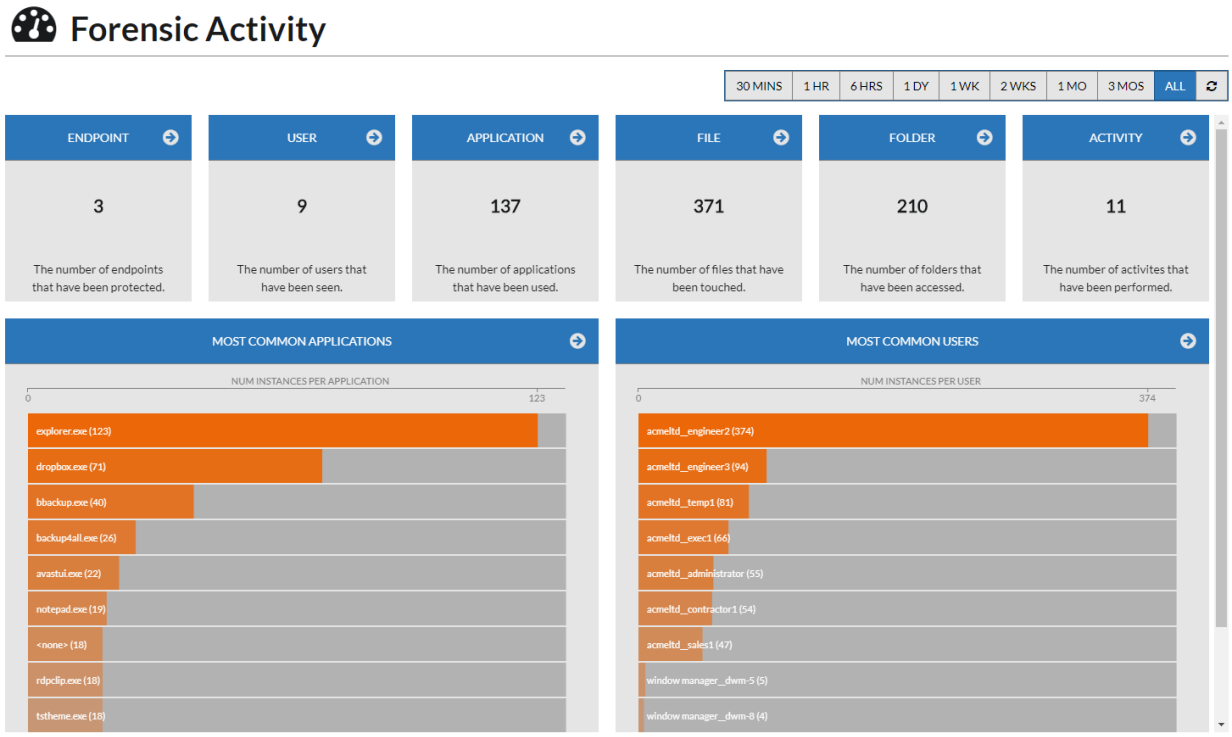
You can configure these widgets or build custom widgets to display the desired metrics. See Custom dashboard configuration on page 40.

Forensic Activity dashboard

The **Forensic Activity** dashboard provides an overview of all activity recorded by FortiInsight, including the following:

- Top 10 endpoints, users, applications, files, folders, and activities
- Lists of the most common applications and users

The following image shows an example of the **Forensic Activity** dashboard:



Alerts dashboard

The **Alerts** dashboard provides an overview of all alerts that have been triggered by policy breaches, including the following:

- The number of users who have breached policies.
- The number of policies that were breached.
- The number of critical policies that were breached (policies with a severity level of 60 and above).
- A breakdown of the number of alerts generated by each policy, or associated with specific tags.

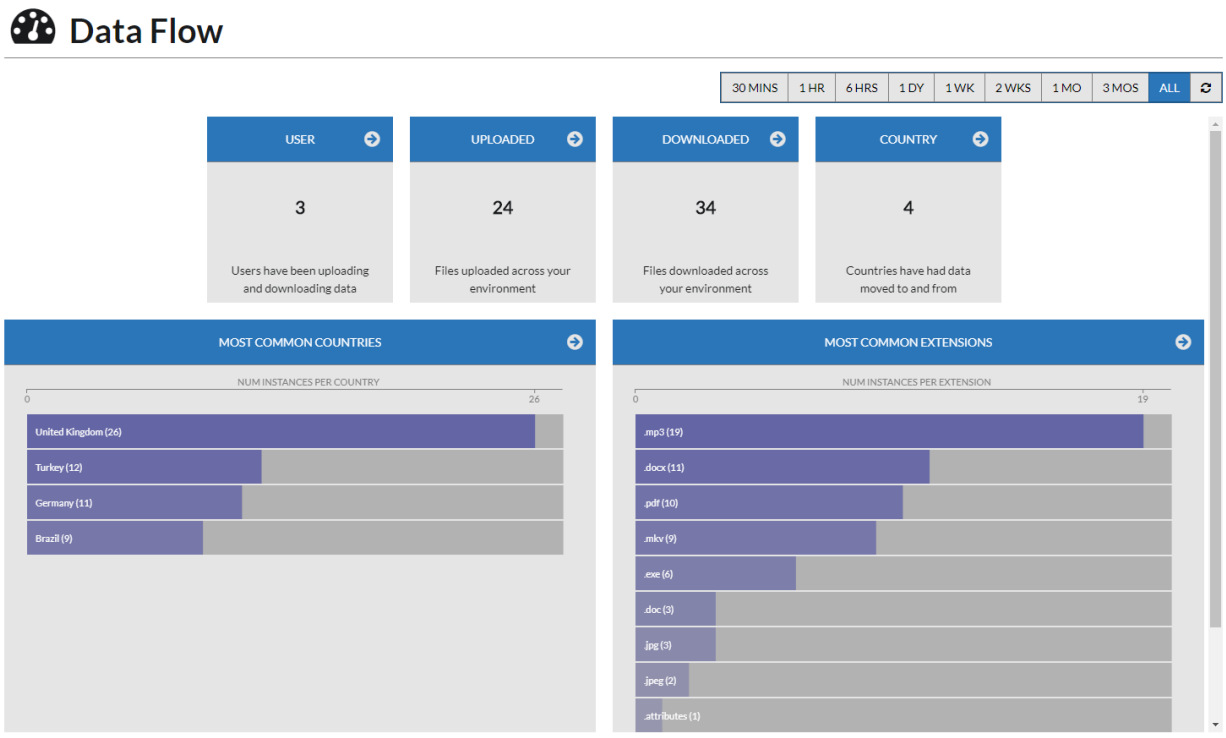
The following image shows an example of the **Alerts** dashboard:

Data Flow dashboard

The **Data Flow** dashboard gives an overview of the following:

- The amount of data that has been transferred into and out of your organization's network, including the users responsible and the countries involved.
- A breakdown of the most common file extensions. This information gives you an idea of what types of data are being transferred.
- A daily breakdown of data transfer.

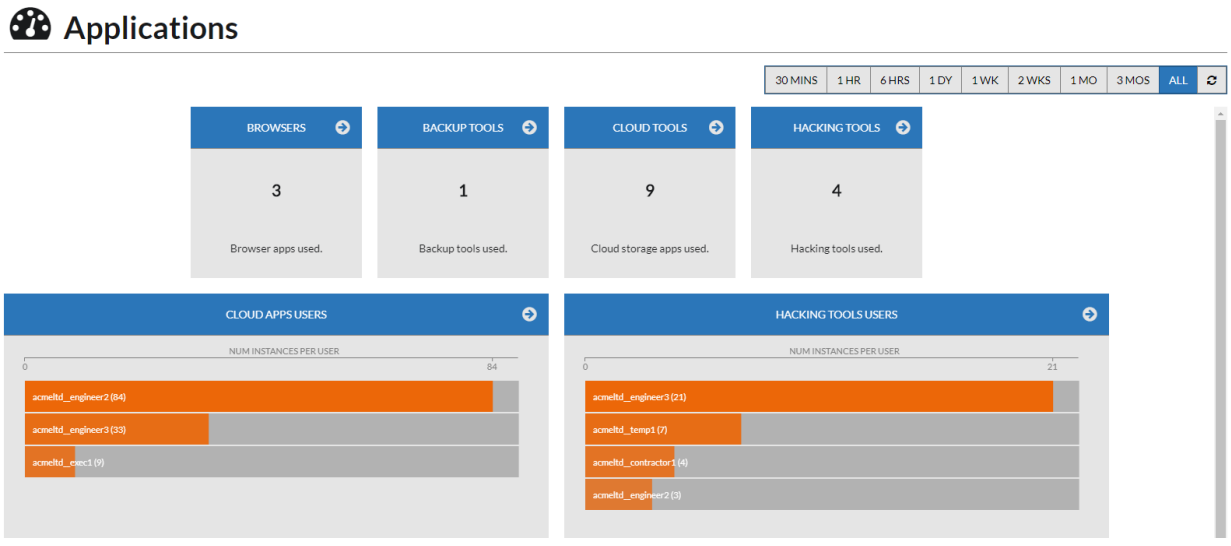
The following image shows an example of the **Data Flow** dashboard:



Applications dashboard

The **Applications** dashboard provides an overview of the key categories of applications that have been seen in your network

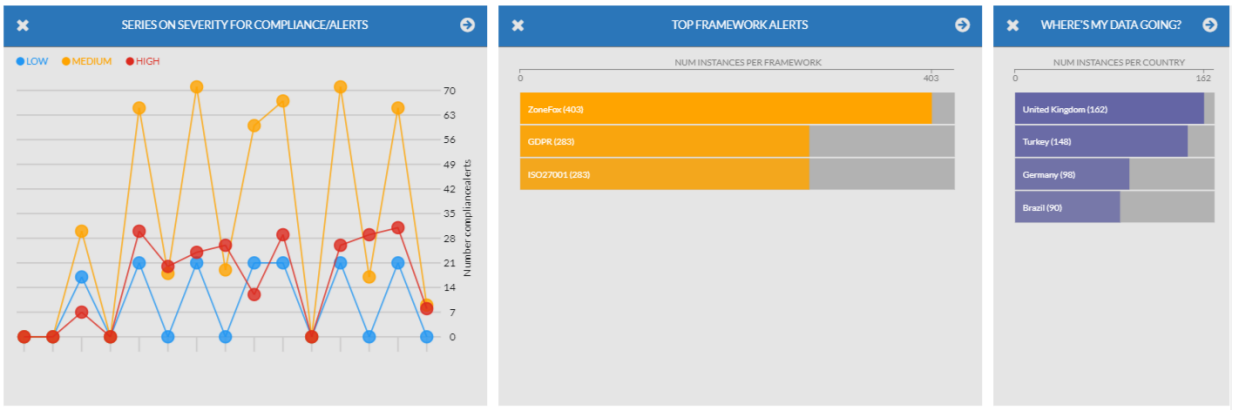
The following image shows an example of the **Applications** dashboard:



Custom dashboard configuration

The Custom dashboard consists of configurable widgets that you can build and modify to display the summary data you desire. You can add, remove, resize, and move around the widgets to create your own custom dashboard display.

The following image shows some examples of widgets:



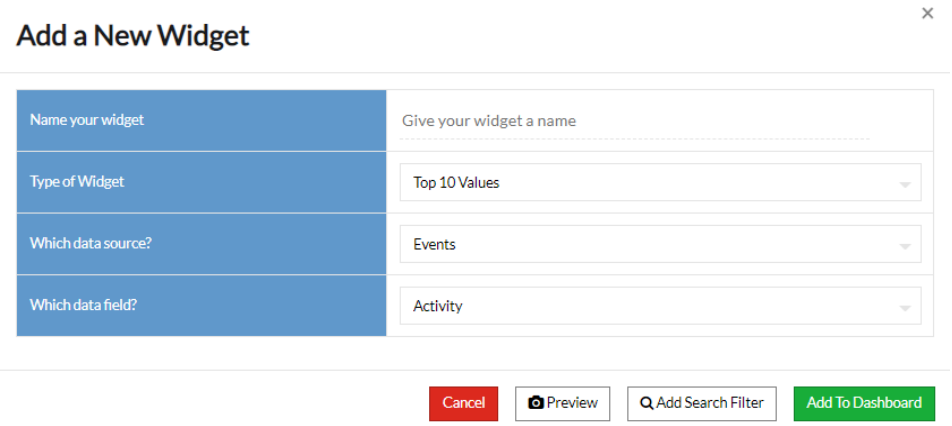
Widget types

To create a new widget, click **Add**, name the widget, and select the type, data source, and field.

The following widget types are available:

Widget Type	Description
Top 10 Values	Creates a bar chart.
Series over time	Creates a line graph.
Count of Unique Values	Metric type
Top 100 Pie	Creates a pie chart.

The following image shows an example of the new widget window:

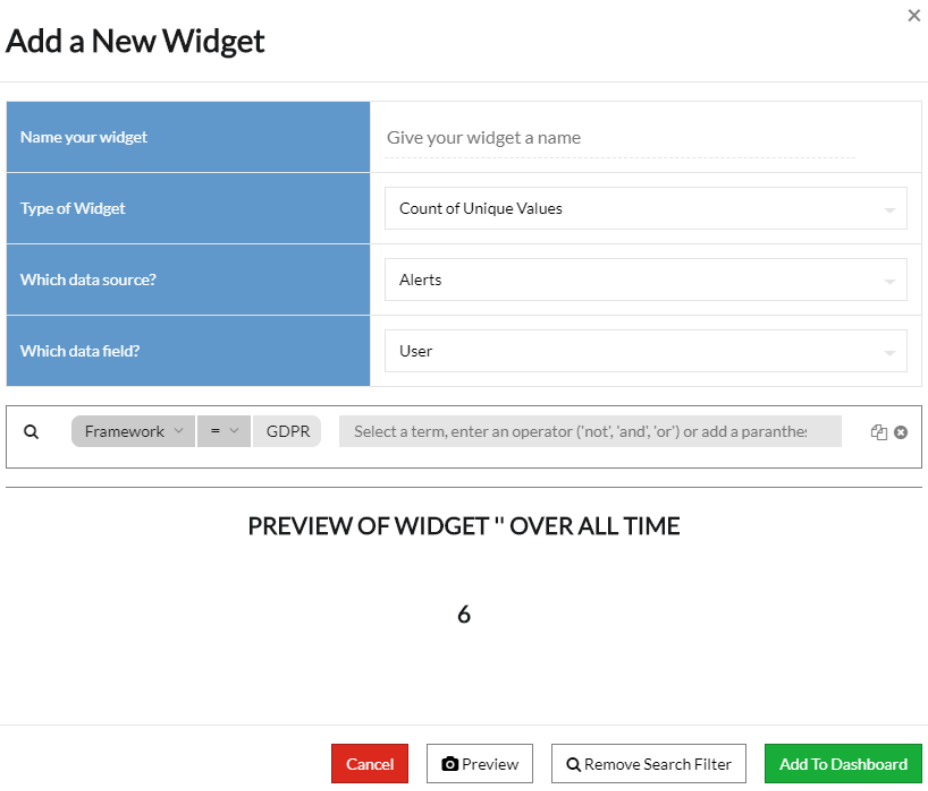


Filtering widgets

To further refine the data that is displayed in the widgets, use the **Add Search Filter** option. The filter option works in the same way as the search bar.

Widget example

The following image shows an example of the number of users who triggered alerts. Using filters to search for alerts with the GDPR compliance framework, we can see that six users triggered GDPR-related alerts.



Reports

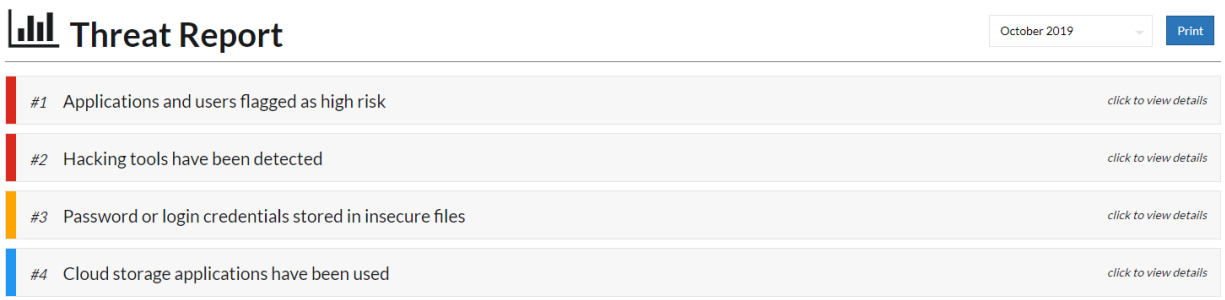
Threat Report

The **Threat Report** provides automated reports for various behaviors, from which you can export releveant charts and raw data.

Navigate to **Reports > Threat Report**. From here, you can view the automated reports which show headline activity for a number of key user behaviors, including the following:

- **Applications and users flagged as high risk**
- **Hacking tools have been detected**
- **Password or login credentials stored in insecure files**
- **Cloud storage applications have been used**

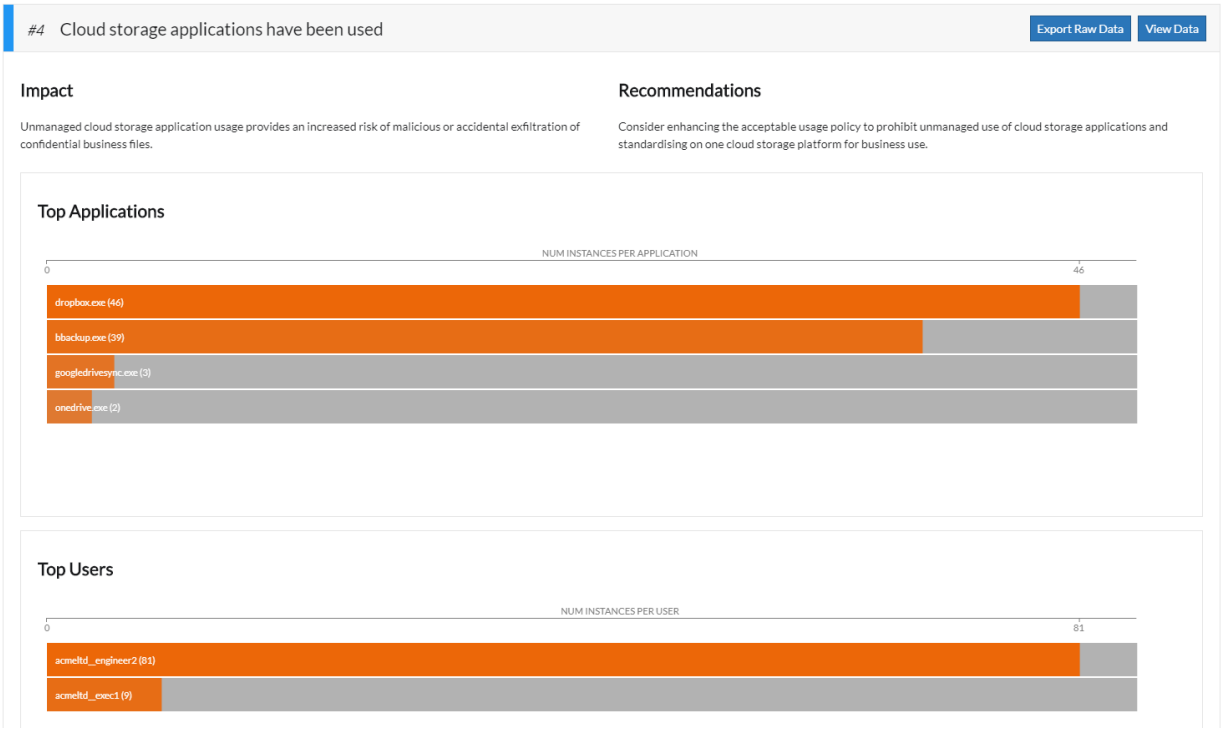
The following image shows an example of the **Threat Report** dashboard:



Threat Report recommendations

To show the recommendations, select **click to view details**. To hide the recommendations, click the headline section again. The information provides security advice about how to protect your network from the identified behaviors.

The following image show an example of recommendations for the use of Cloud storage applications:

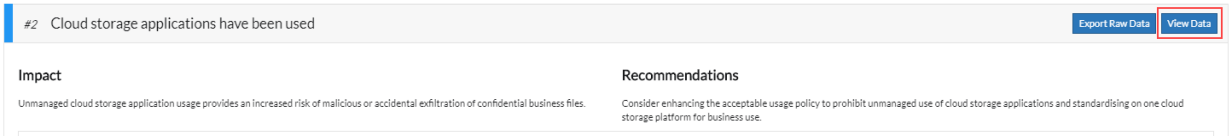


Threat Report interactive elements

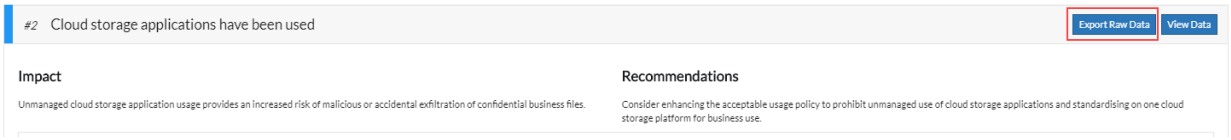
You can click individual fields in the bars graphs to jump to the **Threat Hunting** dashboard with the relevant search criteria already populated.

Threat Report export

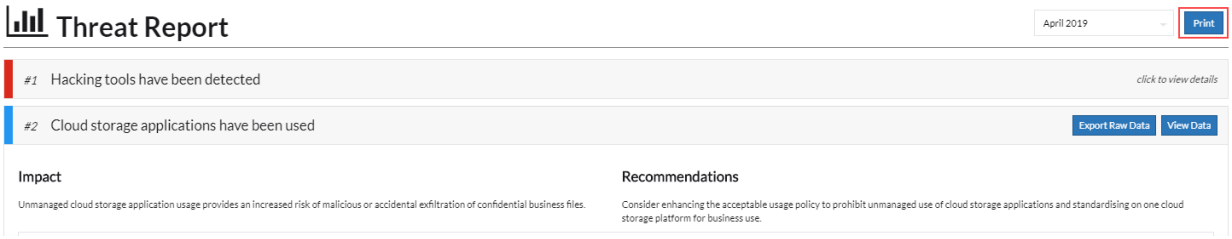
To jump to the FortiInsight page with the relevant data used in the report, click **View Data**.



To export elements of a **Threat Report** as CSV files, so that you can use them in other reporting tools, click **Export Raw Data**.



To print a formatted version of the **Threat Report** with title and end pages, click **Print**.


Threat Report
April 2019
Print
#1 Hacking tools have been detected
click to view details
#2 Cloud storage applications have been used
Export Raw Data
View Data
Impact
Unmanaged cloud storage application usage provides an increased risk of malicious or accidental exfiltration of confidential business files.
Recommendations
Consider enhancing the acceptable usage policy to prohibit unmanaged use of cloud storage applications and standardising on one cloud storage platform for business use.

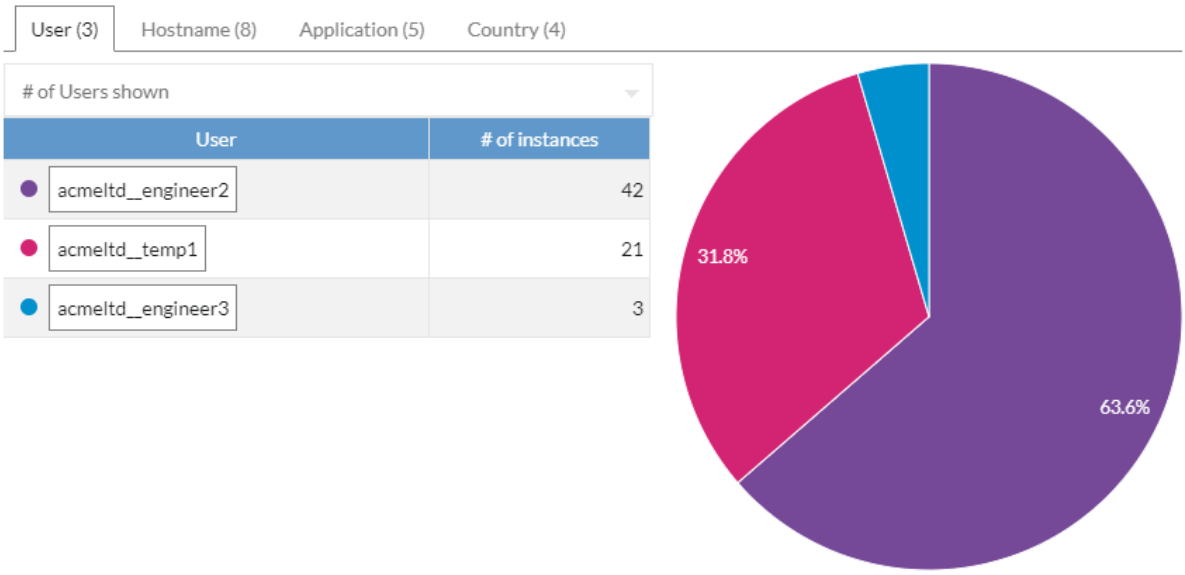
Networking

The **Network** page (**Threat Hunting > Network**) shows file upload and download events, and provides additional details about the data that has been moving in and out of your organization.

Networking statistics

The **Network** page provides high-level statistics for the number of upload and download events. You can find more granular details about individual events in the tables on the **Network** page.

The following image shows an example of the networking statistics:

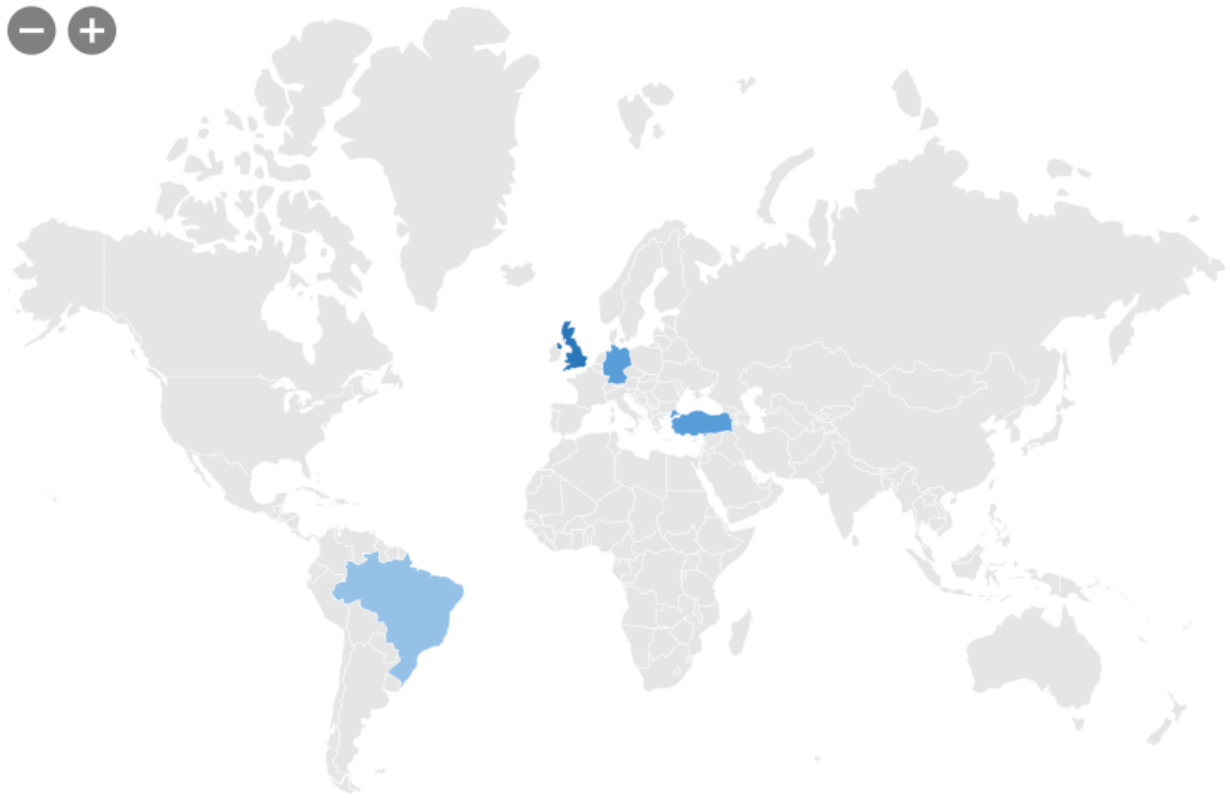


Map

The map shows the geographical sources and destinations of upload and download events. The darker color shows a greater number of network events.

- To move the map, click and drag in the ocean.
- To zoom in and out, use the icons in the top left of the map.
- To add or exclude a country from the search terms, right-click on the country.

The following image shows an example of a map:



Investigations

Investigations collate alert information in a single location. To prepare reports, you can use the collated information. For example, you can create a report to submit to HR or a data regulator.

Creating investigations

To create an investigation, click **Start Investigation** in the details page for any alert. You can also add alerts to existing investigations from here. You can create investigations based on policy alerts, AI alerts, or a combination of both. You can also add notes to provide context around alerts.

Using investigations

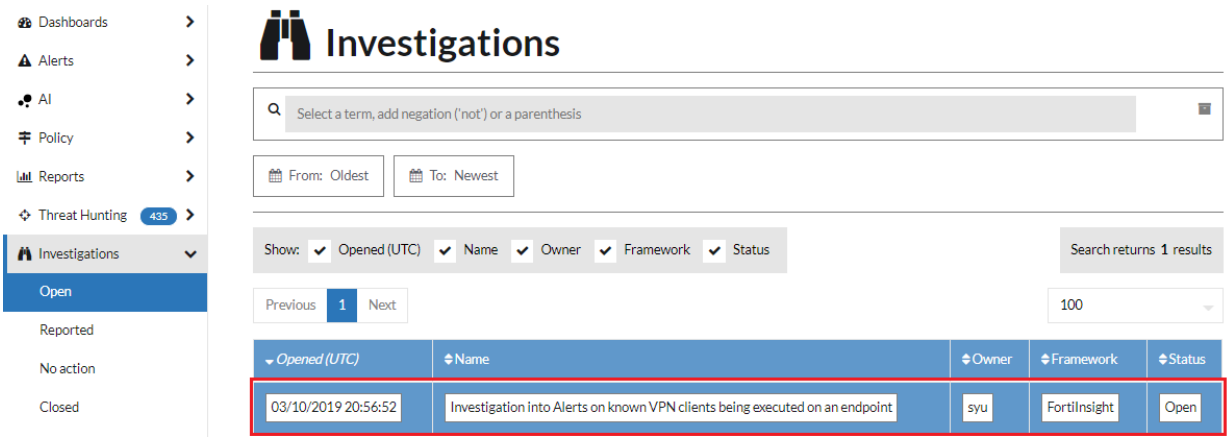
Investigations have the following options:

- **Owners**: Investigations have an owner. If you want to transfer the ownership to someone else, you can change the owner by editing the investigation.
- **Note**: You can add notes to an investigation to add context and comments to alerts that have been recorded.
- **Update Status**: You can update the status of an investigation to **Reported**, **No action**, or **Open**.

Exporting investigations

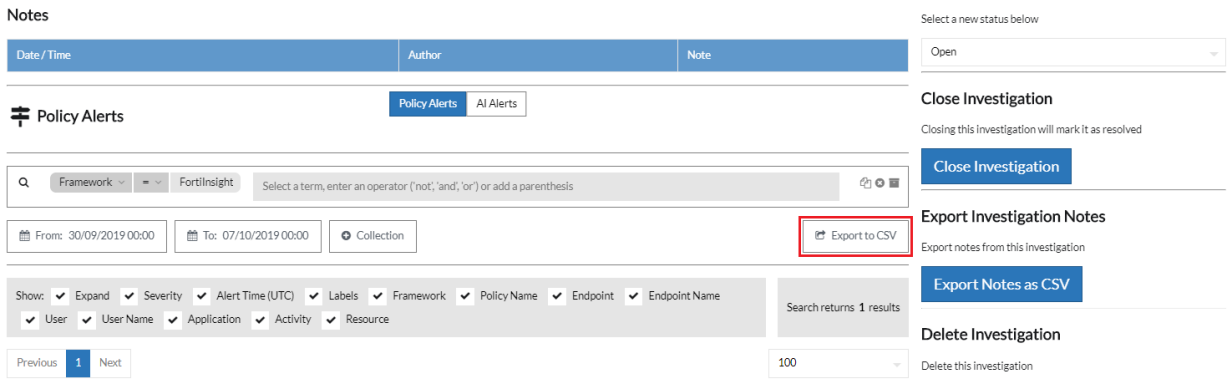
To export investigations as CSV files, first navigate to the Investigation Details page of the desired investigation. To do so, pick a type of investigation (Open, Reported, No Action, or Closed) from the **Investigations** drop-down menu and then select the row of the desired investigation from the table of investigations.

The following image shows an example of a selected row from the table of investigations on the **Investigations** page, outlined in red:



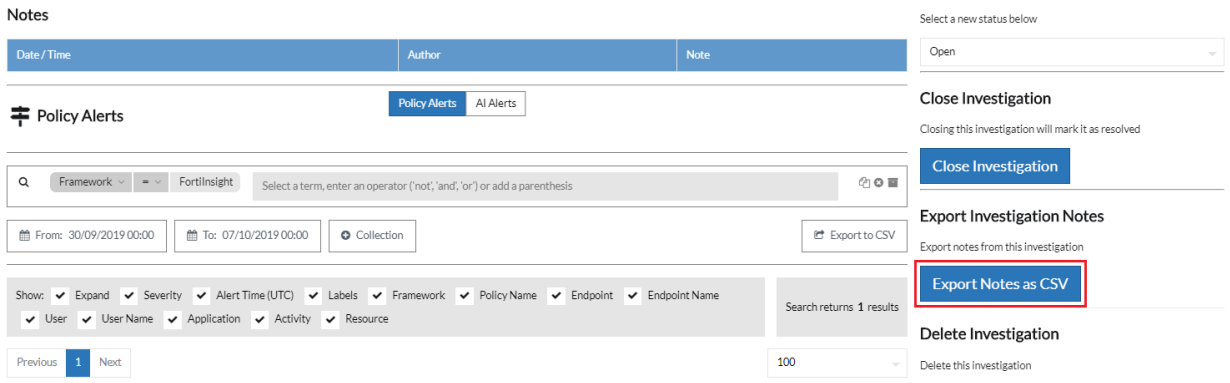
You can then export the investigation as a CSV file by clicking the **Export to CSV** button below the Policy Alerts or AI Aerts search bar on the **Investigation Details** page.

The following image shows the location of the **Export to CSV** button, outlined in red:



To export Investigation notes, use the **Export Notes as CSV** button under the **Export Investigation Notes** heading on the righthand side of the UI.

The following image shows the location of the **Export Notes as CSV** button, outlined in red:

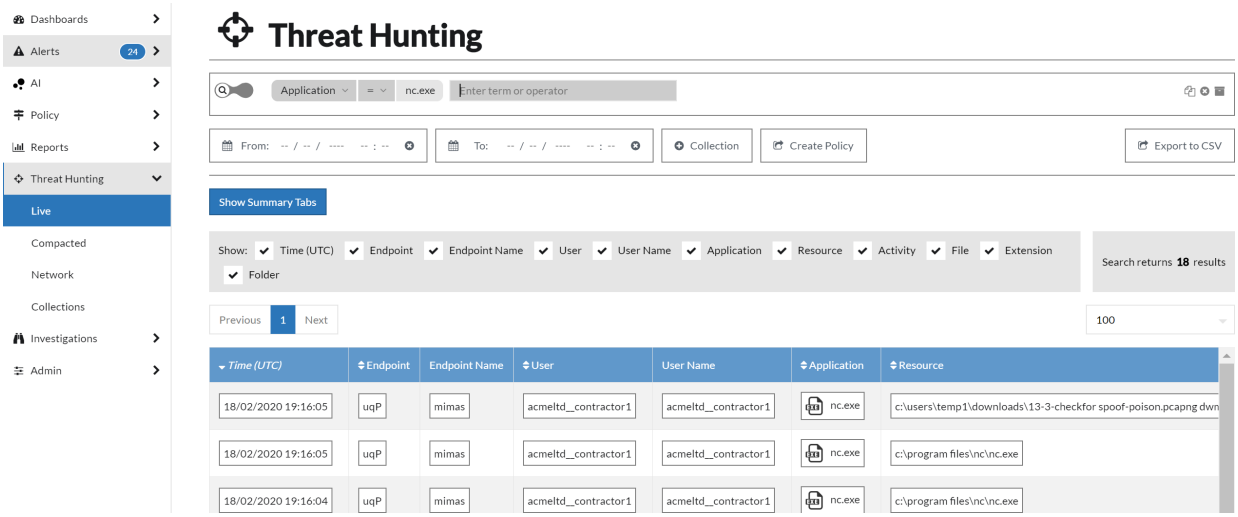


User Timeline

The **User Timeline** allows you to view alerts, and select events across a timeline. This view collates multiple sources of data into a single timeline so you can see all information on the specific user. For instance, in one view you can see AI alerts, Policy alerts, Event information summaries - including applications, files, activities and user log-on, log-offs.

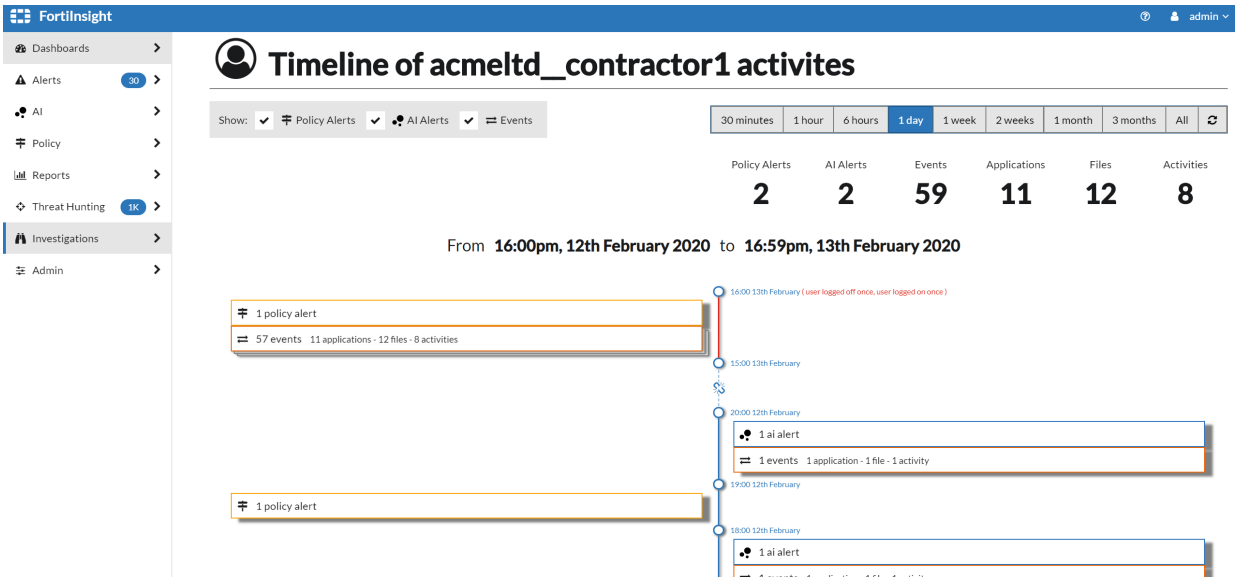
The **User Timeline** can be accessed via the context menu, where FortiInsight provided helpers, like add direct to search, exclude and so on. Right click on the user element, i.e. User, Username columns in tables or summary tabs.

Threat Hunting Live Table

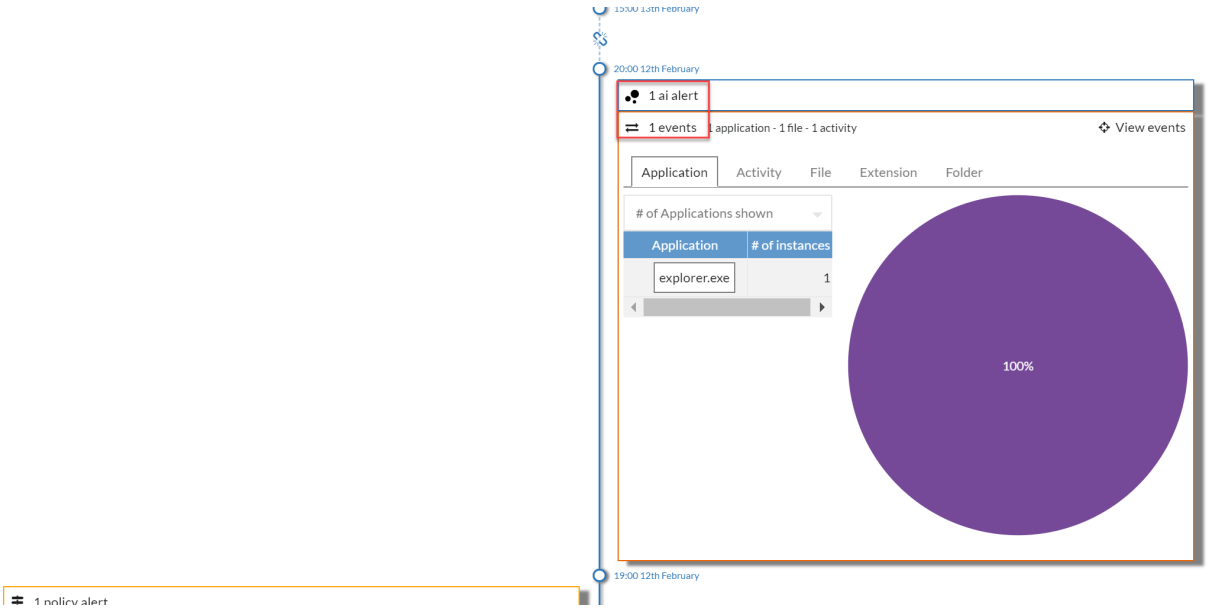


The following image shows where to right click and how to pull up the User Timeline.

The following image shows the **User Timeline**.



Click into the Timeline element to display more information. It will give you two types of information: Alerts, for AI or Policy, and data for events. The following image shows that all applications in the event have used explorer.exe.


20:00 12th February
1 ai alert
1 events
1 application - 1 file - 1 activity
View events
Application
Activity
File
Extension
Folder
# of Applications shown
Application
# of instances
explorer.exe
1
100%
19:00 12th February
1 policy alert

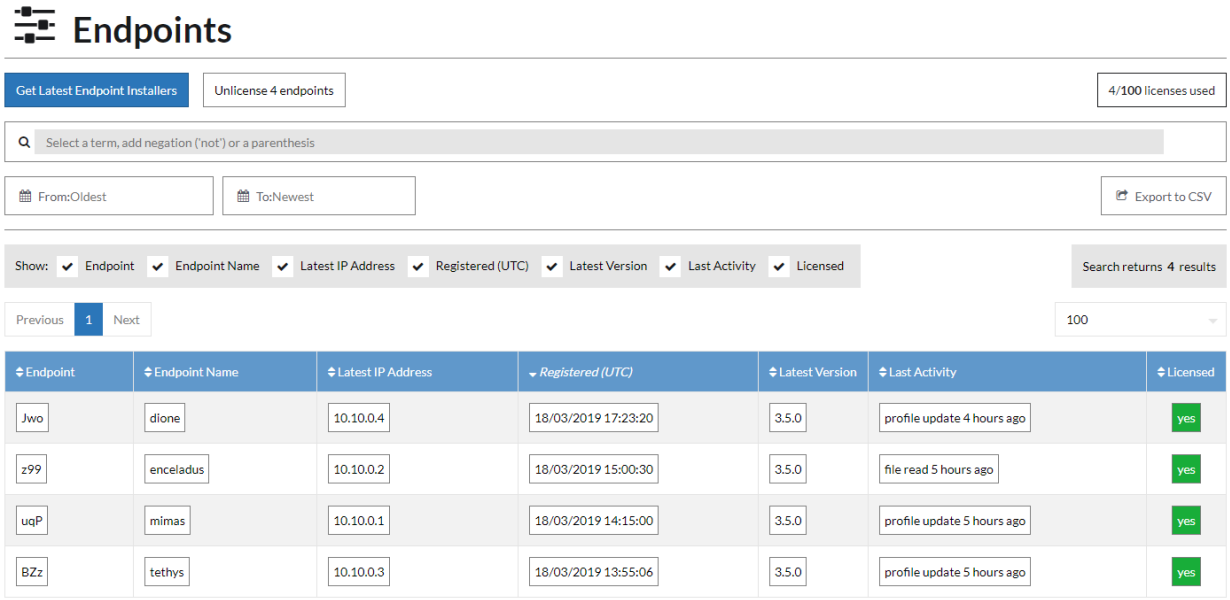
Admin

This section describes the options that are available in the **Admin** section in the FortiInsight UI.

Endpoints

The **Endpoints** page (**Admin > Endpoints**) displays the endpoints that are currently deployed, along with their latest activity. You can select the information that is displayed on the page, such as **Endpoint ID**, **Latest IP Address**, and **Last Activity**.

The following image shows an example of the **Endpoints** page:



Unlicensing endpoints

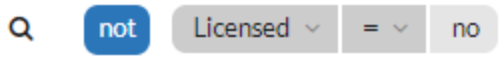
To unlicense old endpoints, click the **Unlicense endpoints** option. You can select this option to replace old endpoints with new ones.

You can unlicense endpoints in bulk by using the search bar and calendar filters to specify the group of endpoints you want to unlicense. For example, to unlicense a group of endpoints that have not been active past a certain date, select the date in the **To:** calendar field and leave the **From:Oldest** calendar field as is. Once the endpoints are filtered to the desired group, click the **Unlicense endpoints** option.

Hiding unlicensed endpoints

To hide unlicensed endpoints, first create a NOT modifier by typing "not" into the search bar and pressing Enter. Then, create a search pill that says "Licensed = no".

The following is an image of how the search pill should look:



Accounts

The **Accounts** page (**Admin > Accounts**) displays user accounts that have access to the FortiInsight UI. You can create new user accounts, disable accounts, and change account passwords.

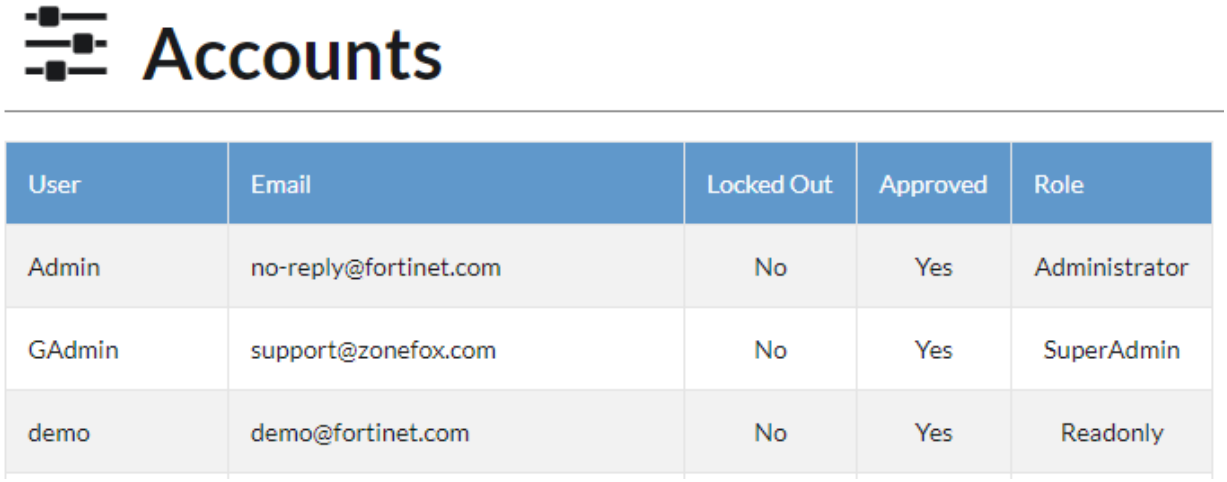
To create a new user, click **New User**.

The following role options are available:

- **Administrator**: Full access, including performing administrative tasks.
- **User**: Partial access, minus the ability to create users.
- **Readonly**: Not allowed to do any change actions, such as updating policies or the dashboard. The user is limited to viewing the collected data.

Account passwords must be at least eight characters. Fortinet recommends that you use a long, randomly generated, string as your password and record it in a password manager.

The following image shows an example of the **Accounts** page.



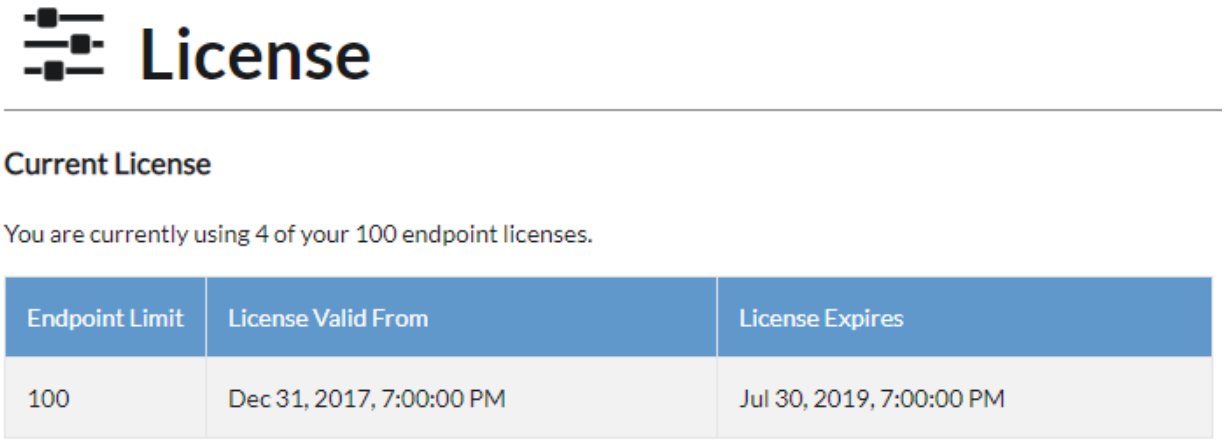
License

The **License** page (**Admin > License**) displays details about the current FortiInsight license, including an endpoint count and the license validity period.

One month before your license is due to expire, a license expiry warning is displayed in a ribbon at the top of the FortiInsight UI. If you do not renew your license, FortiInsight stops working one month after the expiration date.

If you have questions about your FortiInsight license, contact your account manager.

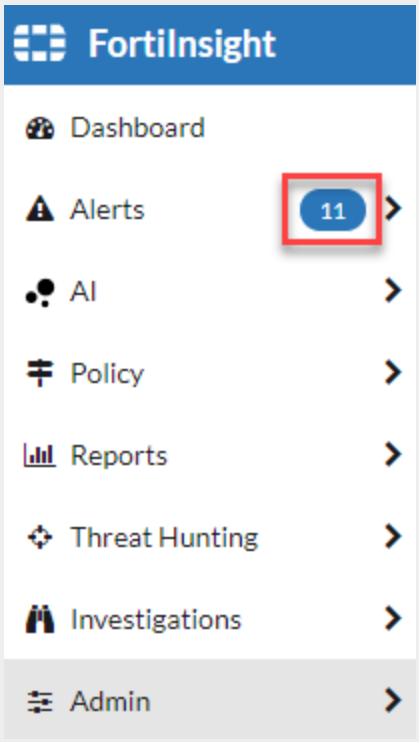
The following image shows an example of the **License** page.



Preferences

To set FortiInsight UI preferences, click the username icon in the top right of the FortiInsight UI and select **Preferences**.

Setting	Description
Email	Add or change an email address.
Notifications	Select the notifications that you want to turn on. If you want help bubbles to appear in the FortiInsight UI, select the **Hover Help Bubbles** option.
Badges Refresh Time	Set the refresh time for delta badges. Delta badges appear on the left menu in the FortiInsight UI and show you the number of events (**Threat Hunting** pages) or alerts (**Policy** pages) that have been generated since you last visited these pages. Badges show you a quick overview of what is going on across your network. After you visit the page, the badge disappears, and FortiInsight resets the event count. The following image shows an example of a delta badge.

Setting	Description
	

The following image shows an example of the **Preferences** page: