



FortiInsight Cloud - Administration Guide

Version 21.2

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



September 17, 2021

FortiInsight Cloud 21.2 Administration Guide

52-640-543474-20201214

TABLE OF CONTENTS

Change log	6
Introduction	7
What's new in FortiInsight Cloud version 21.2	7
In Case You Missed It (ICYMI) FortiInsight 21.1	11
Related resources	12
How FortiInsight works	13
Solution architecture	13
Secure storage	14
FortiInsight Cloud deployment and activation	15
Deploying FortiInsight Cloud	15
Activating FortiInsight Cloud entitlement	15
FortiInsight agent installation	17
Prerequisites	17
Downloading the latest endpoint agent installer	17
Installing the FortiInsight agent for Windows	17
Package management installation	18
Installing the FortiInsight agent for MAC OS	20
Package management installation	20
Verifying that the agent is reporting to the FortiInsight Cloud service	21
Troubleshooting	21
Searching	24
Modes	24
Design	24
Plain text	26
Limiting searches to a specific date range	26
Copying and pasting search queries	27
Deleting a search pill	27
Clearing a search	27
Last searches	27
Sticky searches	28
Finding related events	28
Summary tables	29
Converting a threat hunting search into a policy	29
Table settings	29
Threat hunting	31
Collections	32
Creating a collection	32
Refreshing a collection	32
Taking snapshots of searches	32

Policies	33
Creating a policy	33
Editing a policy	34
Retrospective policy breaches	34
Frameworks and labels	34
Out-of-the-box policies	35
Alerts	36
Policy alerts	36
AI alerts	36
Timeline	36
Searching alerts	37
Finding related alerts	38
Alert details	38
AI	39
AI scoring	39
Feedback	39
AI tags	40
Using AI tags	40
Change tag risk setting	41
AI training	41
AI settings	41
Dashboard	42
Dashboard Controls	42
Custom Dashboard	42
Widget Types	43
Filtering Widgets	44
Widget Controls	44
Forensic Activity Dashboard	45
Alerts Dashboard	45
Data Flow Dashboard	46
Applications Dashboard	47
Notable Users Dashboard	47
Reports	49
Threat Report	49
Threat Report recommendations	49
Threat Report interactive elements	50
Threat Report export	50
Networking	52
Networking statistics	52
Map	52
Investigations	54
Creating or Adding to Investigations	54
Using Investigations	54

Investigation Timeline	55
User Timeline	56
Contexts	59
User Contexts	59
Collecting the Information	59
Admin	64
Endpoints	64
Unlicensing endpoints	64
Hiding unlicensed endpoints	65
Accounts	65
License	65
Preferences	66

Change log

Date	Change description
2021-09-17	FortiInsight Cloud 21.2
2021-02-26	FortiInsight Cloud 21.1
2020-12-14	FortiInsight Cloud 6.4.0 document update to FortiAgent Installation .
2020-10-09	FortiInsight Cloud 6.4.0 document release. FortiInsight Cloud has been separated from FortiInsight.
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 Cloud version 21.2

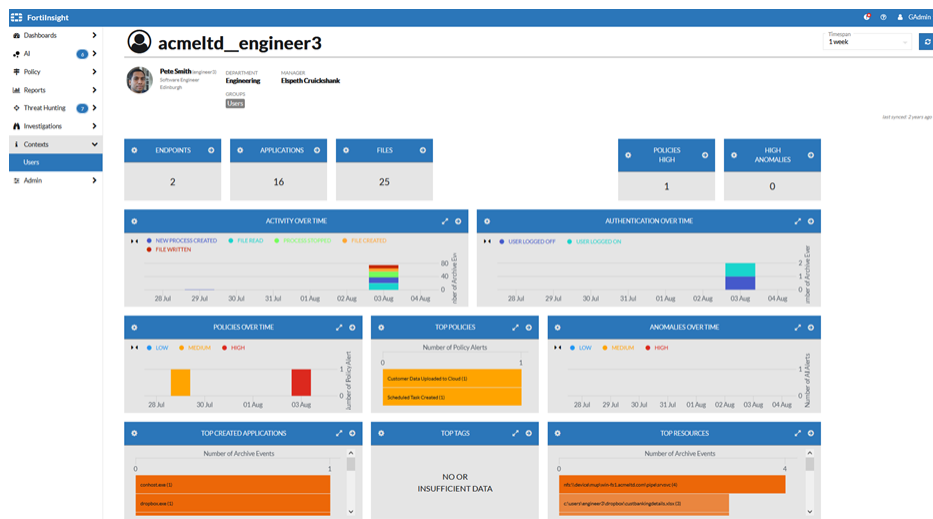
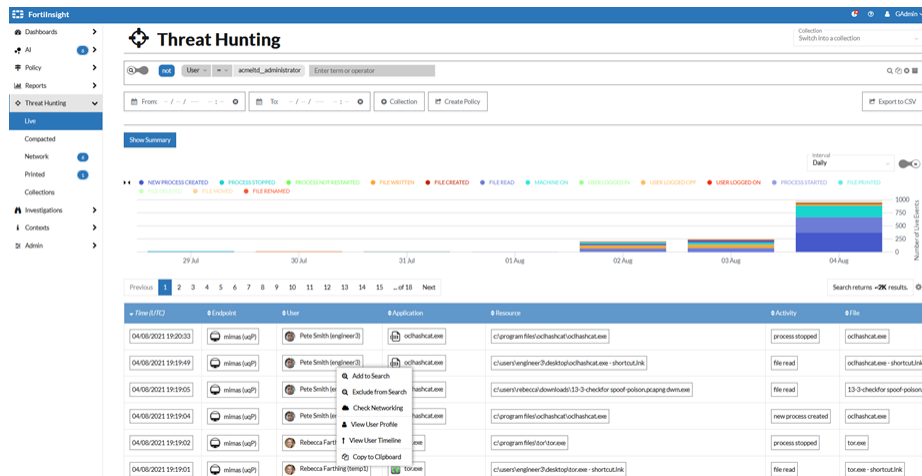
The following table lists new features and enhancements in FortiInsight Cloud version 21.2.

Feature	Description
Enhanced User Profile / Timeline	<ul style="list-style-type: none">• User Context Dashboard. A dashboard giving a high level overview of user activity.• User Context Timeline• User Context Details• User Context Tracking
Updated Policies	The following policies have been updated to reduce noise: File Downloaded Through a LOLBAS Binary PSEXec Executed On All Machines In Domain

Enhanced User Profile / Timeline

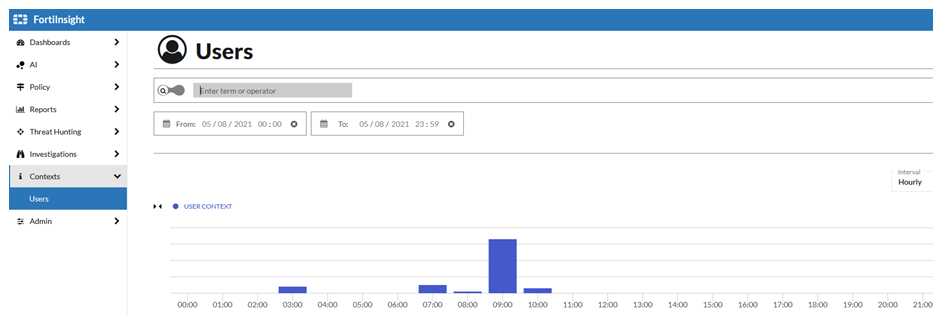
User Context Dashboard

For example, from **Threat Hunting > Live**, right click on the user and select **View User Profile**. This now displays the user profile in a widget style, like the FortiInsight Dashboard. Widget data can be exported to file, maximised for viewing or drill down to view the low-level data.

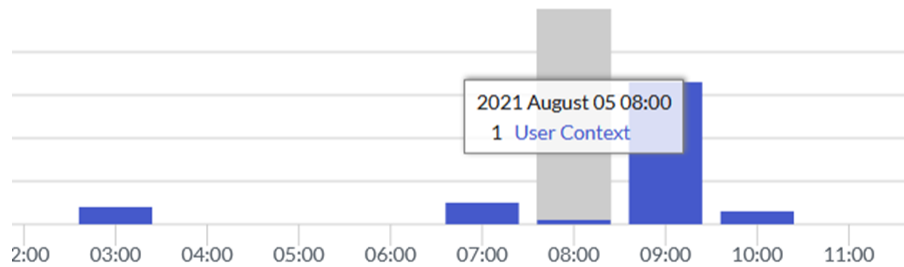


User Context Timeline

From **Contexts > Users** on the navigation pane. User activity is shown on a new timeline chart, detailing the number of active users at a given time.



Hovering over the bar will highlight the number of users.



Double clicking on the bar will display enhanced user information for those users.

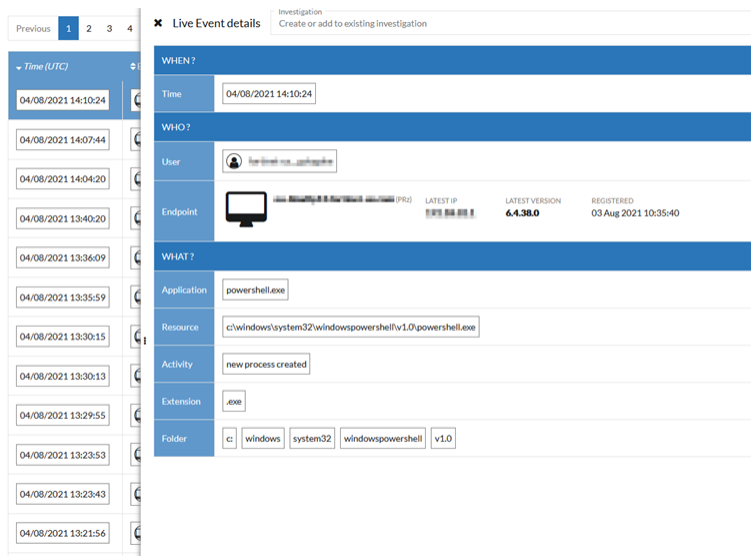
Such as:

- **Department**—Corporate department the user works in.
- **Manager**—Full name of the user's manager. Click to navigate to the manager's user profile.
- **Status**—Whether the user's account is active, disabled.



User Context Details

From **Contexts > Users** on the navigation pane. Previously, hovering over the user's name displayed the user context details. Now, clicking on the user name field displays the details in a standardized view.

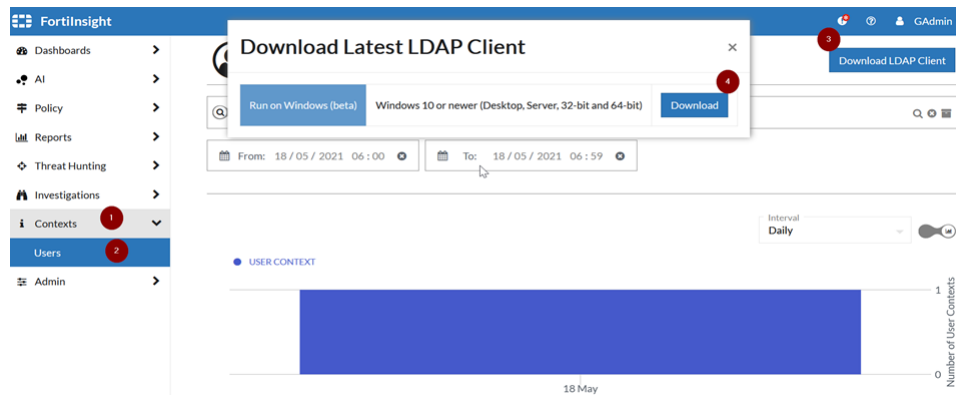


User Context Tracking

The LDAP agent allows you to sync your Active Directory to FortiInsight. Its aim is to increase the effective searches based on individual users, their managers, department and location.

To install the agent

1. Go to **Contexts**.
2. Select **Users**.
3. Select **Download LDAP Client**.
4. Click **Download**.



FortiInsight Agents

Feature	Description
MAC Connector[DH1]	<ul style="list-style-type: none"> • Adds support for MacOSX 11 “Big Sur” • Integrates with Endpoint security framework provided by MacOSX • All “new process created” activities will now report the command line arguments used to start the process
Windows Connector	<ul style="list-style-type: none"> • Support for “shift-delete” on files, or folders, has now been added ensuring these are reported correctly as “file deleted” events. • You can now ensure that the endpoint agent will verify SSL/TLS certificates before attempting to send data. • Added further enhancements to “file uploaded” and “file downloaded” events. • Support added for very short-lived process, to ensure that collection is not disrupted.

Mac Connector

Endpoint Security Framework

The MacOSX connector now supports directly with the Endpoint Security Framework provided by Apple. Internally, this ensure that all events are now collected via this method rather than utilising a custom Kext module. It also allows support for MacOSX 11 (Big Sur).

Command Line Arguments

Command line arguments, if applicable, are now shown for each Mac event, to standardise agent collection of data.

Time (UTC)	Application	Resource	Activity	File	Command Line Arguments
05/08/2021 09:39:08	sh	/bin/sh	new process created	sh	sh -c /usr/bin/dsccacheutil -flushcache; /usr/bin/killall -hup mdnsresponder;

Windows Connector

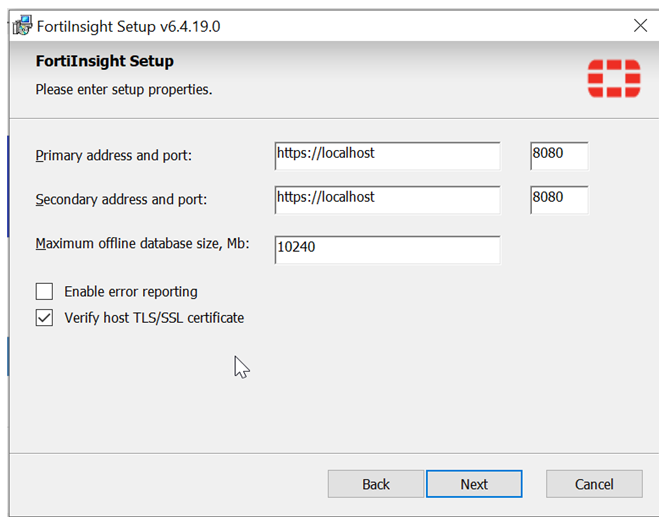
Files Deleted Event for Shift Delete

Shift delete operations and removable media deletes have been added to the windows connector and are shown as **File Deleted** operations in FortiInsight.

Application	Resource	Activity	File	Extension	Folder
explorer.exe	c:\mydeletefolder\testfilefordeletion.txt	file deleted	testfilefordeletion.txt	.txt	c:\ mydeletefolder
explorer.exe	c:\mydeletefolder\testfilefordeletion2.txt	file deleted	testfilefordeletion2.txt	.txt	c:\ mydeletefolder

Verify SSL Certificate

When installing the windows agent, if the **Verify host TLS/SSL certificate** box is ticked any connection to the host will be blocked if the SSL/TLS certificate is invalid or the url does not match the certificate. This is disabled by default.



In Case You Missed It (ICYMI) FortiInsight 21.1

<https://docs.fortinet.com/document/fortiinsight-cloud/21.1.0/release-notes/535328/introduction>

The following table lists new features and enhancements in FortiInsight Cloud version 21.1.

Feature	Description
User Contexts & LDAP connector	Enhanced User metadata, for all collected users. The collection of this data will utilize the new FortiInsight LDAP connector to gather required user metadata which includes, but not limited to, Display Name, Job Title, Department and Office location. You can then use these new meta fields across FortiInsight whether that is creating policies or general threat hunting searches.
Most Notable Users	New Most Notable Users Dashboard provides you with a single dashboard for all the highest risk users within your organization. Any user with a high severity policy or anomaly will feature here.
FortiGuard GEO IP Database	FortiInsight now uses the FortiGuard GEO IP database to resolve location data based on collected IP Addresses sent by endpoints.
Trend Charts	Trending charts have been added to all Threat Hunting views allowing you to view, highlight, and investigate via the trending charts.
Investigation Timeline	Added simplified view of Investigations within FortiInsight - showing you a simple easy to understand the flow of your created investigations. As part of this enhanced view, we have added the ability to add Event types into the investigation (Live, Printed, Network) allowing you to investigate the entire user threat landscape.
Collection Source	Easily switch into your Collections from any supported data view.
Dashboard Management Enhancements	Standardized all charts across the dashboard, adding better functional controls such as import/export, clone, and enlarge. You can now also export an embedded dashboard and make it your custom one by importing.

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 thirty 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 Cloud 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.

Serial Number	Description	Start Date	End Date	Number of Seats	Region	Created	
	FortiInsight Deployment	Tuesday, June 18, 2019	Wednesday, June 17, 2020	500			Activate
	FortiInsight UEBA Service	Thursday, November 14, 2019	Friday, November 13, 2020	500	Europe (Ireland)	Tuesday, September 29, 2020	Edit

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

FortiCloud dhart@fortinet.com

FortiInsight 923180 - ACME Ltd

Serial Number	Description	Start Date	End Date	Number of Seats	Created	
fueba00000000107	FortiInsight Deployment	Tuesday, June 18, 2019	Wednesday, June 17, 2020	500	Monday, February 17, 2020	Save
<div style="display: flex; justify-content: space-between;"> <div> <p>Console CIDR Block(s)</p> <p><small>CIDR ranges of IP addresses able to access the console</small></p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">187.99.45.12/32</div> <div style="background-color: #007bff; color: white; padding: 2px 5px; text-align: center;">+</div> </div> <div> <p>Collector CIDR Block(s)</p> <p><small>CIDR ranges of IP addresses from which the server will accept event data</small></p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">187.99.45.12/32</div> <div style="background-color: #007bff; color: white; padding: 2px 5px; text-align: center;">+</div> </div> </div>						
FUEBA00000000130	FortiInsight UEBA Service	Thursday, November 14, 2019	Friday, November 13, 2020	500		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
- d. Region selection



Region deployment cannot be changed after initial deployment.

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 Cloud will launch in a new browser tab

FORTINET ONE testuser00108@163.com
Unified Cloud Services Login

FortiInsight 906203 - company 906203

Current stacks:

Serial Number	Description	Start Date	End Date	Number of Seats	Created	
fueba00000000101		Tuesday, January 1, 2019	Wednesday, January 1, 2020	500	Thursday, May 23, 2019	Go To Insights

FortiInsight agent installation

Follow these procedures to install the FortiInsight agent on either supported versions of Windows or Mac OSX.

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 latest 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. For Windows installation select **Download** on the **Windows File Agent** section.
 - Follow the steps for [Installing the FortiInsight agent for Windows](#) below.
4. For Mac installation select **Download** on the **Mac File Agent** section.
 - Follow the steps for [Installing the FortiInsight agent for Mac OS](#) below.

Endpoint agent download window example

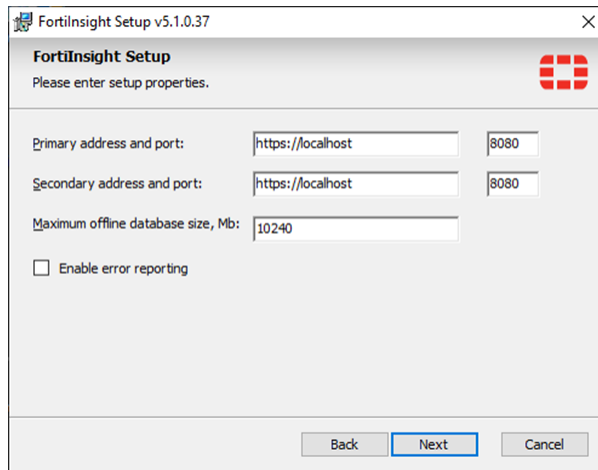
Download Latest Endpoint Agents			×
Windows File Agent	Windows 7 or newer (Desktop, Server, 32-bit and 64-bit)	Download	
Mac OS File Agent	Mac OS Version 10.9 (Mavericks) to 10.15 (Catalina)	Download	

Installing the FortiInsight agent for Windows

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**.
8. Verify that communication between the FortiInsight Mac OS agent and the FortiInsight backend is working properly by following the [verification process](#).

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.

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.
<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.

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.
/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
```



When using a deployment technology such as SCCM, you must make sure that the package (cms.msi) is available on the target machine - it must also have permissions for SCCM runners to interact with the directory on the target.

Installing the FortiInsight agent for MAC OS

Follow these steps to install and run the FortiInsight agent.

1. Unzip the compressed agent package
2. Double click the FortiInsight.pkg, package file and follow the install wizard.
3. Follow the instructions to set the [FortiInsight Cloud Service settings](#) for the Mac OS Agent.

Package management installation

Installing or updating the agent using Installer

1. Unzip the compressed agent package.
2. In a Terminal window, change to the folder containing the FortiInsight.pkg file and run the installer:

```
sudo installer -pkg ./ FortiInsight.pkg -target /
```
3. Follow the instructions to set the [FortiInsight Cloud Service settings](#) for the Mac OS Agent.

Note: After installation, the daemon is immediately launched.

Uninstalling the FortiInsight Mac OS Agent

To uninstall the FortiInsight Mac OS Agent, run the following steps:

1. `sudo launchctl unload /Library/LaunchDaemons/com.fortinet.fortiinsight.daemon.plist`
2. `sudo launchctl unload /Library/LaunchAgents/com.fortinet.fortiinsight.agent.plist`
3. `sudo -u root launchctl unload /Library/LaunchAgents/com.fortinet.fortiinsight.agent.plist 2>/dev/null`
4. `sudo rm -r /Library/Extensions/FortiInsight.kext`
5. `sudo touch /Library/Extensions/`
6. `sudo rm -r /usr/local/libexec/fortiinsight`
7. `sudo rm -r /usr/local/libexec/fortiinsightagent`
8. `sudo rm /Library/LaunchDaemons/com.fortinet.fortiinsight.daemon.plist`
9. `sudo rm /Library/LaunchAgents/com.fortinet.fortiinsight.agent.plist`
10. `sudo defaults delete com.fortinet.fortiinsight`

Setting the FortiInsight Cloud Service settings

1. To configure the agent to connect to your Collector Server, you must set the correct URL to be used. In a Terminal window, run the following command supplying the URL in the correct format including the port number and ending in `/api/`, for example `https://fortinet.fortiinsight.cloud:8080/api/`.

```
sudo defaults write com.fortinet.fortiinsight ServerURL -string <Collector_Server_URL>
```

Note: Settings are only re-read on daemon launch, so you must restart the daemon (or reboot the machine) for changes to take effect.

In a Terminal window, to restart the daemon, run:

```
sudo launchctl unload /Library/LaunchDaemons/com.fortinet.fortiinsight.daemon.plist
```

```
sudo launchctl load /Library/LaunchDaemons/com.fortinet.fortiinsight.daemon.plist
```

2. After a successful installation, there should be two processes running: FortiInsight, FortiInsightAgent.
3. Verify that communication between the FortiInsight Mac OS agent and the FortiInsight backend is working properly by following the [verification process](#).

Parameter	Description
<Collector_Server_URL>	The address of the primary FortiInsight Cloud service.

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](#) for more information about steps that you can take to determine why the agent is unable to send data correctly.

Troubleshooting

Whitelist files if antivirus software interferes with FortiInsight on Windows

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 on Windows

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 FortiInsight Cloud service details in the FortiInsight defaults on Mac OS

In a Terminal windows run the following:

```
sudo defaults read com.fortinet.fortiinsight
```

This will print the last known setting for the defaults for the FortiInsight Mac OS Agent, example:

```
{
  ServerURL = "https://fortinet.fortiinsight.cloud:8080/api/";
}
```

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

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 JSON 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 for Windows

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.

How to gather data for a Fortinet Support request for Mac OS

If you need to contact [Fortinet Support](#) for help, gather the following data and have the `FortiInsight.log` file ready to share with Fortinet Support.

1. Read the [current settings](#) from the defaults and ensure they are correct
2. Collect the latest log file from `/var/log/FortiInsight.log`. 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:

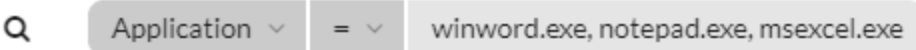
Criteria	Options	Description
Field to search	The list of available search fields varies according to the type of data that you are searching for.	Select the field that you want to search.
Type of comparison to make	<ul style="list-style-type: none"> • Less Than • Greater Than • Greater Than or Equal To 	<p>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.</p> <p>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.</p>

Criteria	Options	Description
	<ul style="list-style-type: none"> Less Than or Equal To 	
Value to search for		<p>The value that you want to search for.</p> <p>You can enter more than one value by separating the values with commas.</p>
	Terms	<p>This is a text-based search. The search pill defaults to this type of search.</p> <p>You can use the following special characters for additional search control:</p> <ul style="list-style-type: none"> 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	<p>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</p>

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 26](#))

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**.

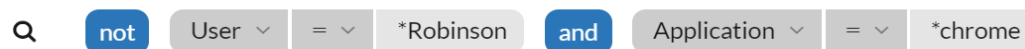
Logical operators

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**.

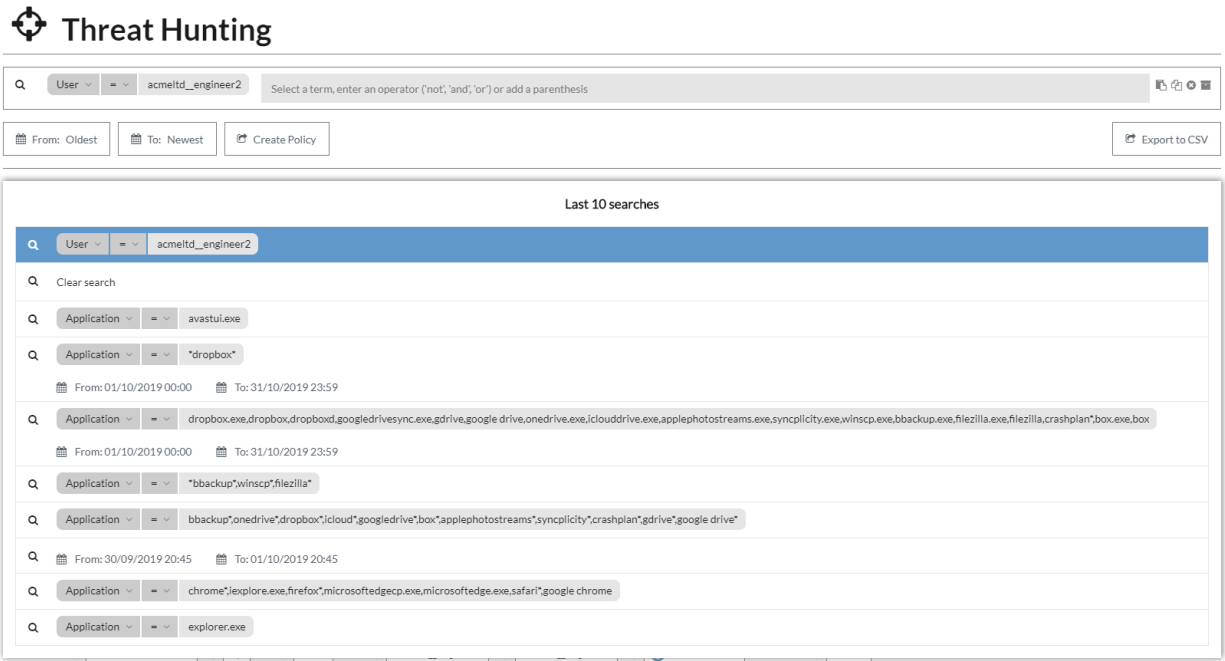
Clearing a search

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.

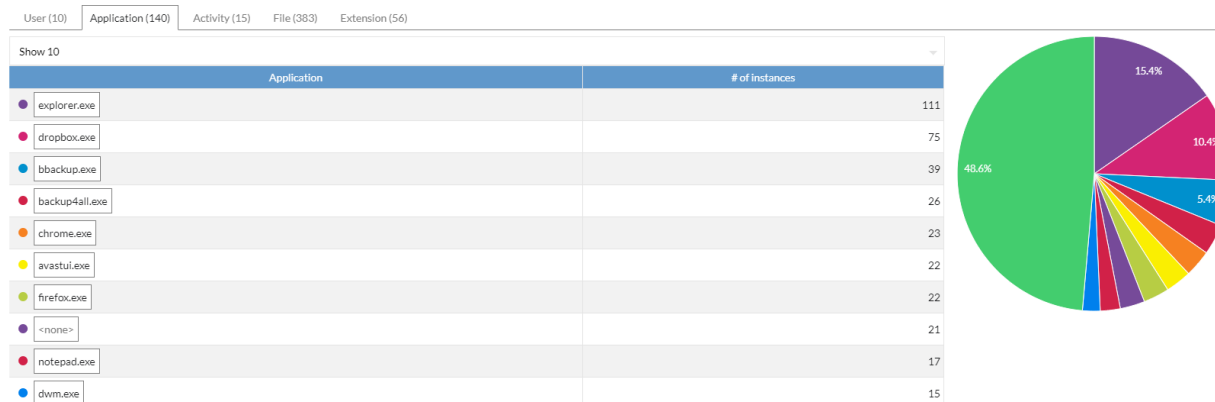
1. Right-click on the timestamp of an event.
2. Select **Find Items Around This Time**.

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:

<input checked="" type="checkbox"/> Time (UTC)	<input checked="" type="checkbox"/> Endpoint	<input checked="" type="checkbox"/> Endpoint Name
<input checked="" type="checkbox"/> User	<input checked="" type="checkbox"/> User Name	<input checked="" type="checkbox"/> Application
<input checked="" type="checkbox"/> Resource	<input checked="" type="checkbox"/> Activity	<input checked="" type="checkbox"/> File
<input checked="" type="checkbox"/> Extension	<input checked="" type="checkbox"/> Folder	<input checked="" type="checkbox"/> Port Name
<input checked="" type="checkbox"/> Printer	<input checked="" type="checkbox"/> Pages Printed	<input checked="" type="checkbox"/> Bytes Printed
<input checked="" type="checkbox"/> 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.

Time (UTC)	Endpoint	User Name	Application	Resource	Activity
03/04/2019 13:13:56	uqP	acmeltd_engineer2	chrome.exe	c:\users\charlotte\Documents\master_cust_llst.xls -> tcp://bronyfanclub.turkey.tur	file uploaded

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

Repeated	First Seen	Endpoint Name	User Name	Application	Resource	Activity
20 times	01/03/2019 03:34:22	mimas	acmeltd_contractor1	notepad.exe	rmc:\f\copytolremdrive\newappbeta.cs	file written

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.


New Policy
Save Policy

Name	Give your policy a name
Description	Give your policy a description
Frameworks	Frameworks to assign your policy to
Enabled	<input checked="" type="checkbox"/>
Severity	10
Emails to notify	e.g. you@yourdomain.com
Labels to assign	e.g. potential leavers

Policy to build

Search
Raw EPL

Q Select a term, add negation ('not') or a parenthesis

Retrospective policy breaches: 75 alerts would have been generated

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:

Retrospective policy breaches: 40 alerts would have been generated

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.

Enabled	Name	Severity	Framework	Label	Description
<input checked="" type="checkbox"/>	Customer database changes	90	GDPR	Customer Data	Looking for unauthorised changes to the customer database
<input checked="" type="checkbox"/>	Uploads of sensitive data to non-EEA countries	70	GDPR	<none>	<none>
<input checked="" type="checkbox"/>	HR Data Access	50	GDPR	Restricted Access	Unauthorised access of staff files
<input checked="" type="checkbox"/>	Customer Data Uploaded to Cloud	90	GDPR	Customer Data	Captures specific customer data sources being copied to cloud storage providers
<input checked="" type="checkbox"/>	Protect Sensitive Folders - Board Minutes	40	ISO27001 ZoneFox	Sensitive Data	Monitor unauthorised access to Board Minutes folder
<input checked="" type="checkbox"/>	Segregation of Duties	60	ISO27001	Folder Access Segregation of Duties	Ensure only authorised personnel are accessing sensitive folders
<input checked="" type="checkbox"/>	Removable Media Audit	10	ISO27001	Removable Media Use	Audit use of removable media

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 non 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

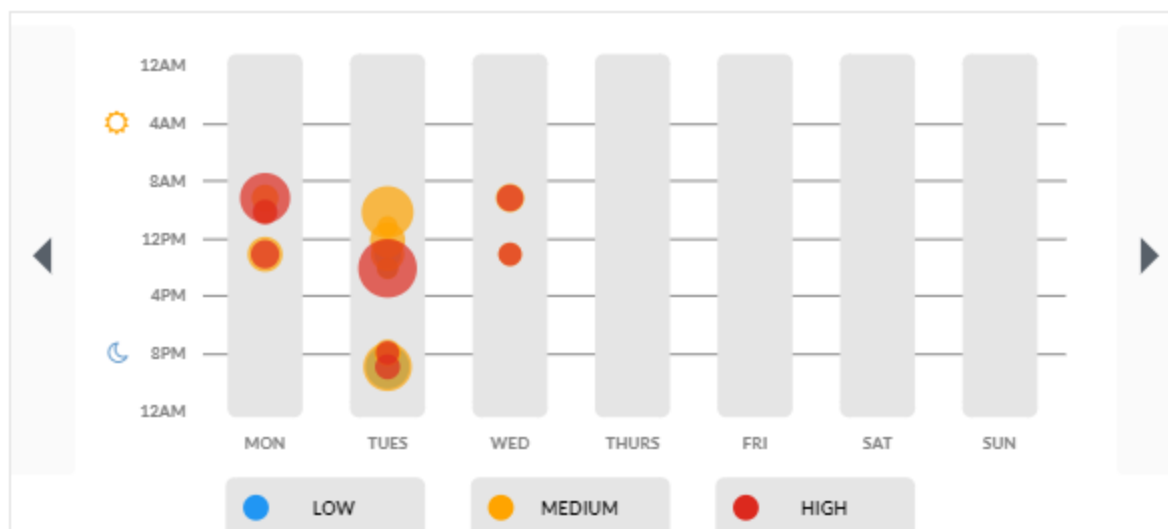
The **AI Alerts** page shows alerts that FortiInsight AI generates. If there are alerts on this page, it means that FortiInsight AI detected some anomalous behavior based on one or more events, as well as any tags that you defined.

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.

Expand	Severity	Time (UTC)
	40	30/05/2018 09:12:24
1 more	60	31/05/2018 16:09:18
Hide	50	31/05/2018 16:15:23
		31/05/2018 16:15:23

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**.

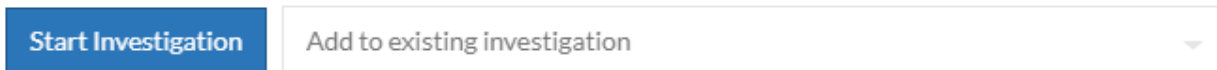
FortiInsight narrows the list to alerts that occurred within a five minute radius (five minutes before to five minutes after) of the alert that you selected.

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 an example of the **Feedback** column.

Users Entities Tags		
User	Alerts	Feedback
acmeltd_temp1	71	 
acmeltd_sales1	52	 
acmeltd_engineer2	46	 

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.

Tag browser_read

Delete Tag Back Save

Tag ID: browser_read

Tag Name: Browser Read (Upload)

Icon: Internet-explorer

Description: Matches events which are likely uploads from browser

Colour: ● ● ● ● ●

Enabled: ☒

Preview: BROWSER READ (UPLOAD)

Weighting: ▲ MEDIUM RISK

Field	Relation	Values (newline separated)	Delete
Application	does	equal	chrome.exe safari.exe microsoftedge.exe firefox.exe
Activity	does	equal	file read
Resource filename	does not	end with	zone.Identifier link url website

+ Add Rule

Note: Folders must be separated using the / (forward slash) character

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.

Weighting ▲ MEDIUM RISK

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.

Dashboard

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 six dashboards: one configurable Custom dashboard and five pre-defined dashboards (**Forensic Activity**, **Alerts**, **Data Flow**, **Applications**, and **Notable Users**).

Each dashboard contains a variety of widgets that provide information about events, users, and alerts.

Dashboard Controls

To export (custom, or pre-defined) dashboards, select the Export button. This will download the dashboard, plus all widgets currently available, in JSON format. You can then share this, with other analysts who can Import from the locally generated JSON file.



To change the timespan of the dashboard click on the Timespan dropdown, supported relative time selections are: **30 minutes**, **1 hour**, **6 hours**, **1 day**, **1 week**, **2 weeks**, **1 month**, **3 months**, and **All time**.

Selecting the refresh icon will refresh all widgets in the dashboard changing the relative time to now.



As well as export, on pre-defined dashboards, there is also the option to update your current custom dashboard to be the selected pre-defined one.



Custom Dashboard

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 New, name the widget, and select the type, data source, and field.

Widget Type	Description
Unique Count	Metric Type, providing the count of unique values of the selected data field.
Top N Table	Creates a bar chart, with a max of N records.
Series Over Time	Creates a line graph.
Stacked Bar Over Time	Creates a stacked bar graph using the values from the data field.
Top 100 Pie Chart	Create a pie chart.

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

Add a New Widget

Name your widget
NAME ME

Which data source?
Events

Which data field?
Activity

Type of Widget
Top N Table

Top Limit
20

PREVIEW OF WIDGET 'NAME ME' OVER THE PAST WEEK

Number of Archive Events

file read (212)

new process created (176)

process stopped (123)

file written (95)

file created (64)

file downloaded (34)

file uploaded (25)

Cancel
Q Add Search Filter
Add To Dashboard

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.

The following shows an example of Top event activities filtered to the group name users.

Add a New Widget ×

Name your widget	TOP ACTIVITY FROM ALL USERS IN GROUP USERS
Which data source?	Events
Which data field?	Activity
Type of Widget	Top N Table
Top Limit	20

☒ GroupName = Users Enter term or operator 🔍

PREVIEW OF WIDGET 'TOP ACTIVITY FROM ALL USERS IN GROUP USERS' OVER THE PAST WEEK

Number of Archive Events

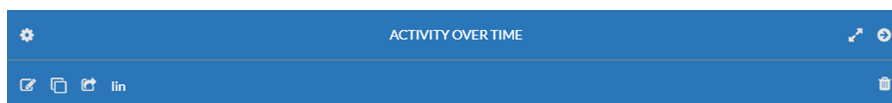
Activity	Count
file read	199
new process created	145
process stopped	109
file written	84

Cancel 🔍 Remove Search Filter Add To Dashboard

Widget Controls

There are some basic controls for managing your widgets on custom dashboards - these include:

- **Settings:** Providing access to the following, in the order seen below.
 - a. **Edit:** To edit the metadata around your widget - updating its type, data source and field selections. For the Top N widget, you can also control the number of records to display.
 - b. **Clone:** Cloning a widget into your custom dashboard, to help with create widgets from templates of existing ones.
 - c. **Export:** To export individual widgets to share these with any other analysts.
 - d. **Linear/Log:** Provided on any chart type widgets (Line, Stacked or Column) to update the view to a linear or logarithmic scale.
 - e. **Remove:** Remove this widget from the dashboard
- **Enlarge:** Allowing the widget to scale to full screen, providing you with a larger view to investigate the data
- **Go To:** Go directly to the data source, pre-filling the search filter provided, and the timespan selected.

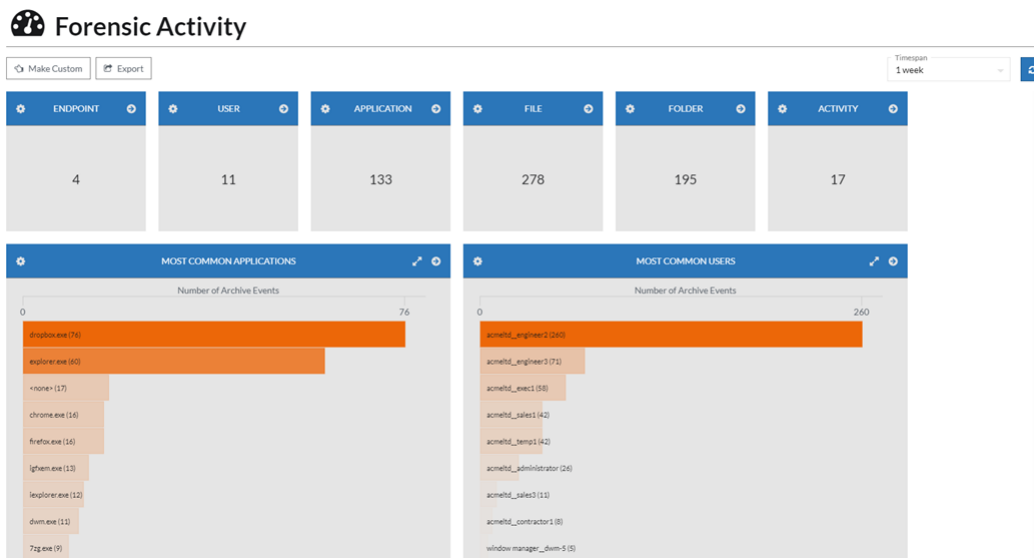


Forensic Activity Dashboard

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:

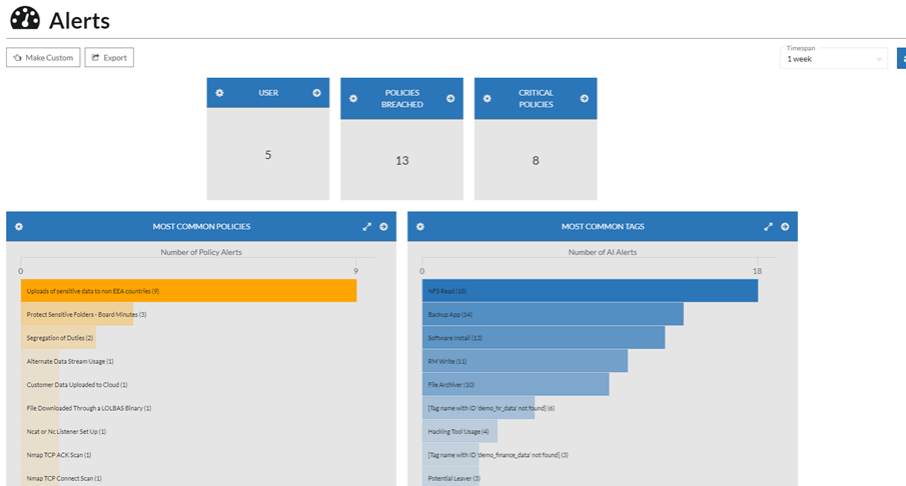


Alerts Dashboard

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:

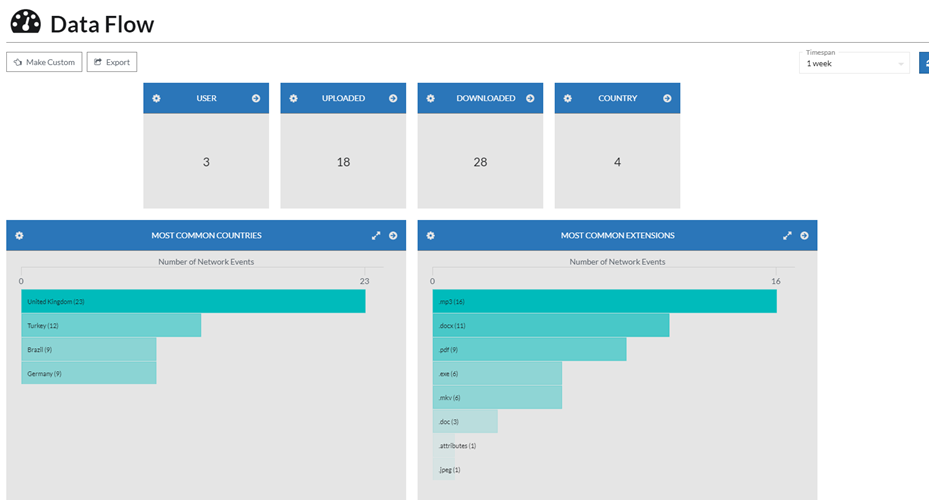


Data Flow Dashboard

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.

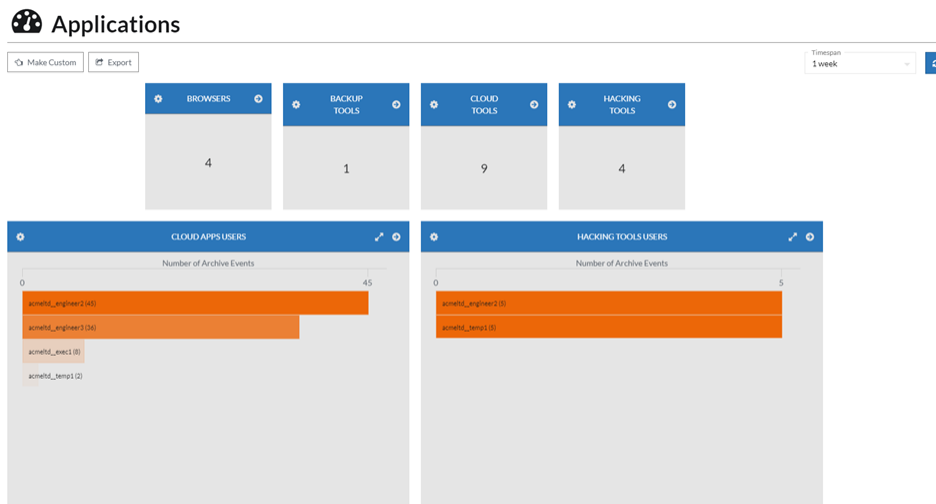
The following image shows an example of the Data Flow dashboard:



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:



Notable Users Dashboard

The notable users' dashboard provides an easy way to collate together the riskiest users into a single dashboard. The dropdown provides you with those users who have either fired a High severity Policy or AI Alert, ordered by the most occurrences.

Select the dropdown to change which user you are currently focussing on.

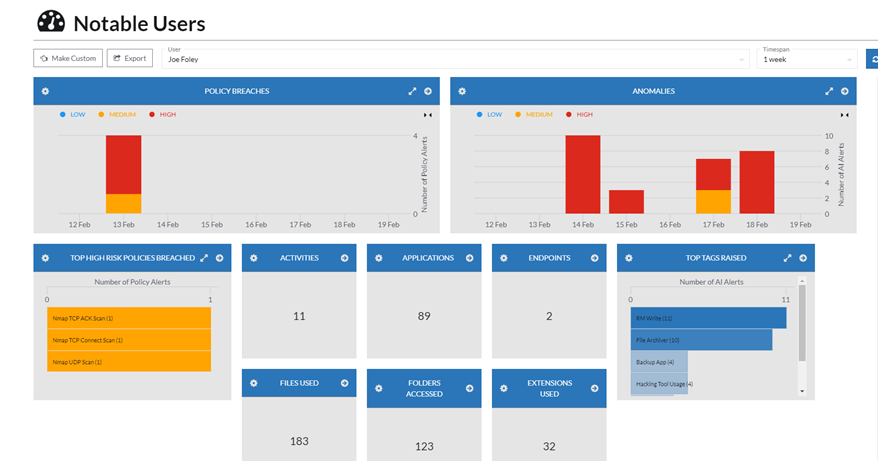


Once selected the dashboard will refresh automatically providing you with the following, across your chosen timespan:

- A trend of all Policy Alerts, stacked by severity.
- A trend of all Anomalies, stack by severity.
- The top high policies that have been associated with the user
- The top tags associated with the user
- Unique counts of
 - a. Activities
 - b. Applications

- c. Endpoints
- d. Files Used
- e. Folders Accessed
- f. Extensions used

The following image shows an example of the Notable Users Dashboard.



Reports

Threat Report

The **Threat Report** provides automated reports for various behaviors, from which you can export relevant 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**

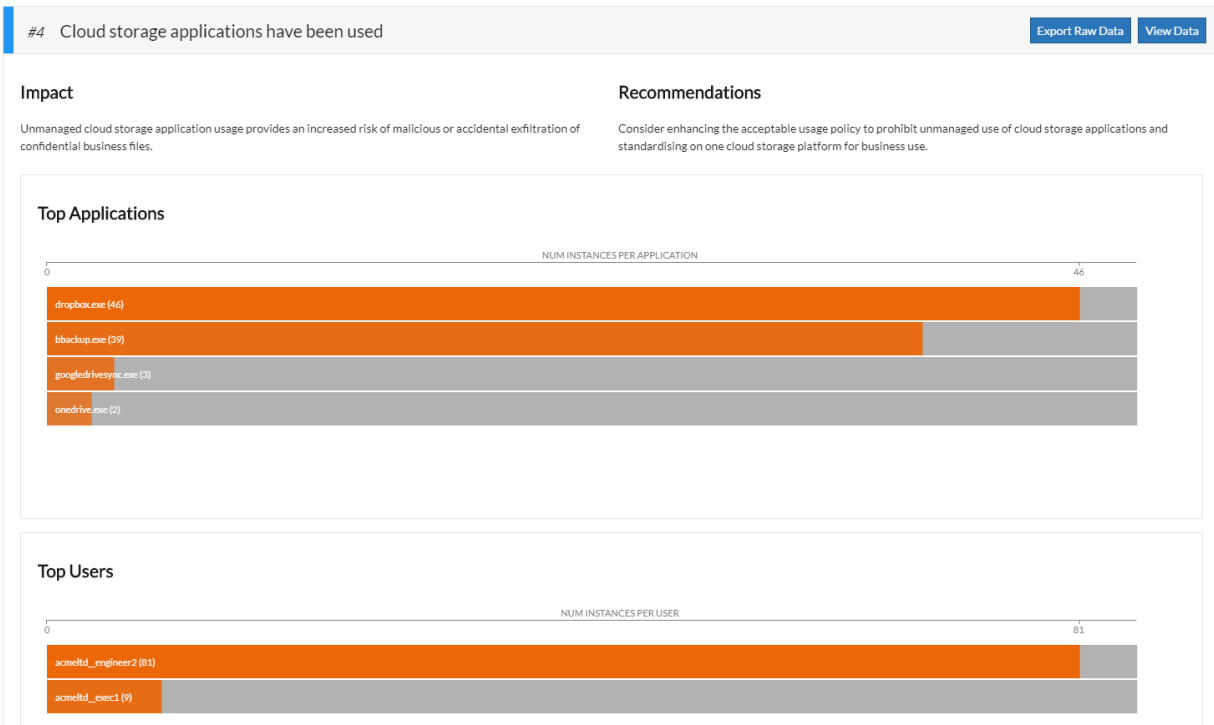
The following image shows an example of the **Threat Report** dashboard:



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:

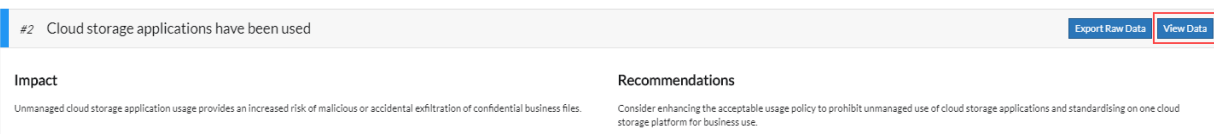


Threat Report interactive elements

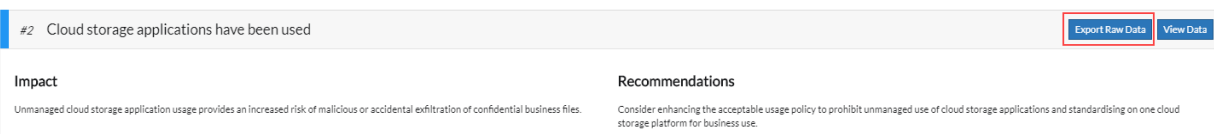
You can click individual fields in the bars graphs to jump to the **Threat Hunting** dashboard with the relevant search criteria already populated.

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.

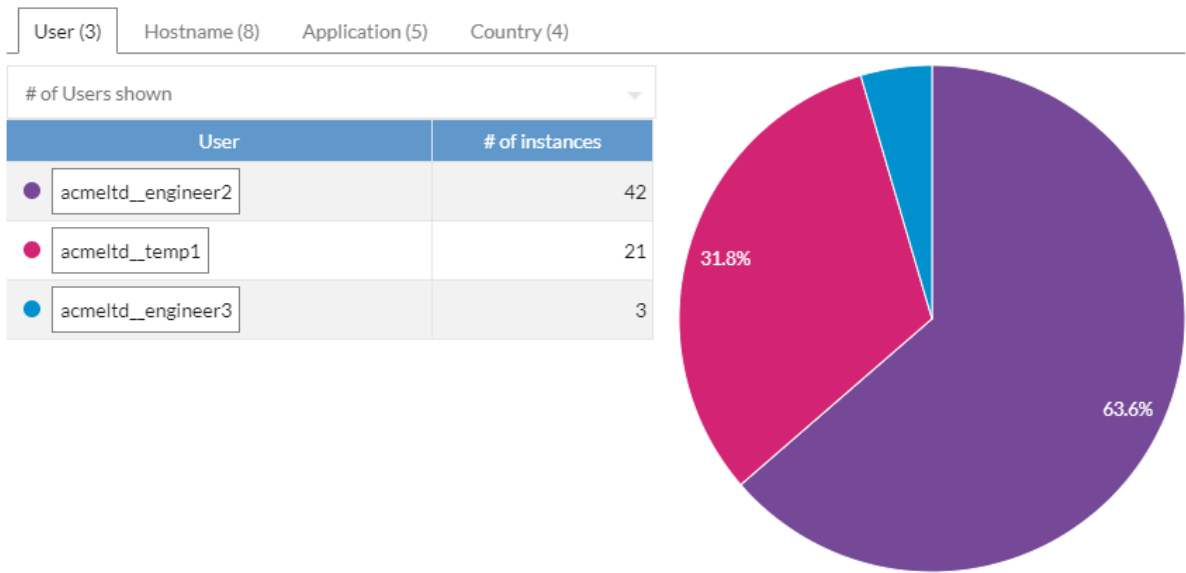
Networking

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:

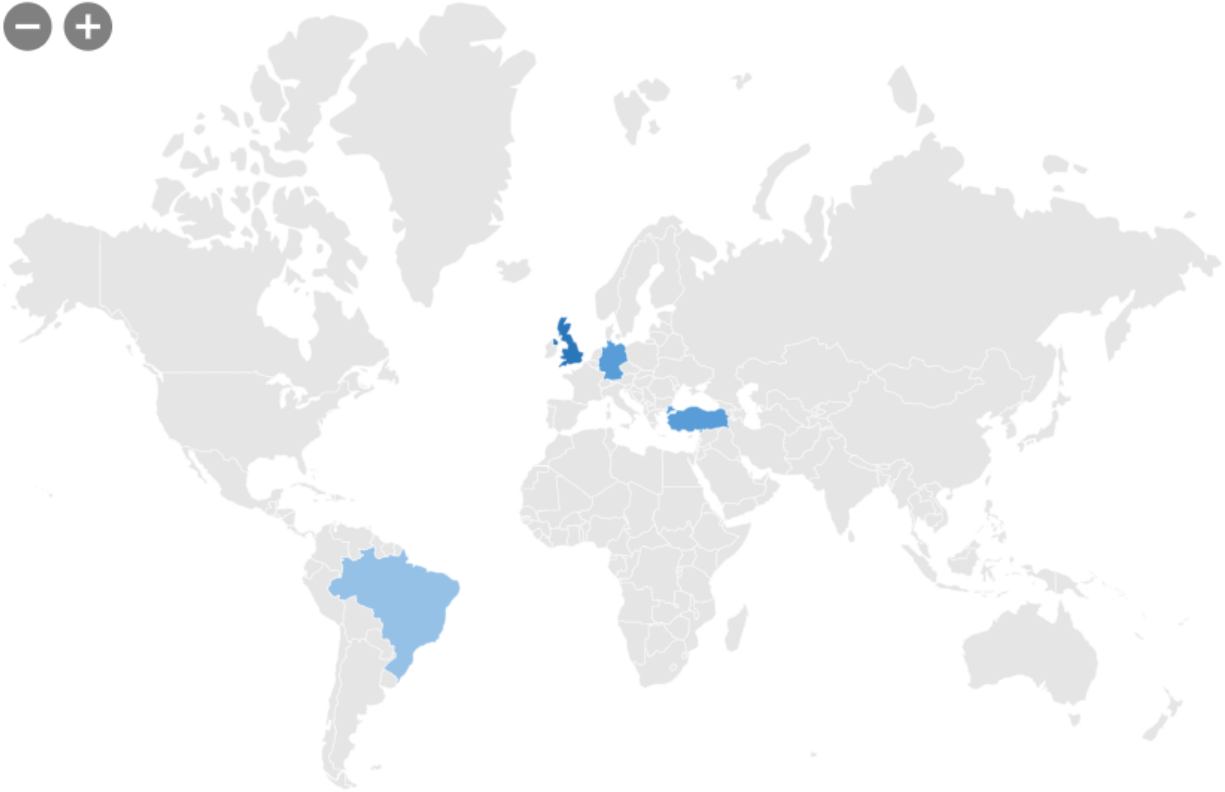


Map

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 and event information into a single timeline of activity.

Creating or Adding to Investigations

To add to an existing investigation, click on the **Create or add to existing investigation** dropdown on any alert or event details quick view. A dropdown will appear, listing any currently open investigations that have been created in the system, to create a new one - just type in a new then either hit the **enter** key or the select the Create button.

Add to existing view:



Create a new Investigation view:



Once this data has been added to the investigation, the system automatically redirects you to the new investigation.

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 selecting the dropdown, and choosing a new owner.
- **Status:** You can update the status of an investigation to Reported, No action, or Open.

You can also choose to Delete or Close investigations at any point. Once an investigation is Closed you can choose to Reopen to record more data against it in the future.

Investigation Timeline

The investigation provides you with a merged timeline of activity for your collated information - be it policy alerts, AI anomalies or indeed raw event logs. Selecting an individual timeline card will reveal the Quick View allowing you to see all information collected.

The screenshot displays the 'Financial Data Breach' investigation interface. At the top, it shows the owner 'GAdmin' and status 'Open', with 'Close' and 'Delete' buttons. Below this, a note states: 'This investigation was opened Wednesday 17th February, 2021, 19:59'.

The timeline on the left lists events from 17th Feb, 2021, 19:00 to 18:48. Key events include:

- 19:00: Breach of Financial Data Breach. Restricted Access (Score: 90)
- 19:00: Breach of Financial Data Breach. Restricted Access (Score: 90)
- 18:49: File written by acmetd_temp1 (Score: 51)
- 18:49: File written by acmetd_temp1 (Score: 51)
- 18:48: File read by acmetd_temp1 (Score: 44)
- 18:48: File read by acmetd_temp1 (Score: 44)
- 18:48: File read by acmetd_temp1 (Score: 44)
- 18:48: File read by acmetd_temp1 (Score: 44)

The right pane shows a 'Quick View' of the selected event, displaying network events, alerts, and a note added by GAdmin at 21:08: 'Add new note to Financial Data Breach'.

You can also add notes to your investigation ensuring additional context and commentary are recorded for an analyst.

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

Threat Hunting

Application = nc.exe Enter term or operator

From: -- / -- / ---- -- : -- To: -- / -- / ---- -- : -- Collection Create Policy Export to CSV

Show Summary Tabs

Show: ☒ Time (UTC) ☒ Endpoint ☒ Endpoint Name ☒ User ☒ User Name ☒ Application ☒ Resource ☒ Activity ☒ File ☒ Extension Search returns 18 results

☒ Folder

Previous 1 Next 100

Time (UTC)	Endpoint	Endpoint Name	User	User Name	Application	Resource
18/02/2020 19:16:05	uqP	mimas	acmeltd_contractor1	acmeltd_contractor1	nc.exe	c:\users\temp1\downloads\13-3-checkfor spoof-poison.pcapng dwn
18/02/2020 19:16:05	uqP	mimas	acmeltd_contractor1	acmeltd_contractor1	nc.exe	c:\program files\nc\nc.exe
18/02/2020 19:16:04	uqP	mimas	acmeltd_contractor1	acmeltd_contractor1	nc.exe	c:\program files\nc\nc.exe

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

Events within this Alert

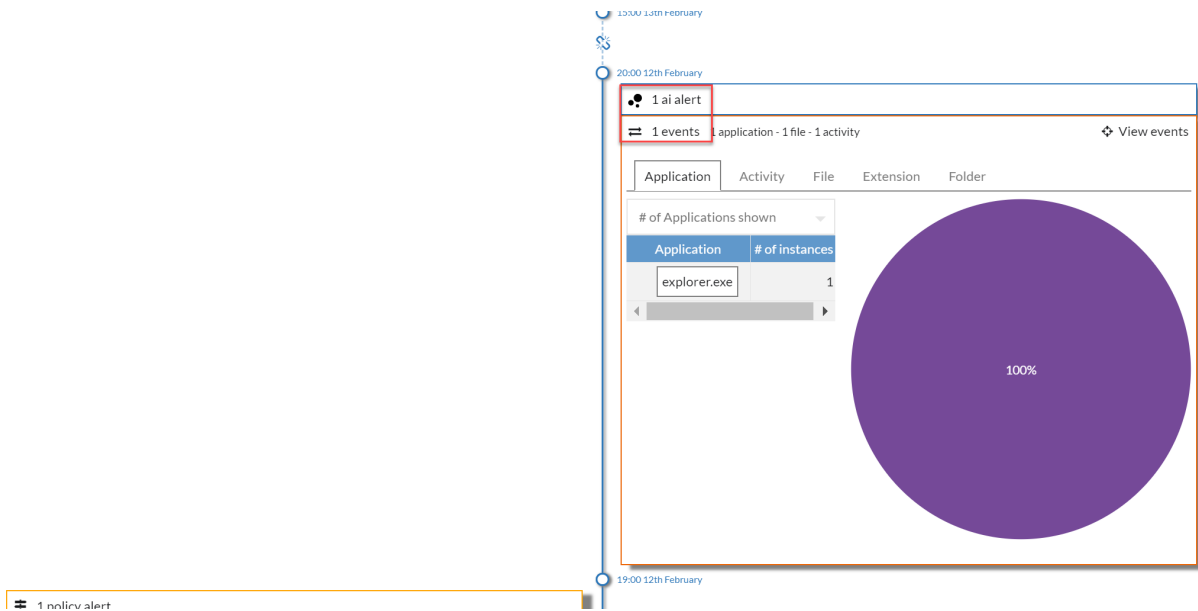
Date (UTC)	13/02/2020 19:12:22
Endpoint	uqP
Endpoint Name	mimas
User	acmeltd_contractor1
User Name	acmeltd_contr
Application	nc.exe
Activity	new process cre
Resource	c:\program files\nc\nc.exe

- Threat Hunt
- Check Networking
- View User Profile
- View User Timeline
- Copy to Clipboard

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.



Contexts

Contexts are the ability to provide additional metadata, or contextual information, around the raw telemetry collected by the FortiInsight platform.

User Contexts

User contexts provide additional information around the user fields that FortiInsight collects, such as Job Title, Manager, Groups, Simple Display Names and Office. This information is gathered by the FortiInsight LDAP client, from your Directory Service - such as Microsoft Active Directory.

The FortiInsight LDAP Client, downloaded via the FortiInsight UI, is a self-contained application, which can be placed, and scheduled, in your environment to query the required information from your Directory Service deployment and push this valuable information up to the FortiInsight platform - providing additional contextual information around the user for the analyst to use - within Policy Settings, general Threat Hunting or for enhanced Anomaly Detection via the AI settings.

Collecting the Information

First, you will need to download and shedule the FortiInsight LDAP Client, from the UI, to run against your Directory Service.

Prerequisites

- A Windows Management server, virtual machine, with a supported OS (Windows 10 or similar)
- The Management Server must have network access to both the Directory Service, and the FortiInsight Platform API.
- A read-only, least privilege user for the LDAP client to authenticate with the Directory Service
- A FortiInsight API key (client id, and client secret).

Downloading the latest FortiInsight LDAP Client

You download FortiInsight LDAP client software from the FortiInsight UI:

1. Go to **Contexts > User**.
2. Click **Download LDAP Client**.
3. Click **Download** on **Run on Windows**.

Running the FortiInsight LDAP Client on Windows

The FortiInsight LDAP client is a self-contained command-line application, this means that it does not require installation into the OS of choice, you can choose to either run the software ad-hoc or schedule it to create a scheduled task in order to keep the User Context information up to date with your Directory Service.

After downloading the LDAP Client package, extract it to your local management server, and update its configuration file with the required information.

All keys are stored in a configuration file, for example:

```
{
  "ApplicationConfig": {
    "LdapConnectionSettings": {
      "Host": "ldap.server.com",
      "Port": 636,
      "Username": "ldap_username",
      "Password": "ldap_password",
      "EnableSSL": true,
      "TrustInvalidServerCertificate": false
    },
    "FinsApiSettings": {
      "ApiUri": "https://example.fortiinsight.cloud",
      "ClientId": "client_id",
      "ClientSecret": "client_secret"
    }
  }
}
```

Key	Description
ApplicationConfig.LdapConnectionSettings	Container for all setting related to your LDAP server.
Host	IP or DNS name for the ldap host.
Port	LDAP host destination port that accepts LDAP traffic. MS Active Directory uses port 636 for encrypted traffic, and port 389 for plain text by default. Depending on the server settings, this port can be TCP/IP or UDP.
Username	is a user with least permissions to access ldap server. This user requires read only permissions to query ldap server for users and groups information
Password	Plain text password to access LDAP server. Note this will be encrypted, on disk, after a successful connection has been established. This password is required in plain text, as it will be used to authenticate with the server.
EnableSSL	Enable this to use standard ldap encryption. The port for encrypted traffic is usually different to the port of plain text traffic

Key	Description
TrustInvalidServerCertificate	When using an encrypted connection, it is possible to trust a server's certificate, even when the current host machine does NOT trust it. This is analogous to a self-signed certificate on the web server. Please use with caution as this allows for trivial MITM attacks on the connection. It is recommended to ensure the server certificate is trusted by this host, and setting this value to false in production.
ApplicationConfig.FinsApiSettings	Container for all settings related to the FortiInsight Cloud Service
ApiUri	The base URL to the FortiInsight Cloud Service,
ClientId	Client ID recovered by creating a new API Key from the FortiInsight UI: Admin > Accounts > New API Key . The downloaded file will contain both the client id and the client secret.
ClientSecret	Client secret to provide authentication with the FortiInsight Cloud Service.

Example complete configuration file:

```
{
  "ApplicationConfig": {
    "LdapConnectionSettings": {
      "Host": "10.1.1.1",
      "Port": 636,
      "Username": "test-query-user",
      "Password": "k*x9P*A4...",
      "EnableSSL": true,
      "TrustInvalidServerCertificate": false
    },
    "FinsApiSettings": {
      "ApiUri": "https://org1.fortiinsight.cloud",
      "ClientId": "Aj2s4oLq...",
      "ClientSecret": "CXC4tpVP9cb5..."
    }
  }
}
```

Once the configuration file has been created and edited with your values, it's time to test the connection, in a command prompt run the following:

```
cd %fins_download_dir%
fins.ldap.exe
```

Check the output for any errors. If you get any errors, most likely some configuration value is not valid or network traffic cannot flow freely to the destination hosts. Once the application finishes running with exit code 0 (success) it means that all the user information and group information has been successfully uploaded to FINS and is available in the user context.

If the application has finished running successfully, it's time to configure a scheduled task for hands off syncing.



Fins LDAP Client will first test the connection to the provided LDAP server and the FortiInsight Cloud Service. If the connection is successful, the application will encrypt the configuration file, in place.

Example encrypted configuration file will look like this:

```
{"CipherText": "AQAAANCMnd8B...=="}
```

After encryption has taken place by the application, the file can no longer be edited, the FortiInsight LDAP Client also provides a `appsettings.json.bac` file, to allow you to recreate the settings should you need to make any changes.

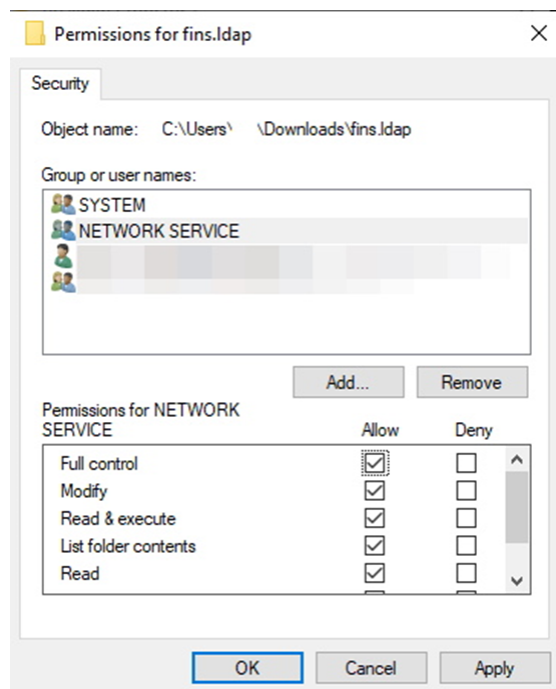
FortiInsight LDAP Client Permissions

During task scheduling, fins ldap client will attempt to grant the required Access Control Permissions for the FINS LDAP Client Folder, for the NT AUTHORITY\NETWORK SERVICE account. This is needed for Windows task scheduler as the FINS synchronization task runs under this account.

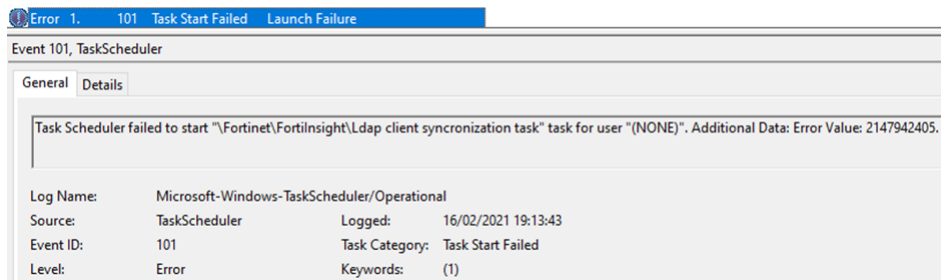
You can check these permissions manually.

When running under Windows task scheduler, ldap client is executed under Network Service account. This allows the task to run when no interactive user is logged on to the machine. Because of this *Network Service* account requires Full Control of the folder.

Please note that these permissions are absent by default if you download the client into the default user download folder.



The error message in Windows task scheduler will contain error code 2147942405 (0x80070005), which corresponds to unauthorised access error.



FortiInsight LDAP Client Options

The FortiInsight LDAP Client has a simple command-line interface to allow you to run, create a scheduled task, or remove the scheduled task.

Run executable, pull info from Ldap server and send data to FINS API. Check appsettings.json for connection settings.

```
Fins.Ldap.exe
Fins.Ldap.exe run
```

Create a scheduled task in a Windows task scheduler. Possible `day` values: mon, tue, wed, thu, fri, sat, sun, all.

Possible `time` is a 24 hour local time in HH:mm format, for example 14:30. You can combine several values using a `SPACE` and wrap the values in `quote marks`.

This command schedules a Windows scheduled task to run on Mondays, Wednesdays and Saturdays, twice on each day at 3AM and 2:30PM

```
Fins.Ldap.exe scheduled --day "mon wed sat" --time "03:00 14:30"
```

This command schedules a Windows scheduled task to run daily at 1AM

```
Fins.Ldap.exe schedule -d all -t 01:00
```

Unschedule, removes FortiInsight Ldap sync scheduled task

```
Fins.Ldap.exe unschedule
```

Other commands

```
Fins.Ldap.exe help
Fins.Ldap.exe version
```


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:

 **Endpoints**

Get Latest Endpoint Installers Unlicense 4 endpoints 4/100 licenses used

Search: Select a term, add negation ('not') or a parenthesis

From: Oldest To: Newest Export to CSV

Show: ☒ Endpoint ☒ Endpoint Name ☒ Latest IP Address ☒ Registered (UTC) ☒ Latest Version ☒ Last Activity ☒ Licensed Search returns 4 results

Previous 1 Next 100

Endpoint	Endpoint Name	Latest IP Address	Registered (UTC)	Latest Version	Last Activity	Licensed
Jwo	dione	10.10.0.4	18/03/2019 17:23:20	3.5.0	profile update 4 hours ago	yes
z99	enceladus	10.10.0.2	18/03/2019 15:00:30	3.5.0	file read 5 hours ago	yes
uqP	mimas	10.10.0.1	18/03/2019 14:15:00	3.5.0	profile update 5 hours ago	yes
BZz	tethys	10.10.0.3	18/03/2019 13:55:06	3.5.0	profile update 5 hours ago	yes

Unlicensing endpoints

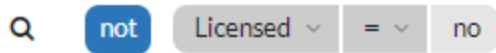
To unlicense old endpoints, click the **Unlicense endpoints** option. You can select this option to replace old endpoints with new ones.

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.

Accounts

User	Email	Locked Out	Approved	Role
Admin	no-reply@fortinet.com	No	Yes	Administrator
GAdmin	support@zonefox.com	No	Yes	SuperAdmin
demo	demo@fortinet.com	No	Yes	Readonly

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.

License

Current License










You are currently using 4 of your 100 endpoint licenses.

Endpoint Limit	License Valid From	License Expires
100	Dec 31, 2017, 7:00:00 PM	Jul 30, 2019, 7:00:00 PM

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
	<div><div> FortiInsight</div><div><div> Dashboard</div><div><div> Alerts</div><div>11</div><div>></div></div><div><div> AI</div><div>></div></div><div><div> Policy</div><div>></div></div><div><div> Reports</div><div>></div></div><div><div> Threat Hunting</div><div>></div></div><div><div> Investigations</div><div>></div></div><div><div> Admin</div><div>></div></div></div></div>

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

demo Preferences

Email

demo@fortinet.com

Notifications

☒ User Preferences

☒ AI Settings

☒ Collections

☒ Dashboard Updates

☒ Licenses

☒ Policies

☒ System

☒ Account

☒ Hover Help Bubbles

Badges Refresh Time

30

Save and Close



FORTINET®



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.