

FortiInsight Cloud - Release Notes

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



August 17, 2021

FortiInsight Cloud 21.2 Release Notes

52-600-543475-20210203

TABLE OF CONTENTS

- Change log** **4**
- Introduction** **5**
 - What's new in FortiInsight Cloud version 21.2 5
 - Related resources 9
- Product integration and support** **11**
 - FortiInsight version 21.2 support11

Change log

Date	Change description
2021-08-17	FortiInsight Cloud version 21.2 document release. First release in v21.1. Previous 6.4.0.

Introduction

This document provides the following information for FortiInsight version 21.2:

- [What's new in FortiInsight Cloud version 21.2](#)
- [Upgrade information](#)
- [Product integration and support](#)
- [Resolved issues](#)
- [Known issues](#)

What's new in FortiInsight Cloud version 21.2

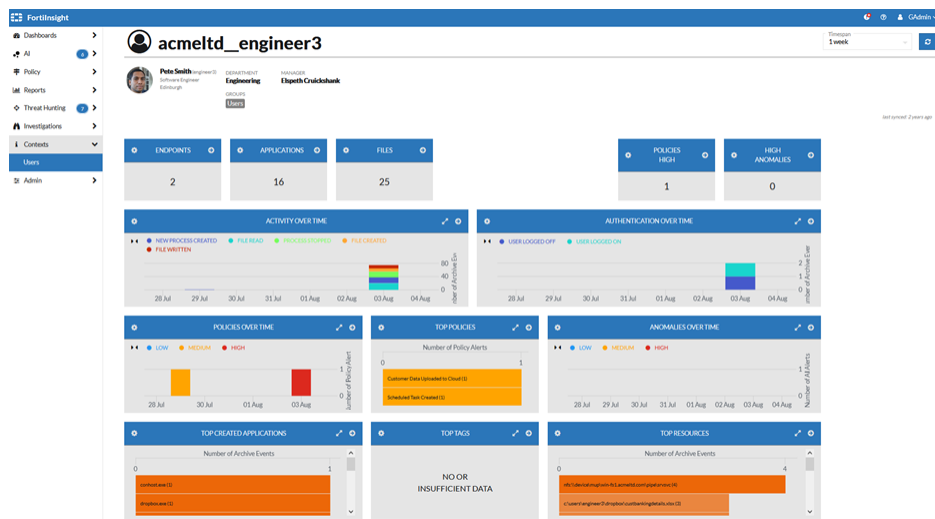
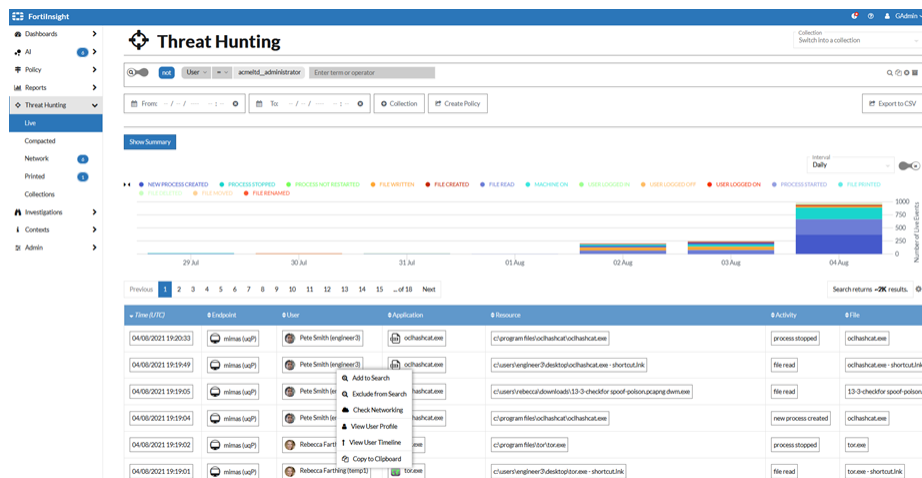
The following table lists new features and enhancements in FortiInsight Cloud version 21.2.

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

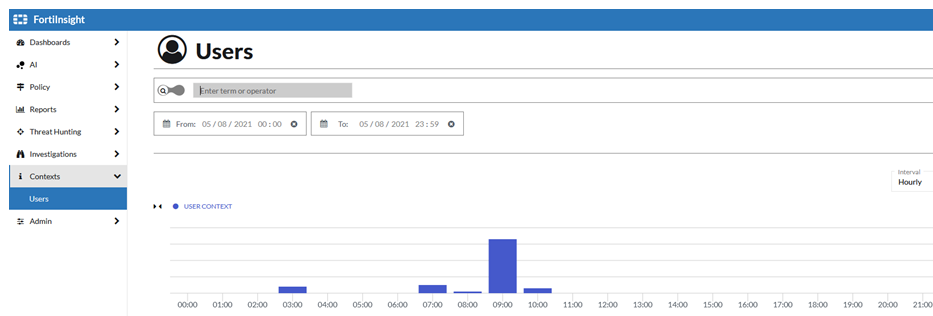
User Context Dashboard

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.

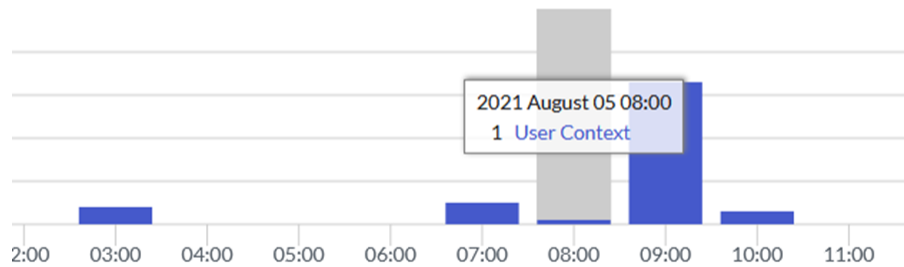


User Context Timeline

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.

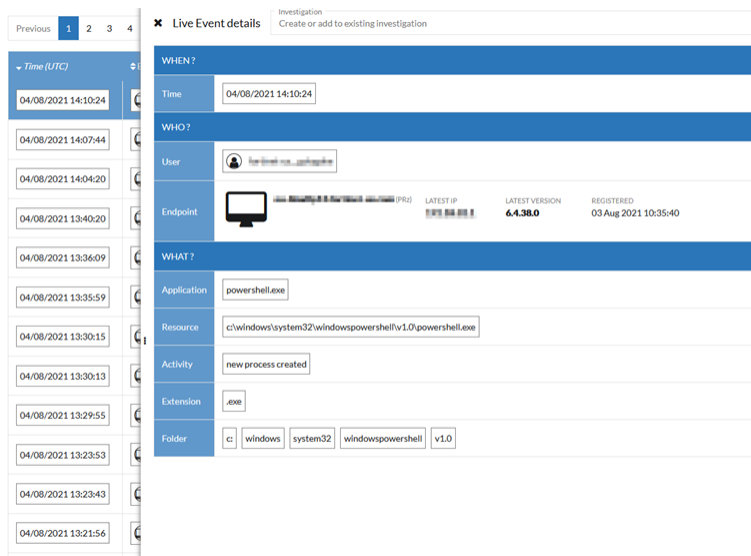
Such as:

- **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

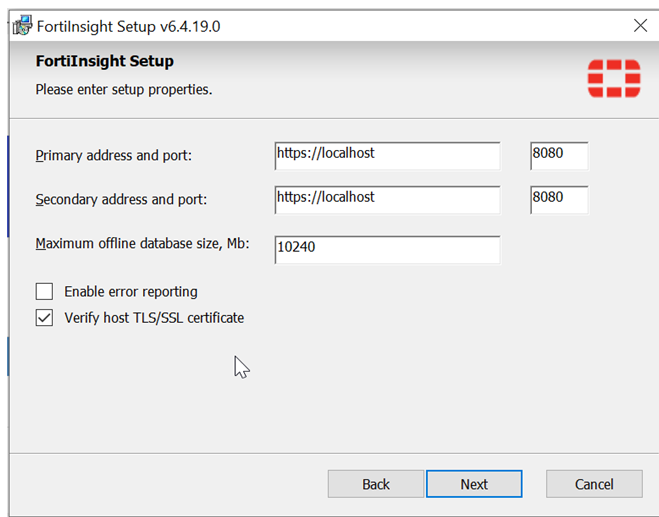
Files Deleted Event for Shift Delete

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.



Related resources

The following resources provide more information about FortiInsight:

- [FortiInsight Documentation](#)
- [Fortinet Knowledge Base](#)
- [Fortinet Support website](#)
- [Fortinet NSE Institute](#)

Product integration and support

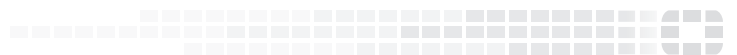
FortiInsight version 21.2 support

The following table lists product integration and support information for FortiInsight version 21.2.

Component	Requirement
Endpoint agent support	FortiInsight provides endpoint agents for the following platforms: <ul style="list-style-type: none">• Windows 7 and later (32-bit and 64-bit)• Windows Server 2008 and later (32-bit and 64-bit)• Mac OS Version 10.9 (Mavericks) and later (32-bit and 64-bit)
Endpoint computers	<ul style="list-style-type: none">• 1.0 GHz CPU - x86 or x64 (agent uses 0.1% to 5%)• 1 GB RAM (agent uses 10 to 30 MB)• 20 MB free disk space (more space is needed to store compressed and encrypted offline events)
Browser	<ul style="list-style-type: none">• Google Chrome (recommended)• Chromium• Mozilla Firefox• Microsoft Edge• Apple Safari <p>Other web browsers may work correctly, but FortiInsight does not support them.</p>
Input devices	<p>The FortiInsight UI is not optimized to use with touch devices. We recommend using a keyboard and mouse as the input devices for interacting with the UI.</p>



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.