FortiInsight Cloud - Release Notes

Version 21.1

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

February 3, 2021
FortiInsight Cloud 21.1 Release Notes
52-600-543475-20210203

TABLE OF CONTENTS

Change log

Date	Change description
2021-02-03	FortiInsight Cloud version 21.1 document release. First release in v21.1. Previous 6.4.0.

Introduction

This document provides the following information for FortiInsight version 21.1:

What's new in FortiInsight Cloud version 21.1

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.

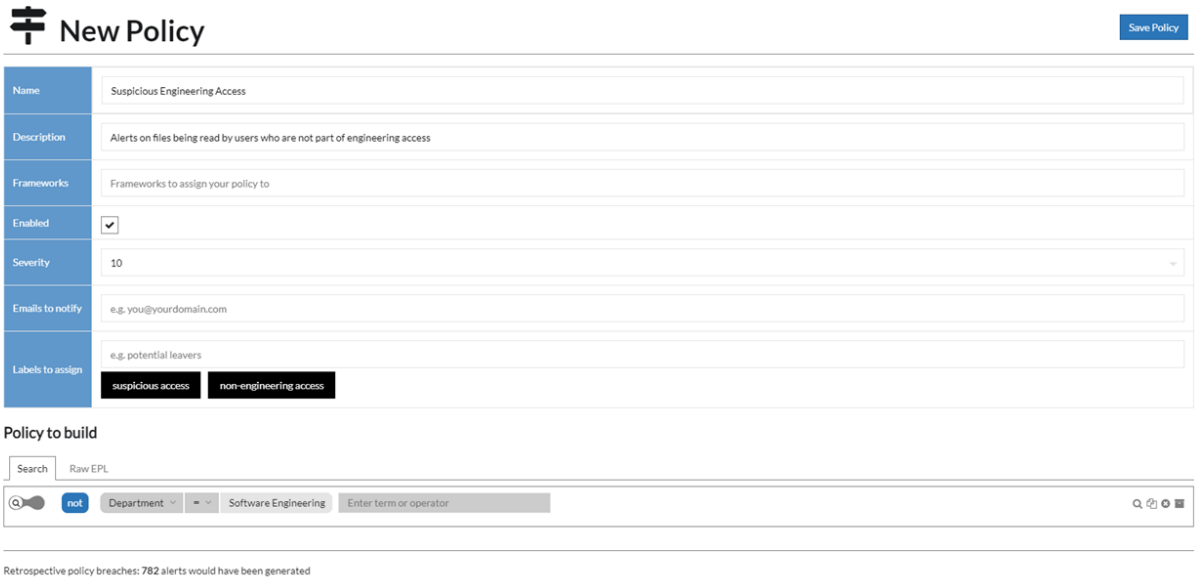
In Case You Missed It (ICYMI) FortiInsight 6.4

https://docs.fortinet.com/document/fortiinsight-cloud/6.4.0/release-notes/970300/introduction

Feature	Description
MAC OS Endpoint Support	FortiInsight now supports event collection of MAC OS.
Improved Default State	Enhanced default out of the box policies and policy collections.
API V2 Release	FortiInsight API V2 has been fully released, an API Explorer is also added to support this new version.
Support More Deployment Regions	FortiInsight now supports being deployed into six new regions across the globe.
Search Bar Tutorials	Added basic, intermediate, and advanced search bar tutorials.
File Printed View	New view for File Printed events. These are stored for default of one year.
Threat Hunting Quick View	Threat Hunting explorer now supports a row quick view allowing you to easily see the row details.
Default sort applied to all tables	Where Time is a supported field in FortiInsight tables, it is now the default sorting method when searching on data. Includes Explore, Policy > Alerts, AI > Alerts and many others.
Automatic concatenation of search pills	Searchbar now supports the automatic concatenation of search pills in design mode. This will default to ‘and’.

User Contexts and LDAP Connector

FortiInsight User Contexts provide the ability to understand the specific user in question whether you are viewing alerts, anomalies, or raw events. This data is valuable to provide additional context to what has happened in your organization, helping you to clarify which user is interacting with which data more easily. Included in this major feature is the ability to create Policies around the user contexts, for example now you can simply create Policies to monitor suspicious access to particular locations based on the user’s Job Title, or Department.



As part of the User Context, FortiInsight has added a new Contexts area - here you will find all information related to the user contexts, plus any additional tracking information such as Last Active, and status of the user. Here you can also download the FortiInsight LDAP connector to schedule, and provide additional contextual information for users - see the download link in the image.

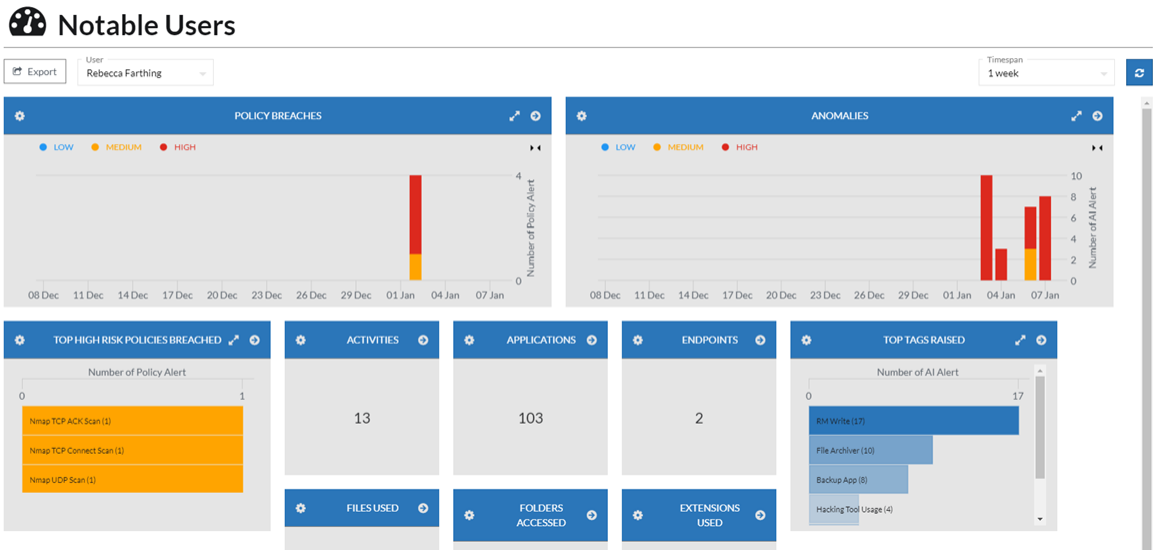
New User Context-specific fields have also been added to all types where User Contexts are supported full list includes:

Search Field	Description
AccountDisabled	Whether the Account in question is in a disabled state
UserName	Full Name of the user i.e John Smith
UserFirstName	First name of the user i.e John
UserLastName	Last name i.e Smith
Office	Office keyword provided by Directory Service
SAMAccountName	Security Account Name used
LogonName	Given name that users use to logon to machine with
Title	Job or Role title given to the user
Manager	Name of the manager for the given user
Department	Department the given user is in

Most Notable Users

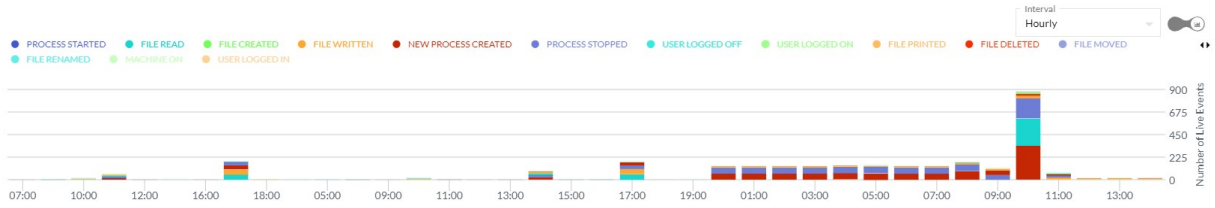
FortiInsight (January) has now introduced a new, interactive, default dashboard to provide the most notable Users that FortiInsight has found across your organization. Notable factors here include any High Policy or AI

Alerts that have been raised against the user in question. From this dashboard, you can at a quick glance view the trend of Policy, or AI, Alerts, which Tags have been raised, which High-Risk Policies have been breached, and a number selection of raw event indications. Using the Notable Dashboard as a starting point you can begin to delve deeper into the underlying data investigating any High Policy Breaches, odd applications, or strange access times for a given user.



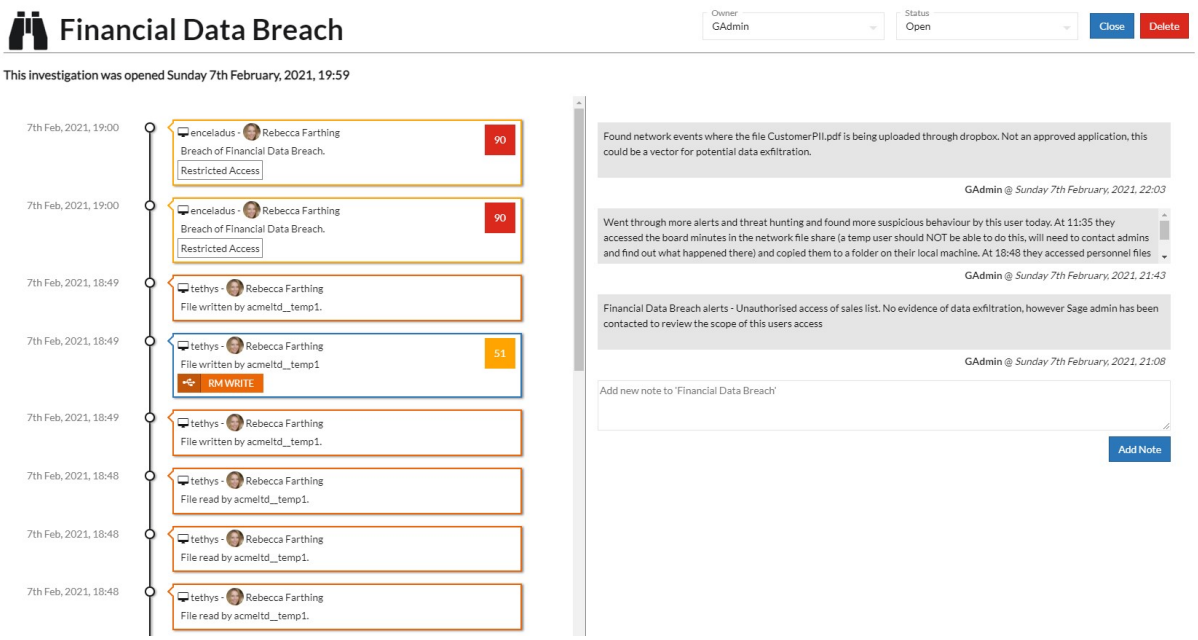
Trend Charts

FortiInsight (January) introduces new Trending charts - a high-level overview of all your data in an interactive time series chart. Trending charts are supported across all threat hunting views (Live, Compacted, Printed, Network) providing you with an easy to understand chart over time. Trending charts provide you with the ability to view counts of the events over a dynamic time period and interval selection. Whether you are investigating a suspicious user, application or endpoint trending charts provide a simple way to understand any anomalous based on volume or suspicious time accesses.



Investigation Timeline

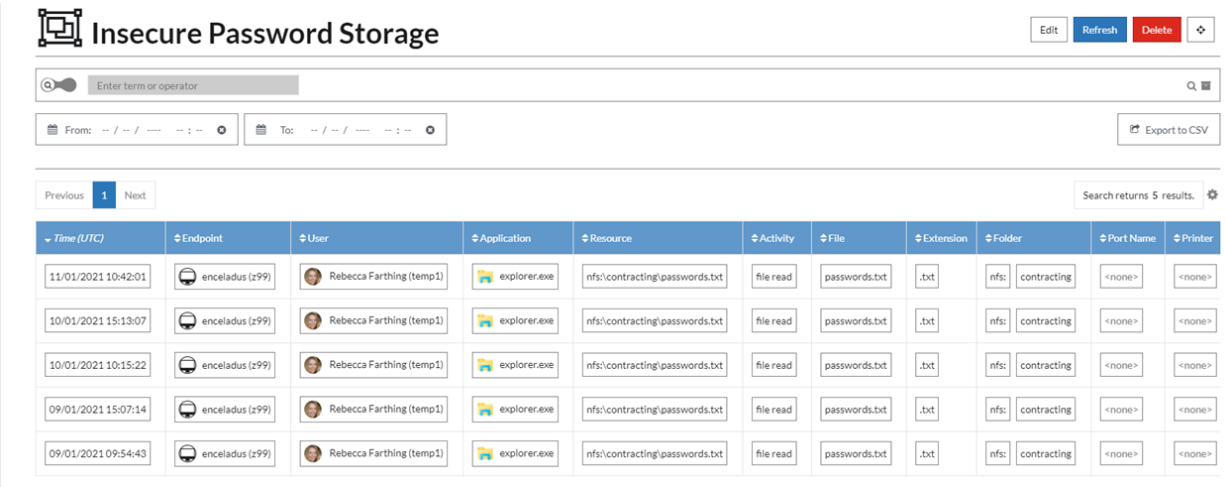
FortiInsight (January) allows you to now view an entire Investigation in one timeline containing all activity that has been collected.



Collection Source

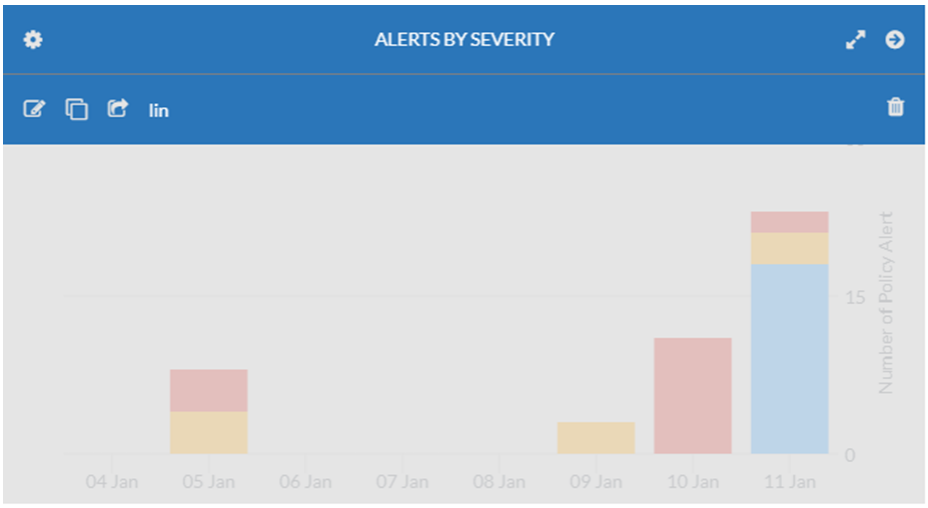
FortiInsight (January) now supports switching into any collections with ease on any supported view (Policy, AI, Live). Simply click into the switch dropdown to view data collected for your collection:

Collections have also had a redesign to allow you get investigate and search much easier with control helpers added to the top, and a ‘Go To’ button added for ease.

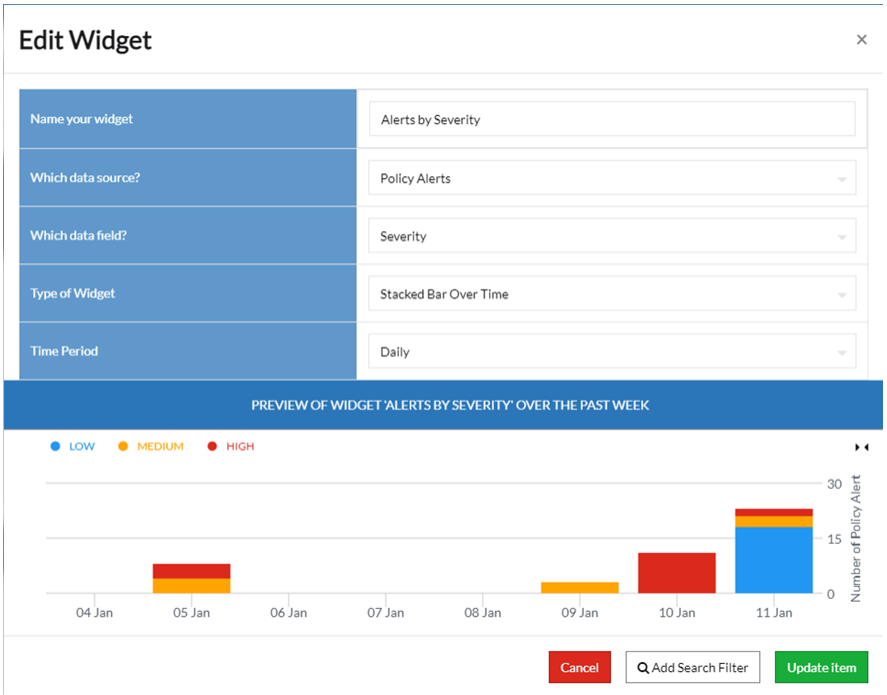


Dashboard Management Enhancements

FortiInsight (January) now support easier control, standardised controls and more options for your dashboards. A new settings bar has been added to allow you Edit, Clone, Export or Remove a particular widget. Enlarge and Shrink control have also been added to allow you to dive deeper into the information on your dashboard - without taking you away from it.



Editing time series widgets now provide you with an interval option, to carve up the data as you see fit, and an “always-on” preview of what your widget will look like - should there be data available.



Editing Top N widgets now gives you control over how many top results to return, max 100, for any given Top N widget.

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 21.1 support

The following table lists product integration and support information for FortiInsight version 21.1.

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