



FortiInsight - Release Notes

Version 7.0.0

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



August 17, 2021

FortiInsight 7.0.0 Release Notes

52-600-543475-20210203

TABLE OF CONTENTS

- Change log** 4
- Introduction** 5
 - What's new in FortiInsight version 7.0.0 5
- Upgrade information** 11
- Product integration and support** 13
 - FortiInsight version 7.0.0 support 13

Change log

Date	Change description
2021-08-17	FortiInsight 7.0.0 release notes first release.

Introduction

This document provides the following information for FortiInsight version 7.0.0:

- [What's new in FortiInsight version 7.0.0](#)
- [Upgrade information](#)
- [Product integration and support](#)
- [Resolved issues](#)
- [Known issues](#)

What's new in FortiInsight version 7.0.0

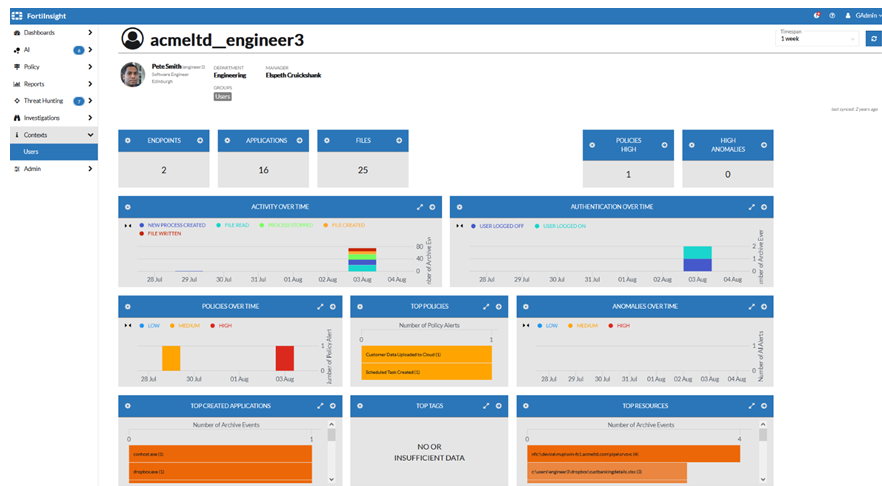
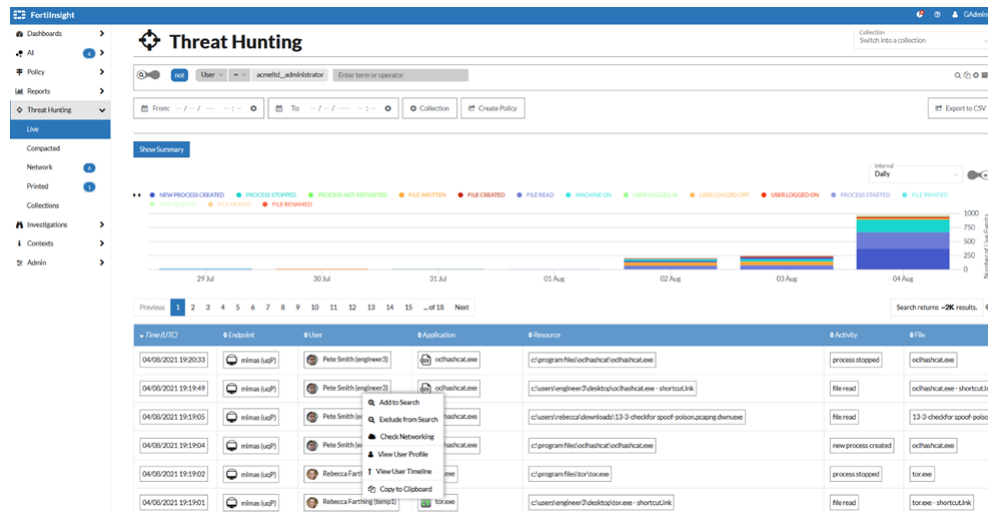
The following table lists new features and enhancements in FortiInsight version 7.0.0.

Feature	Description
Enhancements as Cloud 21.2	<p>Enhanced User Profile / Timeline</p> <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 <p>Updated Policies</p> <p>The following policies have been updated to reduce noise:</p> <ul style="list-style-type: none">• File Downloaded Through a LOLBAS Binary• PSEXEC Executed On All Machines In Domain
Xen build image	FortiInsight VM can now be deployed to AWS using the Xen vhd image.

Enhanced User Profile / Timeline

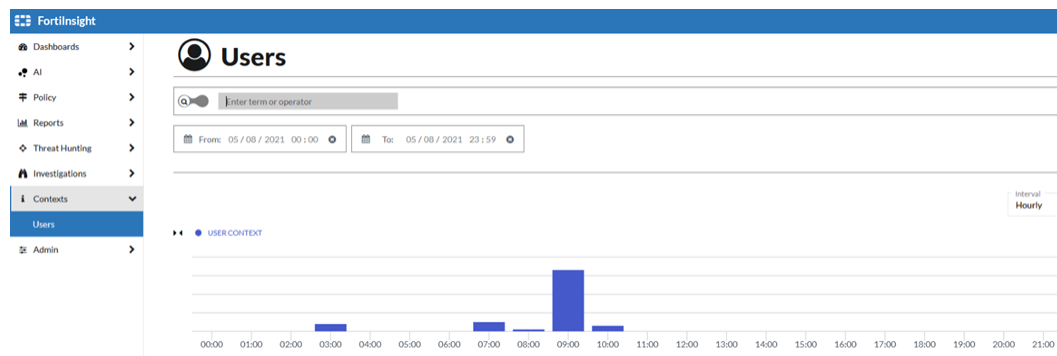
User Context Dashboard

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.

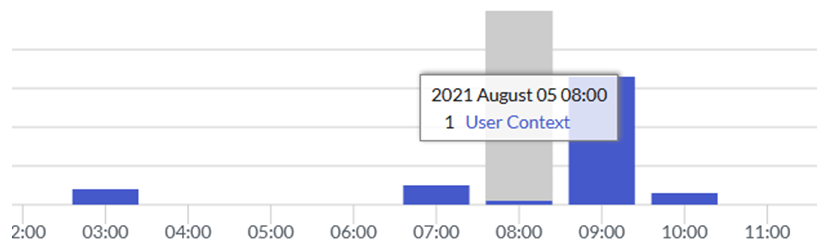


User Context Timeline

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.

Interval: Hourly

USER CONTEXT

08:00

Previous 1 Next

Search returns 1 results.

Disabled	User	User Name	Title	Office	Manager	Department	Last Activity
no	Fortinet Inc. Administration	Fortinet Inc. Administration	<None>	<None>	<None>	<None>	process not restarted 3 hours ago

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.

Previous 1 2 3 4

Time (UTC)

04/08/2021 14:10:24

04/08/2021 14:07:44

04/08/2021 14:04:20

04/08/2021 13:40:20

04/08/2021 13:36:09

04/08/2021 13:35:59

04/08/2021 13:30:15

04/08/2021 13:30:13

04/08/2021 13:29:55

04/08/2021 13:23:53

04/08/2021 13:23:43

04/08/2021 13:21:56

Live Event details

Investigation Create or add to existing Investigation

WHEN?

Time 04/08/2021 14:10:24

WHO?

User Fortinet Inc. Administration

Endpoint Fortinet Inc. Administration (PRO) LATEST IP 192.168.1.100 LATEST VERSION 4.4.38.0 REGISTERED 03 Aug 2021 10:35:40

WHAT?

Application powershell.exe

Resource c:\windows\system32\windowspowershell\v1.0\powershell.exe

Activity new process created

Extension .exe

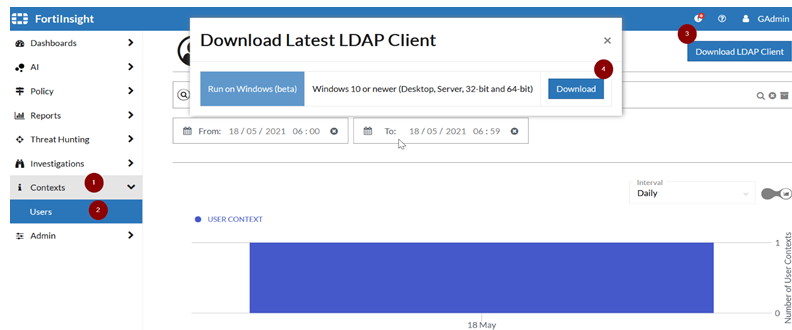
Folder c:\windows\system32\windowspowershell\v1.0

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**.



Xen Build Image

FortiInsight images are currently not available in AWS market place. It is recommended to use your own account to download and launch FortiInsight Virtual Machine (VM). Download the FortiInsight Xen Super image (VHD) file from the Fortinet Support website <https://support.fortinet.com>. For install instructions see [FortiInsight AWS Installation](#).

FortiInsight Agents

Agent Feature	Description
MAC Connector	<ul style="list-style-type: none"> • Add supports 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

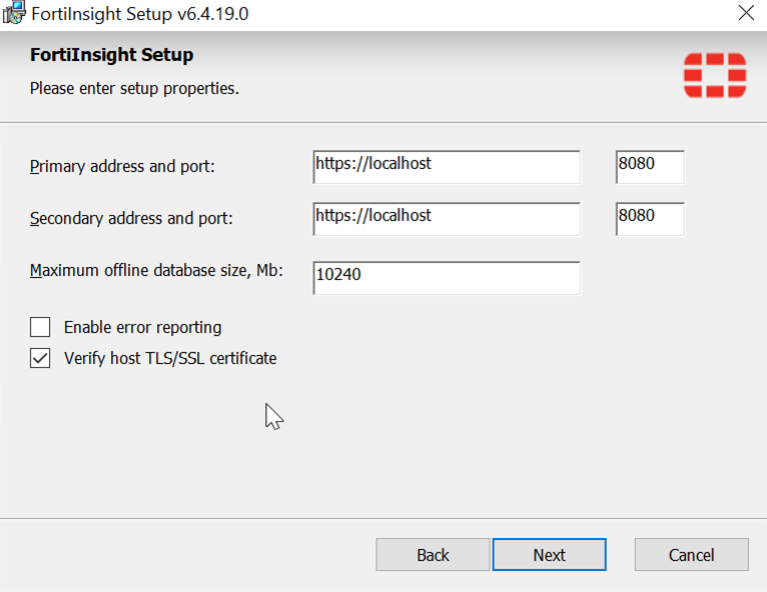
Files Deleted Event for Shift Delete

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.



The image shows a Windows-style setup window titled "FortiInsight Setup v6.4.19.0". The window has a title bar with a close button (X) in the top right corner. Below the title bar, the text "FortiInsight Setup" is displayed in bold, followed by "Please enter setup properties." in a smaller font. To the right of this text is a red Fortinet logo. The main area of the window contains several input fields and checkboxes. The "Primary address and port:" field has a text box containing "https://localhost" and a port box containing "8080". The "Secondary address and port:" field also has a text box containing "https://localhost" and a port box containing "8080". The "Maximum offline database size, Mb:" field has a text box containing "10240". Below these fields are two checkboxes: "Enable error reporting" (unchecked) and "Verify host TLS/SSL certificate" (checked). At the bottom of the window, there are three buttons: "Back", "Next" (which is highlighted with a blue border), and "Cancel".

FortiInsight Setup v6.4.19.0

FortiInsight Setup
Please enter setup properties.

Primary address and port:

Secondary address and port:

Maximum offline database size, Mb:

☐ Enable error reporting
☒ Verify host TLS/SSL certificate

Back Next Cancel

Upgrade information

Upgrading FortiInsight Firmware

1. Download the latest firmware (6.4) to your local computer from the Fortinet Support website. Ensure that you download the correct firmware image for your hypervisor environment.
 - a. VMWare : FIN_VM-v7.0.0.xxx-FORTINET.out
 - b. HyperV : FIN_VM_HV-v7.0.0.xxx-FORTINET.out
 - c. KVM : FIN_VM_KVM-v7.0.0.xxx-FORTINET.out
 - d. AZURE : FIN_VM_AZURE-v7.0.0.xxx-FORTINET.out
 - e. XEN: FIN_VM_XEN-v7.0.0.xxx-FORTINET.out
2. The FortiInsight firmware can be upgraded from the CLI via FTP/TFTP.

To upgrade FortiInsight firmware using the CLI:

1. Copy the latest firmware image file(.out file) to your FTP/TFTP server.
2. Log into the CLI.
3. Enter the following command to copy the firmware image from the FTP server to FortiInsight:

For ftp servers:

```
execute restore image ftp <filename> <ftp_server_ip> <user_name> <password>
```

Where <filename> is the name of the firmware image file and <ftp_server_ip> is the IP address of the FTP/TFTP server and <user_name> <password> are the logon credentials for the FTP/TFTP server.

If you have an anonymous FTP server, leave the username and password blank, i.e.

```
execute restore image ftp <filename> <ftp_server_ip>
```

Example

```
execute restore image FIN_VM-v7.0.0.xxx-FORTINET.out 10.1.1.6 userid passwd
```

```
> execute restore image ftp FIN_VM_KVM-v6.4.0.0153-FORTINET.out 192.168.1.215
This operation will replace the current firmware version of FortiInsight.
Do you want to continue? (y/n)y
```

Anonymous FTP was used in the above example, so username and password were not required.

For tftp servers:

```
execute restore image tftp <filename> <tftp_server_ip>
```

Where <filename> is the name of the firmware image file and <tftp_server_ip> is the IP address of the TFTP server

Example

```
execute restore image tftp FIN_VM-v7.0.0.0005-FORTINET.out 10.1.1.6
```

4. Type y.

FortiInsight uploads the firmware image file, upgrades to the new firmware version, and restarts.



The initial image downloaded from the FTP server can take 5 - 10 minutes, while no progress indicator is displayed.

5. To check the firmware update has been successful, go to **FortiInsight Banner > User ID Dropdown > FortiInsight Version**.

Product integration and support

FortiInsight version 7.0.0 support

The following table lists product integration and support information for FortiInsight version 7.0.0.

Component	Requirement
Endpoint agent support	FortiInsight provides endpoint agents for the following platforms: <ul style="list-style-type: none">• Windows - 7, 8, 8.1, 10 (32-bit and 64-bit)• Windows Server - 2008R2, 2012, 2012R2, 2016, 2019• MAC OSX - 10.9, 10.10, 10.11, 10.12, 10.13, 10.14
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.