

# Release Notes

**FortiNDR Cloud 24.3.0**



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<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/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



March 27, 2024

FortiNDR Cloud 24.3.0 Release Notes

78-241-882729-20240327

# TABLE OF CONTENTS

<b>FortiNDR Cloud release notes</b>	<b>4</b>
<b>Version history</b>	<b>5</b>
27 March 2024 version 2024.3.0	5
New Functionality	5
Improved Functionality	7
13 March 2024 version 2024.2.1	9
Improved Functionality	10
29 February 2024 version 2024.2.0	10
New Functionality	10
Improved Functionality	13
Status definitions	13
Discontinued Functionality	14
14 February 2024 version 2024.1.1	15
31 January 2024 Version 2024.1.0	15
Improved functionality	15
<b>New detection rules and observations</b>	<b>17</b>
2024.3.0	17
Rules	17
2024.2.0	17
Observations	17
Rules	17
<b>Resolved issues</b>	<b>19</b>
2024.3.0	19
2024.2.1	19
2024.2.0	19
2024.1.1	20
2024.1.0	20

# FortiNDR Cloud release notes

This document provides information about FortiNDR Cloud (formerly known as ThreatINSIGHT) releases.

FortiNDR Cloud is a SaaS network security monitoring platform designed to facilitate rapid detection, investigations, and threat hunting within your environment. FortiNDR Cloud is designed to be scalable and to remove the responsibilities of maintaining tooling from security analysts. For more information, see the [FortiNDR Cloud User Guide](#).

## Version history

Date	Version
27 March 2024	27 March 2024 version 2024.3.0 on page 5
13 March 2024	13 March 2024 version 2024.2.1 on page 9
29 February 2024	29 February 2024 version 2024.2.0 on page 10
14 February 2024	14 February 2024 version 2024.1.1 on page 15
31 January 2024	31 January 2024 Version 2024.1.0 on page 15

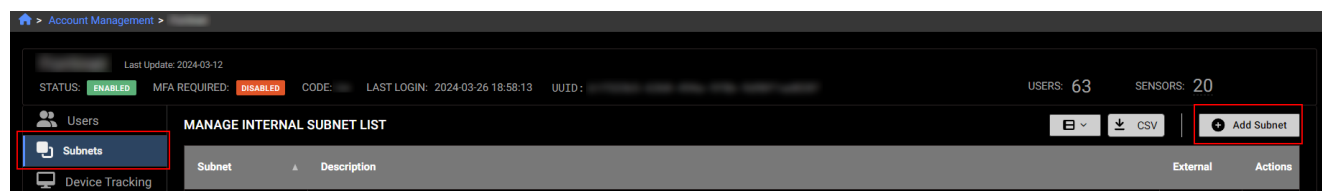
### 27 March 2024 version 2024.3.0

- New Functionality on page 5
  - Edit subnets on page 5
  - Mandatory SSO on page 6
- Improved Functionality on page 7
  - User management on page 7
  - Run a private query on page 8
  - Export sensor information on page 9
- New detection rules and observations on page 17
- Resolved issues on page 19

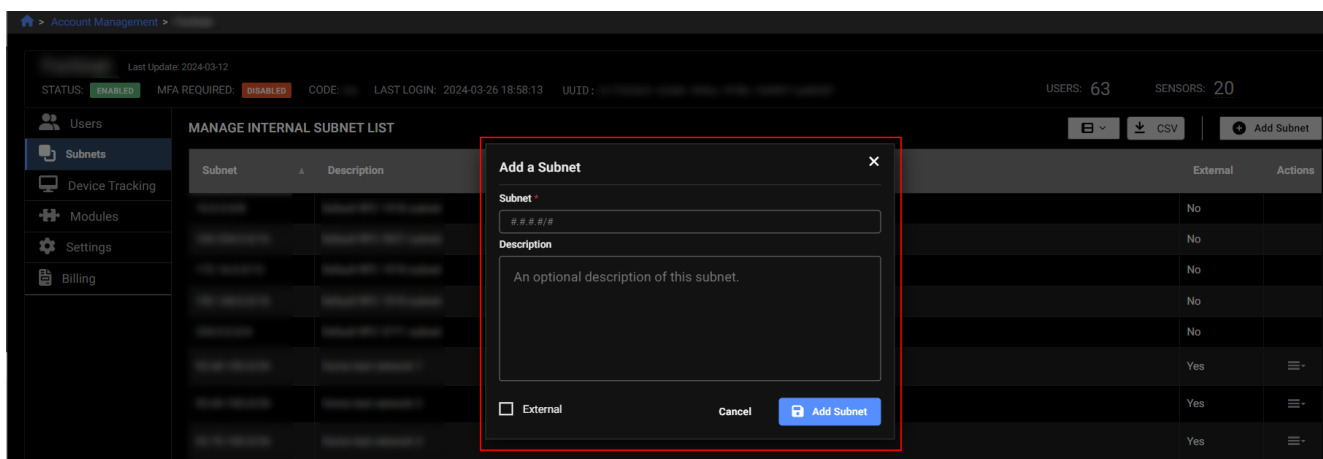
## New Functionality

### Edit subnets

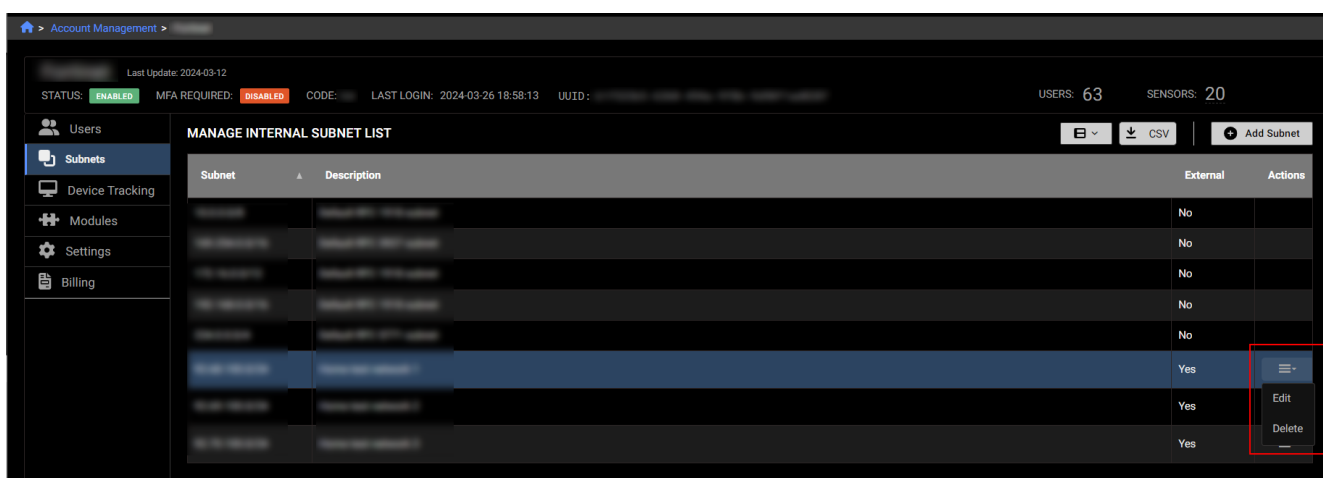
You now have the ability to add and edit subnets. Go to *Account Management > Subnets* and click *Add Subnet*.



Configure the subnet and click *Add Subnet*.

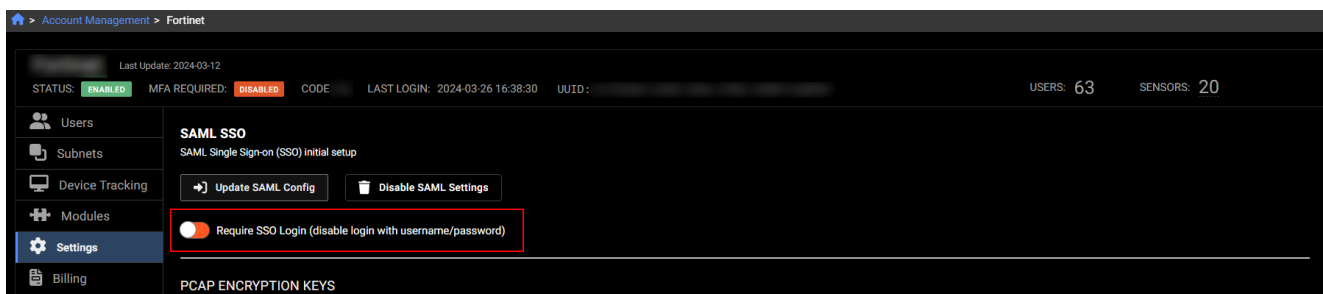


After the subnet is added, you can edit or delete the subnet from the menu in the *Actions* column.

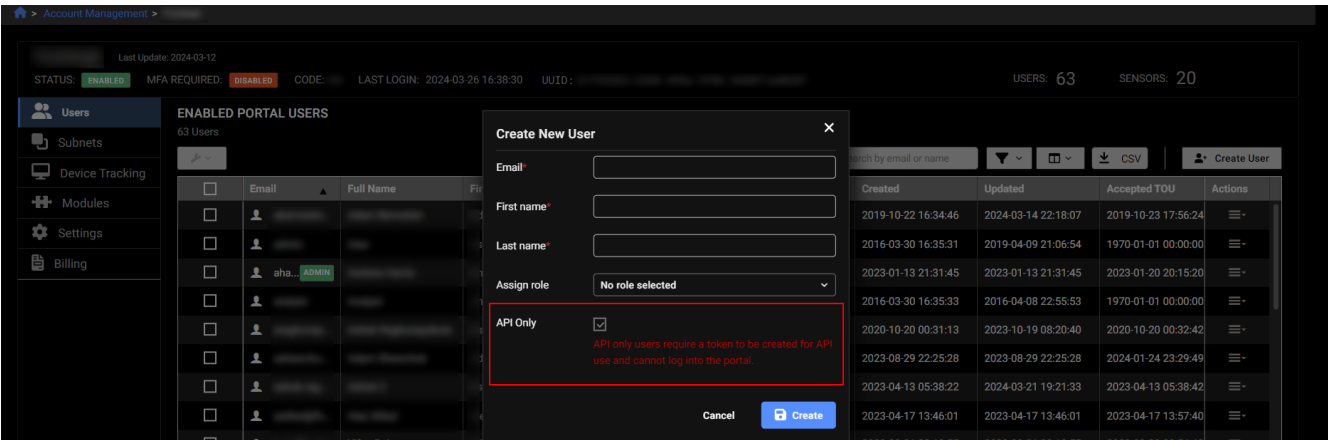


## Mandatory SSO

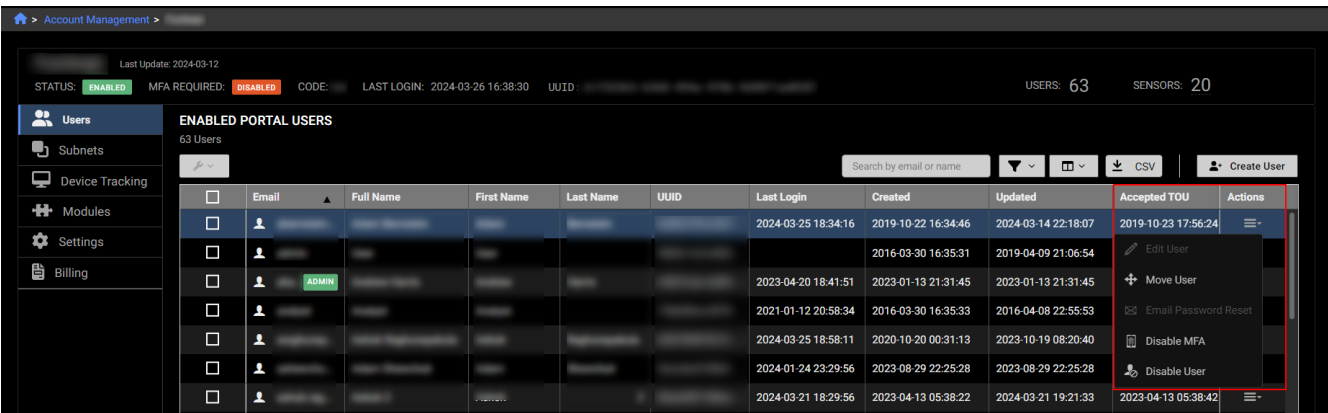
You can now require all users to log in with SSO. Go to *Account Management > Settings*. When SAML SSO is enabled the *Require SSO Login (disable login with username/password)* option is displayed. For more information, see [Settings \(Account Management\) > SAML SSO > Mandatory SSO](#) in the FortiNDR Cloud User Guide.



When mandatory SSO is enabled, *API Only* is selected by default when you create a new user.



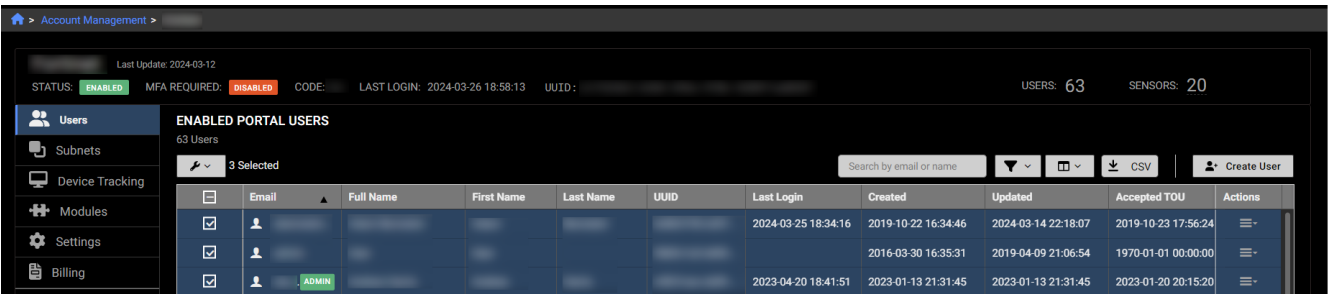
The *Edit User* and *Email Password Reset* options are also disabled in the *Users* page and the user details pane when mandatory SSO is enabled.



## Improved Functionality

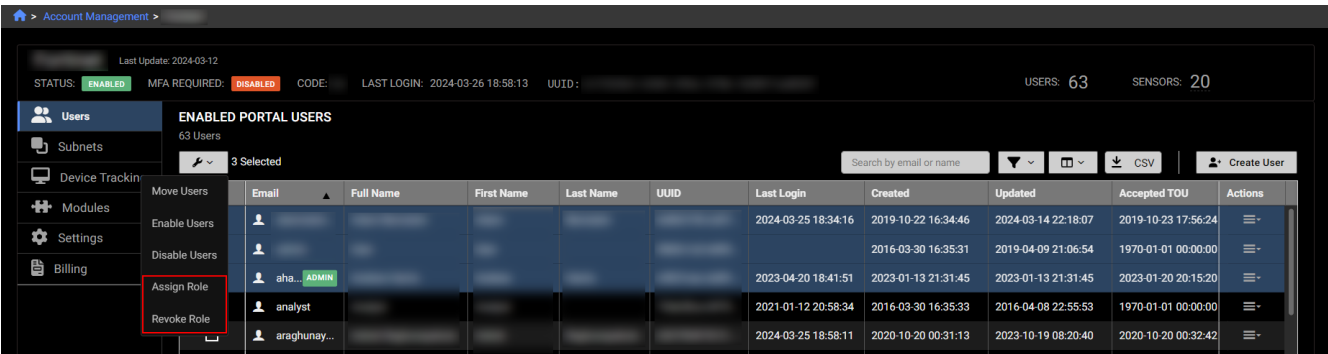
### User management

You can now assign or remove roles in bulk from the *User Management* page. Go to *Account Management > Users* and select the users you want to assign roles to.

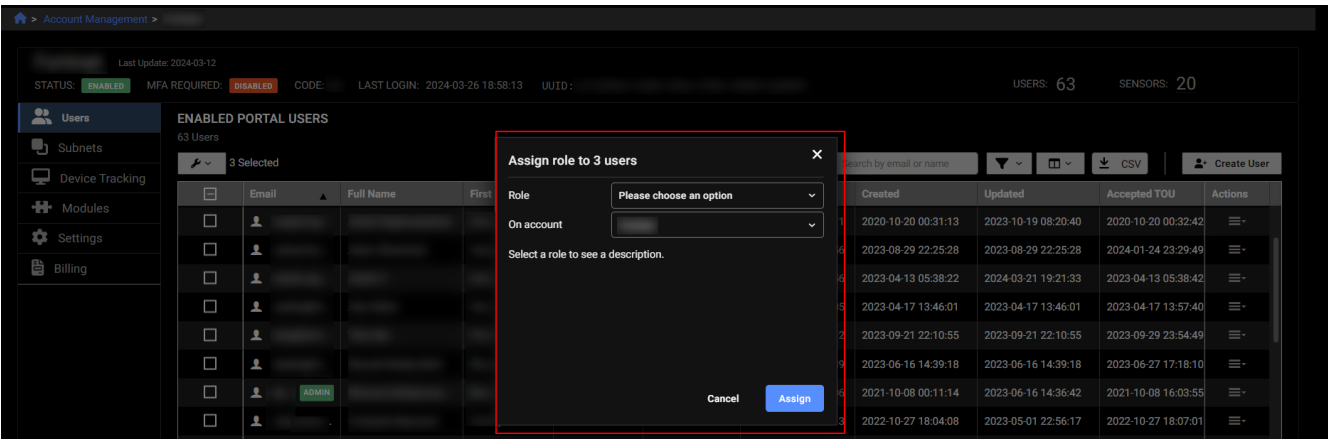


Click the tool icon and select *Assign Role* or *Revoke Role*.





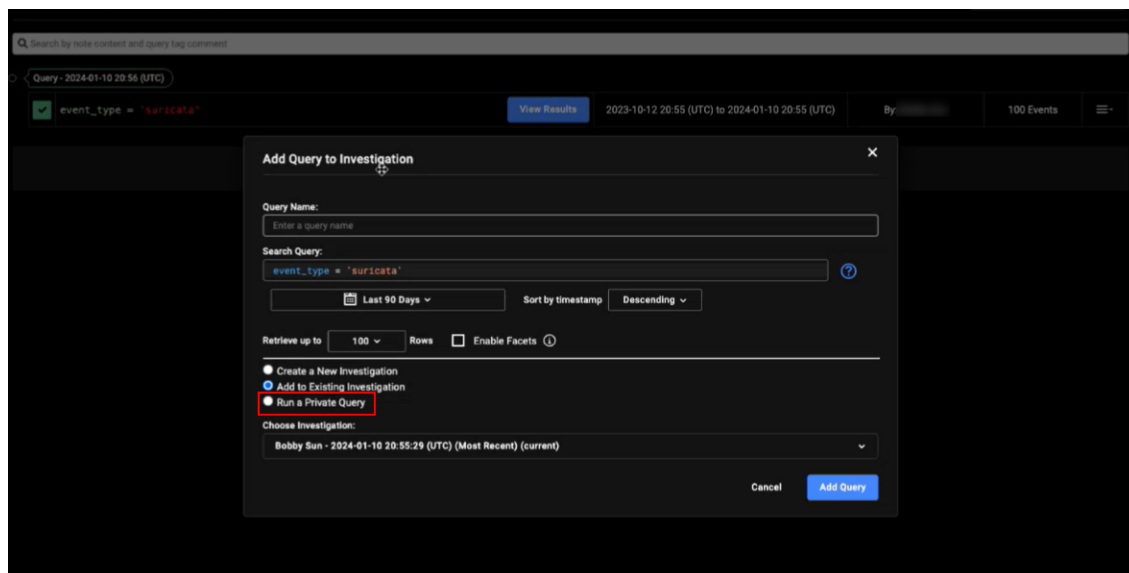
Select an option from the list and then click *Assign* or *Remove*. If the user has access to more than one account, you will see an *On Account* dropdown.



## Run a private query

You can now add a query to an adhoc search. When you clone a query you will see a new *Run a Private Query* option at the bottom of the dialog. This option is available anywhere the *Add query to Investigation* dialog appears. For information, see [Adding queries to an investigation](#).





## Export sensor information

The *Management IP* column was added to the Sensor CSV export. If there is no Management IP to display the cell is blank.

	processor_name	status.processor_core_count	status.suricata_version	status.bro_version	status.updated	status.type	interfaces	admin	prov_status	type	events	throughput	throughput_raw	management_ip
1		0			2024-02-26T19:09:10.283Z				decommissioned		0	0	0	
2	Geon(R) CPU E5-2630 v3 @ 2.40GHz	16	4.0.0-dev (rev 49)	4.1.1-0516	2024-01-22T12:45:39.430Z	ESXi			decommissioned	ESXi	0	0	0	
3		0			2024-02-28T00:25:38.280Z				decommissioned		0	0	0	
4		0			2024-02-28T00:29:37.268Z				decommissioned		0	0	0	
5		0			2024-02-28T00:37:49.477Z				decommissioned		0	0	0	
6		0			2022-11-23T22:14:50.373Z				provisioning		0	0	0	
7		0			2022-12-01T19:52:26.084Z				provisioning		0	0	0	
8	Geon(R) CPU E5-2630 v3 @ 2.40GHz	16	4.0.0-dev (rev 49)	4.1.1-0516	2022-12-02T16:56:18.365Z	ESXi			provisioning	ESXi	0	0	0	
9		0			2022-12-09T19:23:05.988Z				provisioning		0	0	0	
10		0			2022-12-12T22:06:51.496Z				provisioning		0	0	0	
11		0			2022-12-12T23:39:54.758Z				provisioning		0	0	0	
12		0			2022-12-13T00:38:45.045Z				provisioning		0	0	0	
13		0									0	0	0	

## 13 March 2024 version 2024.2.1

- Improved Functionality
  - Sensors
- Resolved Issues

## Improved Functionality

### Sensors

- A link to the [Sensors](#) topic in the *FortiNDR Cloud User Guide* was added to the *Status* column header in the *Sensors* page. This topic contains a description of each status.
- The *Sensor History* table in the *Sensor* detail page is hidden when there are no records to display.

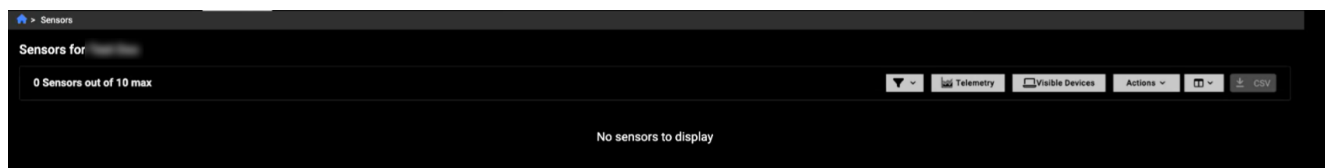
## 29 February 2024 version 2024.2.0

- New Functionality
  - [Sensors page](#)
  - [Sensor history](#)
  - [FortiGate integration](#)
- Improved Functionality
  - [Status definitions](#)
  - [Other improvements](#)
- Discontinued Functionality
  - [Enabled column](#)
- Resolved issues

## New Functionality

### Sensors page

The *Sensors* page now displays a *No sensors to display* message when there are no sensors.



A new *Decommissioned* status was added. You can use this status to filter the page. The *Decommissioned (legacy)* status indicates a sensor that was previously disabled.



In previous versions of FortiNDR Cloud a sensor with a status of *Disabled* could come back online and send data. A sensor with a status of *Decommissioned* will not send data.

Sensors

Sensors for GigaSMART Soak Test

12 Sensors out of 500 max

SENSOR ID	STATUS	VERSION	LABELS	DAY AVERAGE	BITS/S (7 DAY AVERAGE)	TYPE
gsso591	online	Unknown			1.283 Mb/s	ESXi
gsso619	online	Unknown			0 b/s	Zscaler
gsso620	online	Unknown			0 b/s	Zscaler
gsso621	online	Unknown			0 b/s	Zscaler
gsso622	online	Unknown			0 b/s	Zscaler
gsso685	online	1.12.0	ESXi		1.283 Mb/s	ESXi
gsso840	online	1.11.0			1.532 Mb/s	ESXi
gsso865	online	1.12.0			12.049 Kb/s	Large (4th Gen)
gsso920	online	Unknown			9.096 Kb/s	ESXi
gsso932	online	1.12.0		0 EPS	1.879 Kb/s	ESXi
gsso935	online	1.12.0		0 EPS	1.713 Kb/s	ESXi
gsso936	online	1.12.0		0 EPS	414.318 Kb/s	Small (4th Gen)

Additional Filters

Status: Online

All

No Filters

☐ Decommissioned

☐ Decommissioned (auto)

☐ Decommissioned (legacy)

☐ Offline

☒ Online

☐ Provisioning

☐ Shutdown

## Sensor history

A new *Sensor History* table was added to the *Sensors* details page. This table shows the actions performed, the user who performed them as well as any comments from the user. The table is sorted in descending order by timestamp. A message appears if there is no history to display.

Sensors > gsso847

Management IP: 10.10.10.10

Interfaces

ens192 0 b/s

ens224 0 b/s

Hardware

Processor(s): Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz

Number of Cores: 8

Total Memory: 15.638 GB

Total Disk Space: 67.944 GB

Software

Operation System: Debian GNU/Linux 10 (buster)

ZEEK Version: 5.0.10

Suricata Version: 6.0.12.RELEASE

Sensor Version: 1.12.0

Sensor History

34 record(s), sorted by Timestamp descending

Timestamp	Action	User Account Name	User UUID	User Name	Comment
2024-01-27T13:02:01.998983Z	pause				
2024-01-27T12:56:07.131922Z	resume				
2024-01-27T12:55:48.642531Z	pause				
2024-01-27T02:07:50.782904Z	resume				
2024-01-27T01:46:45.553064Z	pause				
2024-01-27T01:28:18.207939Z	resume				
2024-01-27T01:00:23.969226Z	pause				
2024-01-26T20:25:58.167201Z	resume				
2024-01-26T01:42:12.470863Z	pause				

The table supports filtering. However, you cannot sort the *Timestamp* column in ascending order and you cannot fix the columns.

**Hardware**

Processor(s): Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz  
Number of Cores: 8  
Total Memory: 15.638 GB  
Total Disk Space: 67.944 GB

**Software**

Operation System: Debian GNU/Linux 10 (buster)  
ZEEK Version: 5.0.10  
Suricata Version: 6.0.12 RELEASE  
Sensor Version: 1.12.0

**Sensor History**

34 record(s), sorted by Timestamp descending

Timestamp	Action	User Account Name	User UUID	User Name	Comment
2024-01-27T13:02:01.998983Z	pause				
2024-01-27T12:56:07.121922Z	resume				
2024-01-27T12:55:48.642531Z	pause				
2024-01-27T02:07:50.782904Z	resume				
2024-01-27T01:46:45.553064Z	pause				
2024-01-27T01:28:18.207939Z	resume				
2024-01-27T01:00:23.969226Z	pause				
2024-01-26T20:25:58.167201Z	resume				
2024-01-26T01:42:12.470863Z	pause				
2024-01-26T01:01:58.470092Z	resume				

## FortiGate integration

A new FortiGate via FortiManager module was added to the *Modules* page. To add the integration, click the *Configure* button and then enter your username, password and URL.

**Integration Module**

**MetaStream**

MetaStream with Signals provides access to traffic metadata directly from sensors deployed as well as other alert data seen in FortiNDR Cloud. This feature allows access to an AWS S3 bucket that contains all events, detections, and observations, and event aggregations associated with the account.

**CrowdStrike Falcon EDR**

CrowdStrike Falcon Insight EDR integration delivers Network to Endpoint visibility against advanced threats and adversary activity with endpoint context to investigate, hunt, and respond quickly.

**CrowdStrike Intelligence**

Falcon X Threat Intelligence integration delivers visibility from CrowdStrike's real-time feed of global indicators of compromise between adversaries and endpoints with enriched context to hunt and investigate.

**proofpoint TAP**

Intelligence feeds integration for Proofpoint. It provides deeper context and integrates seamlessly with FortiNDR Cloud.

**ThreatConnect**

Intelligence feeds integration for ThreatConnect. It provides deeper context and integrates seamlessly with FortiNDR Cloud.

**Recorded Future Connect**

Intelligence feeds integration for Recorded Future. It provides deeper context and integrates seamlessly with FortiNDR Cloud.

**FortiEDR**

FortiEDR integration shrinks the attack surface, prevents malware infection, detects and defuses potential threats immediately, and automates response and remediation.

**FortiGate via FortiManager**

Through an integration with the FortiGate NGFW, analysts using FortiNDR Cloud can pivot from NDR Cloud's network-based detections to block malicious external traffic using NGFW tools, decreasing incident investigation and response times.

You can view the data collected by the integration and perform FortiGate actions in the *Entity Panel* when you click on an IP in the portal.

Investigation Results | AR FortiManager Integration |

event\_type = 'flow' and uid = [redacted]

Actions 2024-02-04 00:00 (UTC) - 2024-02-06 23:59 (UTC)

Showing all 1 event, ordered by timestamp descending

timestamp	dst	tag	src	type	intel	source
2024-02-05 13:46:34 Z	[redacted]		[redacted]	FLOW		Zeek

Search by query tag comment

Summary

Connections from 0 internal devices yesterday

First seen: N/A  
Last seen: N/A  
Annotations:

Add an Annotation Manage Annotations

VirusTotal

No VirusTotal Results Found

FortiManager  
Installed - 1 device found

WHOIS

Updated: 1995-06-01 00:00:00 UTC

Filter Results by Date

2024-02-04 - 2024-02-06

PDNS

No PDNS Results Found

Detections

No Detections Found

DHCP

No DHCP Records Found

Accounts

No Accounts Found

Software

No Software Records Found

Improved Functionality

Status definitions

You can now click the help icon to view a status definition. The link redirects you to the [Sensors](#) topic in the *User Guide*.

Sensors for chf1

chf1 Provisioning

CREATED 2023-07-17 18:10:23 LOCATION [redacted] EPS (7 DAY AVERAGE) 0 eps BITS/S (7 DAY AVERAGE) 0 b/s TYPE

Status

Telemetry

Settings

Connection Status

Status: provisioning

Serial Number: Unknown

Management IP: Unknown

Hardware

Processor(s): 0

Number of Cores: 0

Total Memory: 0 Bytes

Total Disk Space: 0 Bytes

Software

Operation System: Unknown

BRD Version: Unknown

Suricata Version: Unknown

Sensor Version: Unknown

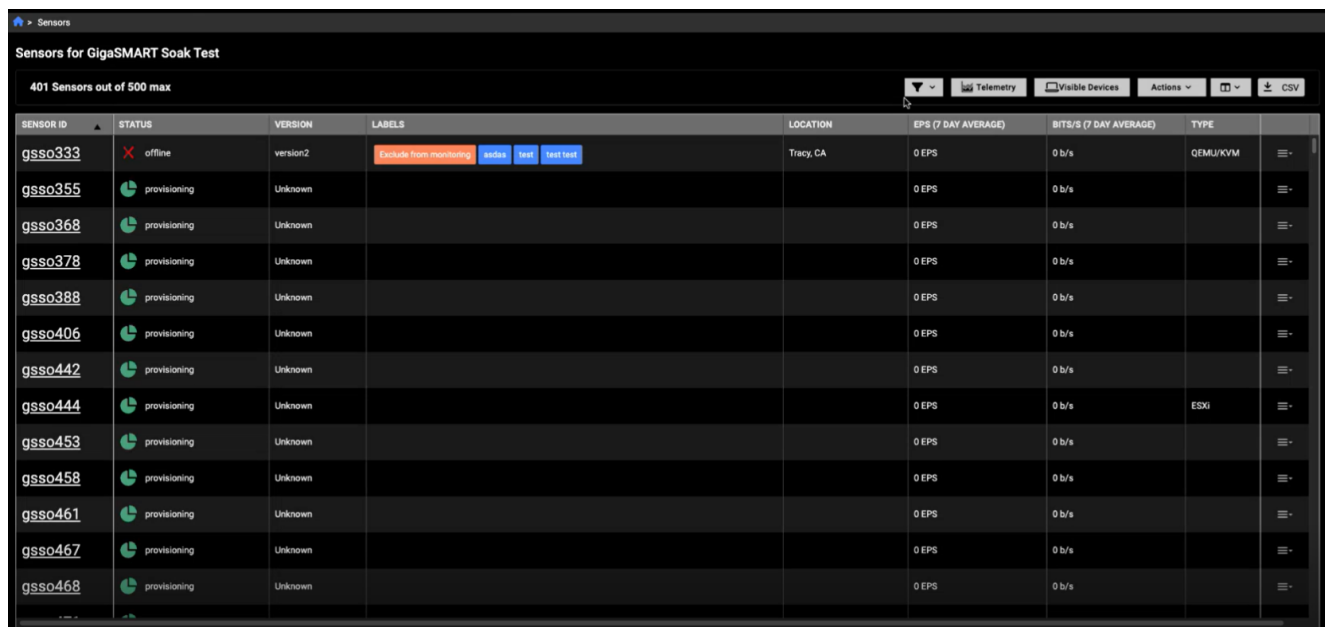
Other improvements

- The *Entity Panel* remains open when you perform an action such as creating a filter.
- The Status definitions have been added to the User Guide. See the [Sensors](#) topic in the *User Guide*.

## Discontinued Functionality

### Enabled column

The *Enabled* column has been removed from the *Sensors* page.

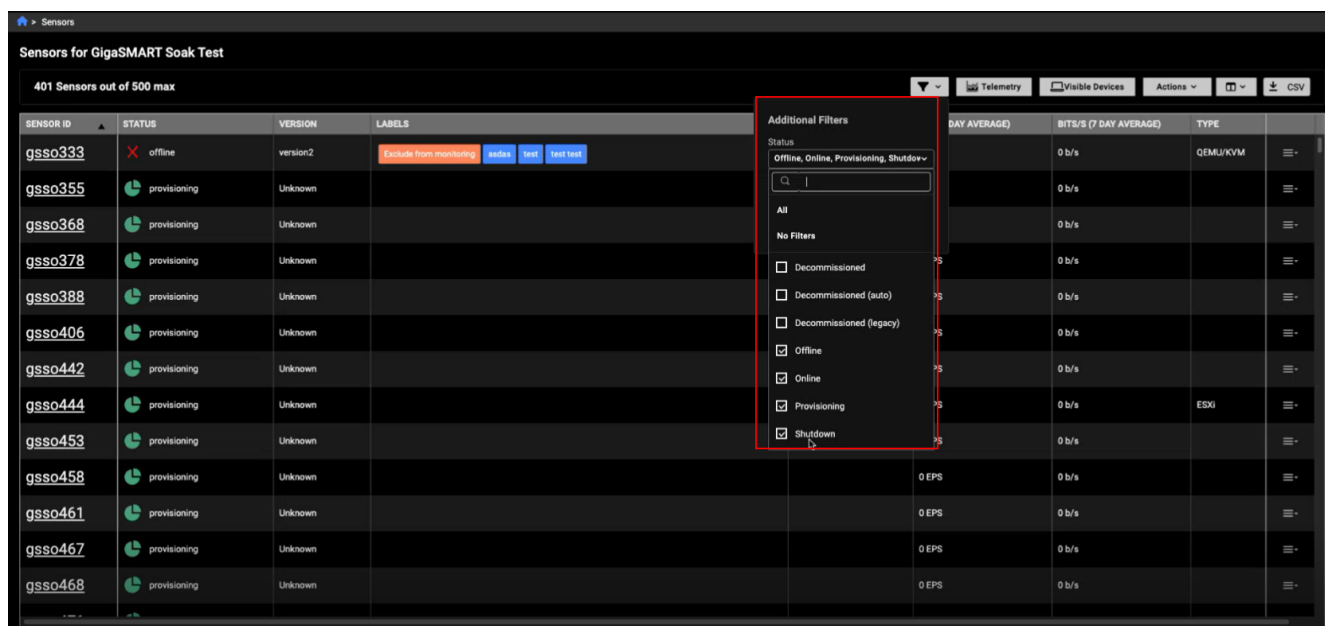


Sensors for GigaSMART Soak Test

401 Sensors out of 500 max

SENSOR ID	STATUS	VERSION	LABELS	LOCATION	EPS (7 DAY AVERAGE)	BITS/S (7 DAY AVERAGE)	TYPE
gssso333	offline	version2	Exclude from monitoring status test test test	Tracy, CA	0 EPS	0 b/s	QEMU/KVM
gssso355	provisioning	Unknown			0 EPS	0 b/s	
gssso368	provisioning	Unknown			0 EPS	0 b/s	
gssso378	provisioning	Unknown			0 EPS	0 b/s	
gssso388	provisioning	Unknown			0 EPS	0 b/s	
gssso406	provisioning	Unknown			0 EPS	0 b/s	
gssso442	provisioning	Unknown			0 EPS	0 b/s	
gssso444	provisioning	Unknown			0 EPS	0 b/s	ESXi
gssso453	provisioning	Unknown			0 EPS	0 b/s	
gssso458	provisioning	Unknown			0 EPS	0 b/s	
gssso461	provisioning	Unknown			0 EPS	0 b/s	
gssso467	provisioning	Unknown			0 EPS	0 b/s	
gssso468	provisioning	Unknown			0 EPS	0 b/s	

By default, the table is filtered by any status that is not *Decommissioned*. The default status filter (any status other than *decommissioned*) is the equivalent of the previous *Enabled* value.



Sensors for GigaSMART Soak Test

401 Sensors out of 500 max

SENSOR ID	STATUS	VERSION	LABELS	LOCATION	EPS (7 DAY AVERAGE)	BITS/S (7 DAY AVERAGE)	TYPE
gssso333	offline	version2	Exclude from monitoring status test test test	Tracy, CA	0 EPS	0 b/s	QEMU/KVM
gssso355	provisioning	Unknown			0 EPS	0 b/s	
gssso368	provisioning	Unknown			0 EPS	0 b/s	
gssso378	provisioning	Unknown			0 EPS	0 b/s	
gssso388	provisioning	Unknown			0 EPS	0 b/s	
gssso406	provisioning	Unknown			0 EPS	0 b/s	
gssso442	provisioning	Unknown			0 EPS	0 b/s	
gssso444	provisioning	Unknown			0 EPS	0 b/s	ESXi
gssso453	provisioning	Unknown			0 EPS	0 b/s	
gssso458	provisioning	Unknown			0 EPS	0 b/s	
gssso461	provisioning	Unknown			0 EPS	0 b/s	
gssso467	provisioning	Unknown			0 EPS	0 b/s	
gssso468	provisioning	Unknown			0 EPS	0 b/s	

Additional Filters

Status

Offline, Online, Provisioning, Shutdown

All

No Filters

☐ Decommissioned

☐ Decommissioned (auto)

☐ Decommissioned (legacy)

☒ Offline

☒ Online

☒ Provisioning

☒ Shutdown

# 14 February 2024 version 2024.1.1

FortiNDR Cloud includes bug fixes, but no new features. See [Resolved issues on page 19](#).

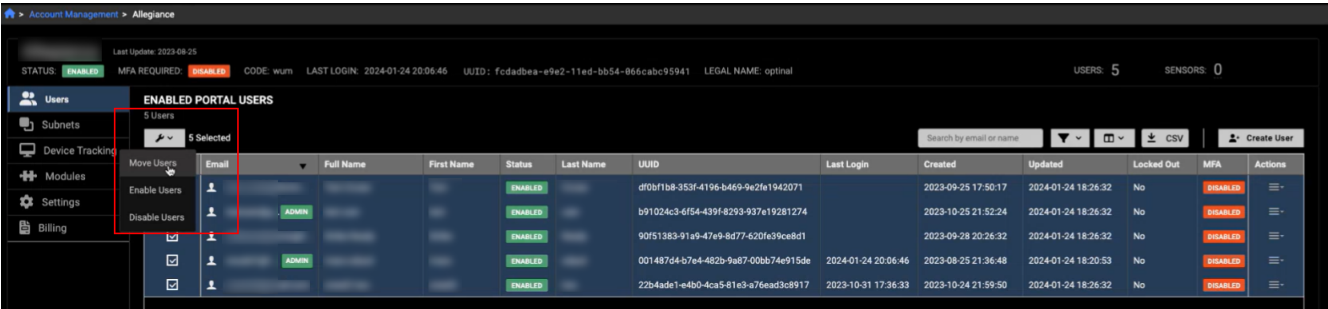
# 31 January 2024 Version 2024.1.0

- Improved functionality
  - Account management
  - Sensor table
  - Password enforcement
- Resolved Issues

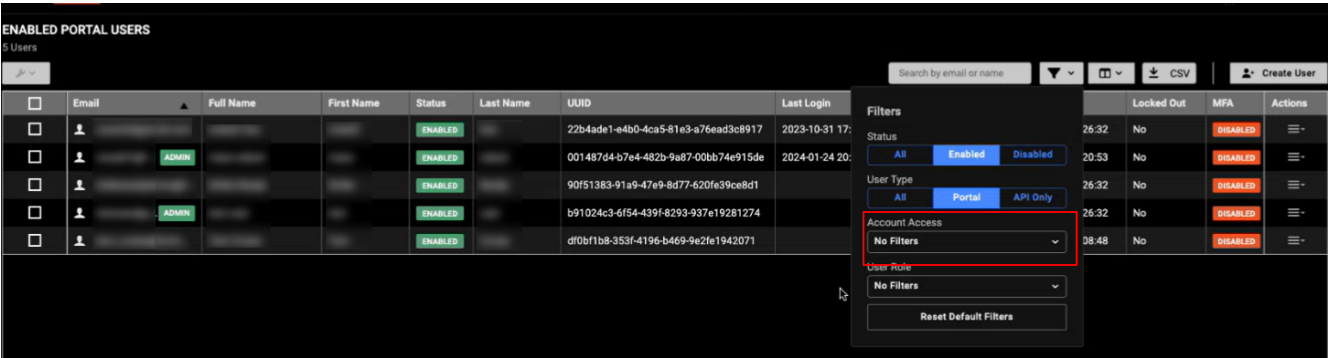
## Improved functionality

### Account management

You are now able to move, enable, and disable multiple users at once in *the Account Management > Users* page. Simply select the users (or select all) and choose a bulk action from the menu. When you click *Confirm*, the bulk action status dialog appears as well as a message with the results. If you attempt to perform a bulk action on your own user account, the action will fail.



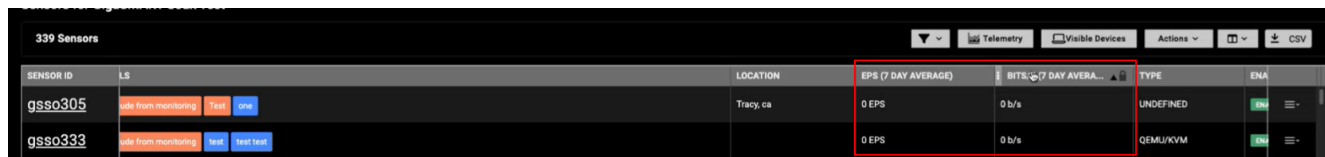
You are also able to filter users by account access.





## Sensor table

The sensor table has been updated to behave like the other tables in FortiNDR Cloud. The *Location* column now displays an empty cell when the location is unknown. The *7 Day Average Throughput* column has been split into two columns: *EPS (7 Day average)* and *BITS/S (7 Day average)*. This allows you to sort each column individually.



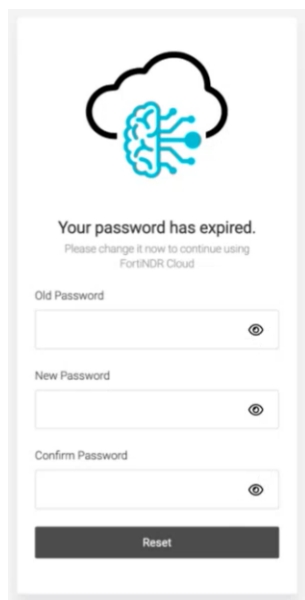
SENSOR ID	LS	LOCATION	EPS (7 DAY AVERAGE)	BITS/S (7 DAY AVERAGE)	TYPE	ENA
gssso305	<a href="#">View from monitoring</a> <a href="#">Test</a> <a href="#">One</a>	Tracy, ca	0 EPS	0 b/s	UNDEFINED	<a href="#">On</a>
gssso333	<a href="#">View from monitoring</a> <a href="#">Test</a> <a href="#">Test test</a>		0 EPS	0 b/s	QEMU/KVM	<a href="#">On</a>


## Password enforcement

The application will notify you when your password is about to expire. You can click the link in the dialog to open the reset password page. After you change a password, it will expire in 180 days. Passwords must be at least eight characters long.



If you attempt to log in after your password has expired, you will be prompted to create a new password.





Your password has expired.  
Please change it now to continue using  
FortiNDR Cloud

Old Password

New Password

Confirm Password

Reset

## New detection rules and observations

The following table lists the new detections rules and observations in FortiNDR Cloud:

### 2024.3.0

#### Rules

Primary ATT&CK Name	ATR Category
<b>Exploit Public-Facing Application</b>	Attack:Exploitation > Exploit Public-facing Application
<b>Non-Application Layer Protocol</b>	Posture:Potentially Unauthorized Software or Device

### 2024.2.0

#### Observations

Name	Description
<b>SSL C2 Beacons Similarity</b>	Identify SSL connections that resemble Command and Control (C2) beacons activity: telemetry that tells a C2 server the client is active and /or requests command(s) to execute. This observation performs statistical characterizations of the SSL connection to look for client software that calls back to a server on an extremely periodic schedule.

#### Rules

Primary ATT&CK Name	ATR Category
<b>Web Protocols</b>	Attack:Command and Control > Web Shell
<b>Ingress Tool Transfer</b>	Attack:Installation > Remote File Copy from External
<b>Domain Groups</b>	Attack:Discovery > Network Directory Scanning
<b>LLMNR/NBT-NS Poisoning and SMB Relay</b>	Attack:Infection Vector > LLMNR/NBT-NS Poisoning

Primary ATT&CK Name	ATR Category
Exploitation for Client Execution	Attack:Exploitation
Lateral Tool Transfer	Attack:Installation > Remote File Copy from External
Application Layer Protocol	PUA:Spyware

# Resolved issues

The following issues have been fixed in version 2024. To inquire about a particular bug, please contact [Customer Service & Support](#).

## 2024.3.0

Description
Power users can see the labels in the <i>Sensors</i> column in all accounts without Read/Write permissions.
Fixed a date picker issue where the start/end date does not update after resolving an error.
An SSO <i>Account</i> error page no longer appears when a page is refreshed.
Resolved an issue where all accounts displayed telemetry data in the <i>Sensor</i> page.

## 2024.2.1

Description
Refreshing the <i>Account Management</i> page no longer generates an error screen.
Resolved an issue where <i>Observations</i> dashboard was not recovering from a previous failed query.
The <i>Account Management</i> detail page no longer shows the wrong permissions.
Resolved all permission issues (such as <i>Edit</i> and <i>Disable</i> ) in the <i>Child Account</i> tab in the <i>Account Detail</i> page.
Fixed issues with Admin permissions in the <i>Subnet</i> tab.
Fixed the permission in <i>Settings</i> tab.
Fixed the Admin permissions in the <i>Device Tracking</i> tab.
The <i>Decommissioned</i> status the sensor's details page now matches the status in the <i>Sensors</i> page .

## 2024.2.0

Description
Users with multiple accounts will see the <i>Edit</i> button for the accounts with <i>Admin</i> permissions.

### Description

Clicking an IP in the *src* column that has multiple annotations no longer opens the *Entity Panel*.

The error message styling has been improved to make it easier to read.

The *Rule Name* filter in the *Detections* table no longer disappears when the dropdown is closed.

## 2024.1.1

### Description

GUI: *Bulk Move* is no longer available to Admins with one account .

GUI: *Sensors* list page no longer displays the *Edit* button to users with only a user role in an account.

GUI: The *BITS/S (7 DAY AVERAGE)* column on the *Sensors* list page no longer displays *undefined/s* units.

A scroll bar was added to the *Update Account Dialog* in the Parent Account dropdown.

*Detections* table does not show error if there are a large number of active rules.

Detail View: Resolved an issue where the description header was missing when switching pages in the *Details* view.

Resolved an issues where the investigation was not selected when clicking *Add to existing investigation*.

## 2024.1.0

### Description

*Account Management*: The *Account Management* breadcrumb no longer appears as plain text when the user has multiple admin roles.

Refreshing the *Edit Rule* page no longer takes you to the *Rule Details* page.

Resolved an issue where clicking the title in a Dashboard widget did not launch the *Add query to Investigation* dialog.

*Investigations*: When a user switches accounts after copying a URL in the *Investigations* page, the URL will redirect back to the correct account as expected.

*Sensors* : *Telemetry* now displays the correct units in the *Sensors* page.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.