Release Notes

FortiNDR Cloud 2024

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

February 27, 2025
FortiNDR Cloud 2024 Release Notes
78-242-1113279-20250227

TABLE OF CONTENTS

FortiNDR Cloud release notes

This document provides information about FortiNDR Cloud 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
11 December 2024	11 December version 2024.11.0 on page 6
05 November 2024	05 November 2024 version 2024.10.0 on page 14
25 September 2024	25 September 2024 version 2024.9.0 on page 20
09 September 2024	09 September 2024 version 2024.8.1 on page 26
28 August 2024	28 August 2024 version 2024.8.0 on page 26
31 July 2024	31 July 2024 version 2024.7.0 on page 35
26 June 2024	26 June 2024 version 2024.6.0 on page 39
29 May 2024	29 May 2024 version 2024.5.0 on page 43
15 May 2024	15 May 2024 version 2024.4.1 on page 46
01 May 2024	01 May 2024 version 2024.4.0 on page 46
10 April 2024	10 April 2024 version 2024.3.1 on page 49
27 March 2024	27 March 2024 version 2024.3.0 on page 49
13 March 2024	13 March 2024 version 2024.2.1 on page 53
29 February 2024	29 February 2024 version 2024.2.0 on page 54
14 February 2024	14 February 2024 version 2024.1.1 on page 59
31 January 2024	31 January 2024 Version 2024.1.0 on page 59

11 December version 2024.11.0

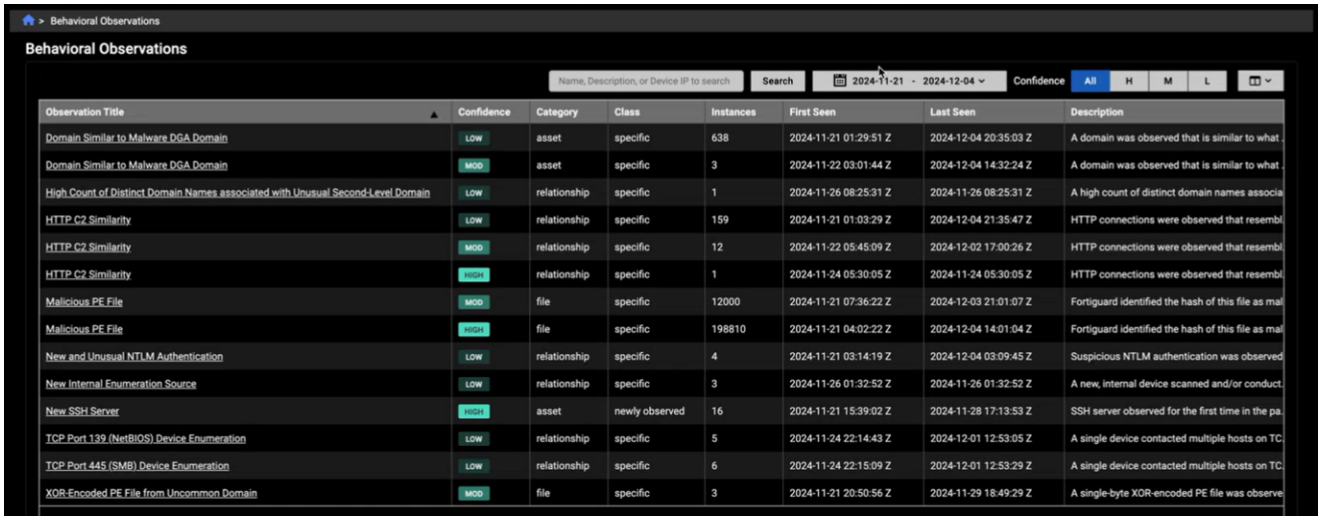
New functionality

Dashboard

Behavioral Observations

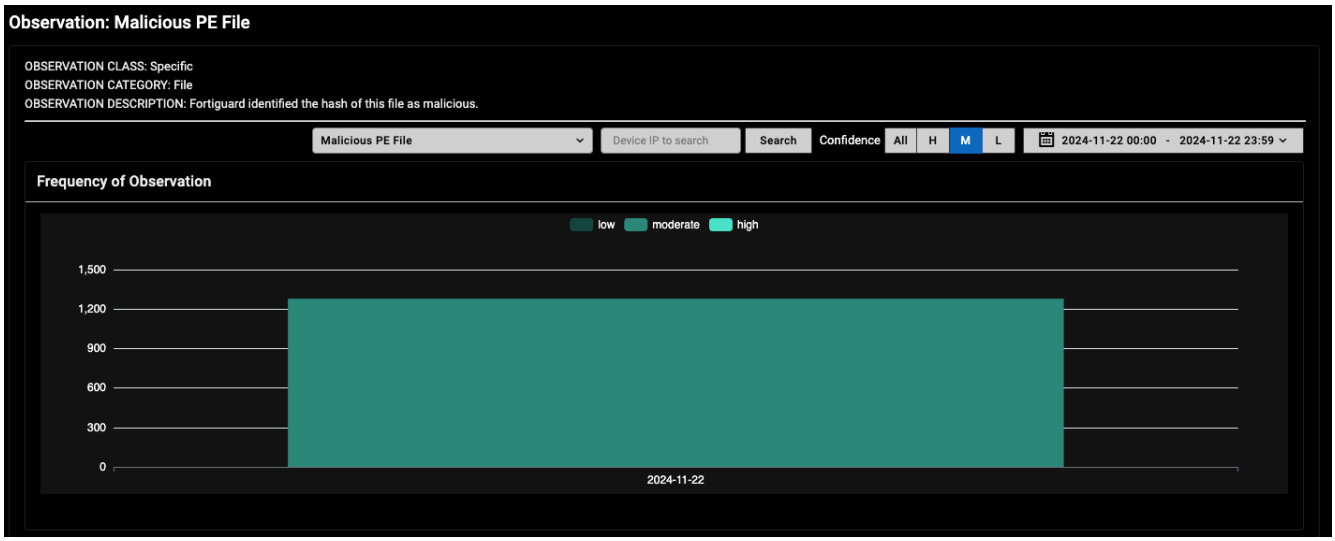
The *Observations* widget in the dashboard has been replaced with the *Behavioral Observations* widget.

Click the widget title to open the *Behavioral Observations* list page. You can use the search field to find observations that contain instances of a specific IP address or text in the *Observation Title* and *Description* columns.

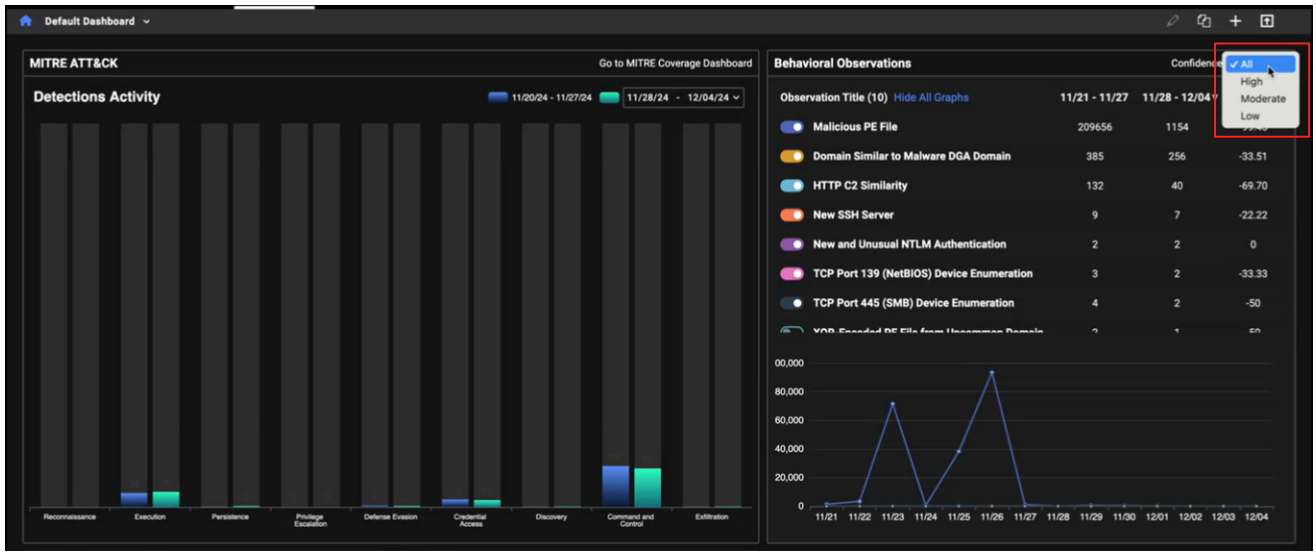


When you click an individual observation in the dashboard widget, it will open the *Observation Details* page.

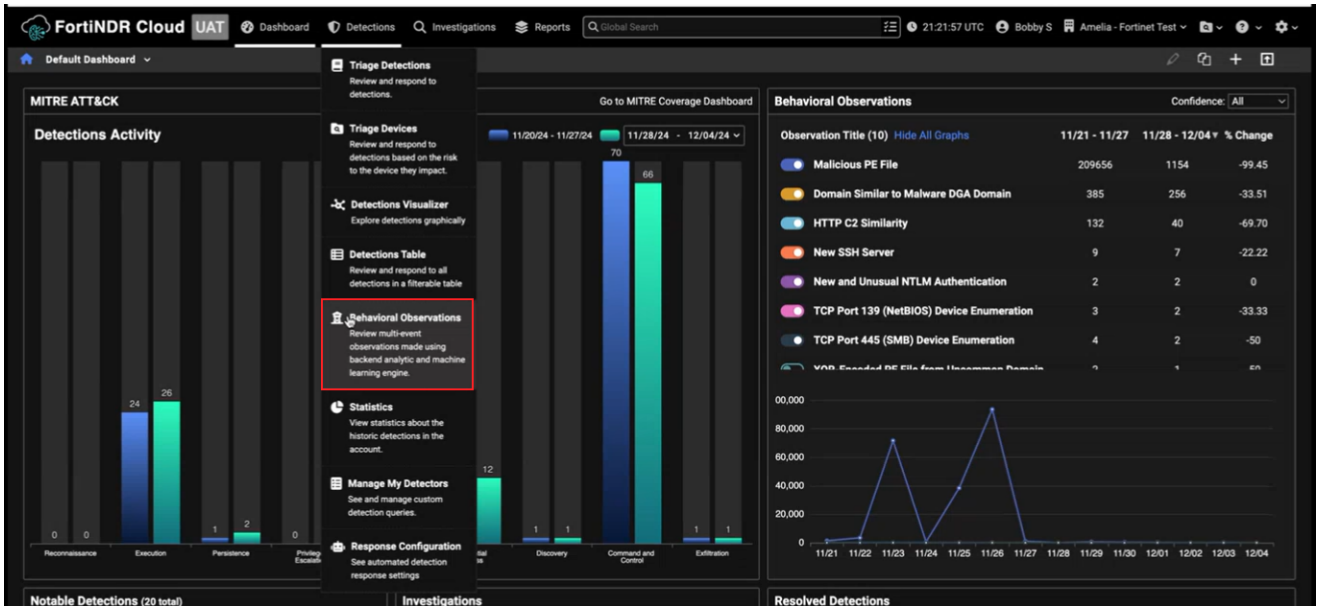
When you click on any part of the observation frequency chart, the time range and confidence filter for that part of the chart will be applied to the page.



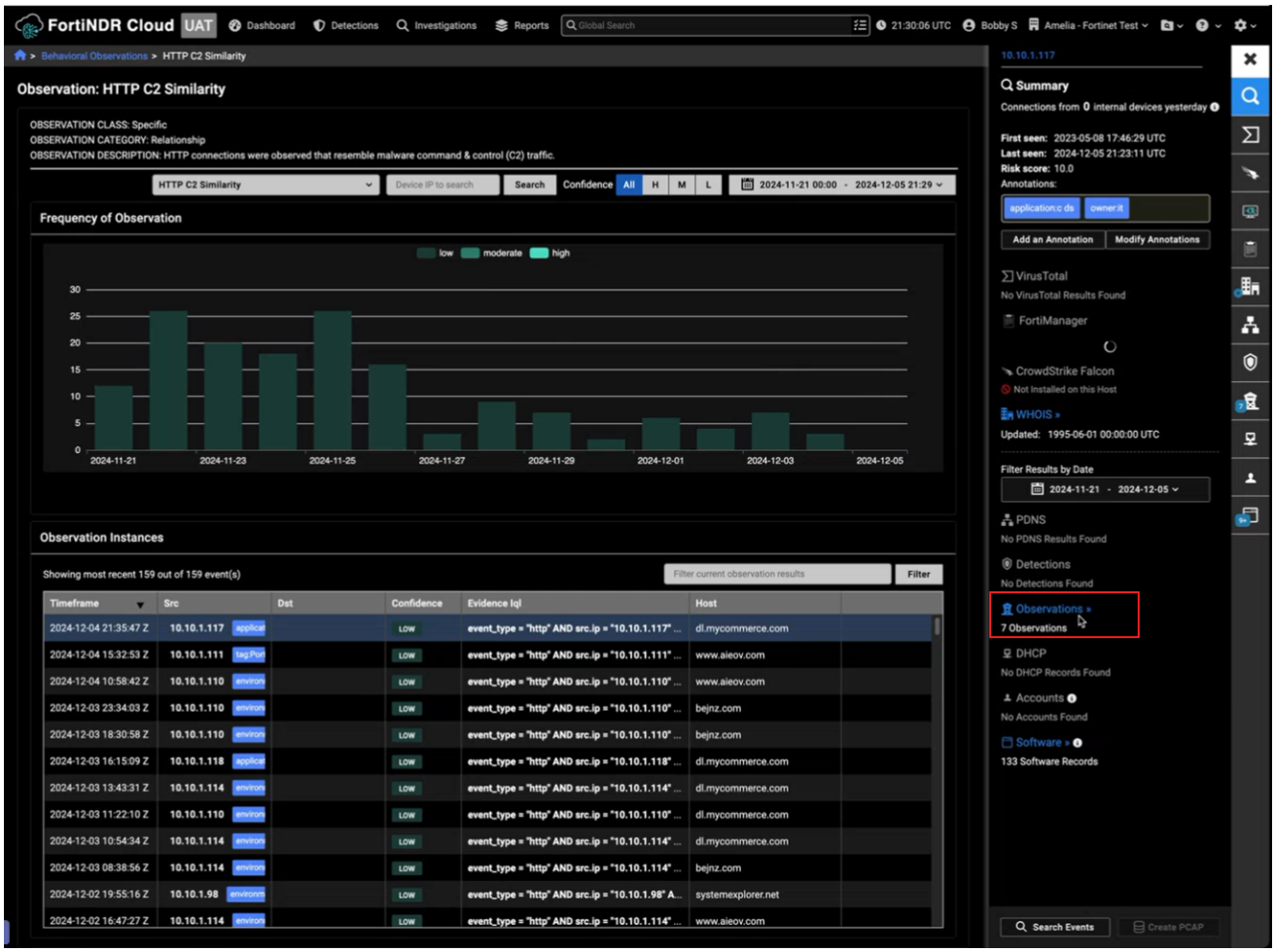
You can filter the observations in the widget by confidence level. When you click an observation with that confidence level in the filter, the observations in the details page will reflect that confidence level.



Behavioral Observations have also been added to the *Detections* menu which takes you to the *Behavioral Observations* list page.

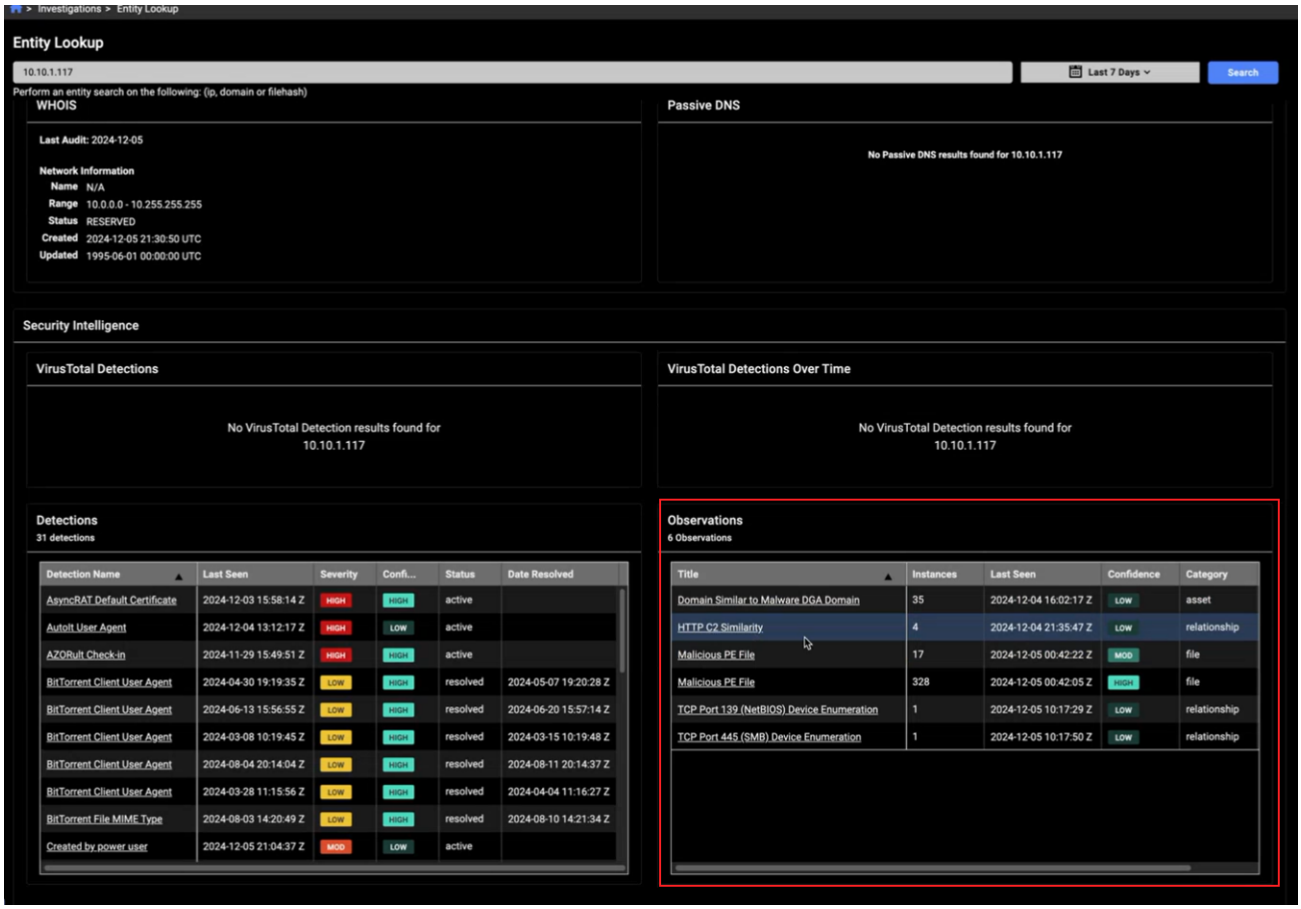


An *Observations* section was also added to the *Entity Panel*.



Click the link, or the *Observations* icon to view the observations in the panel. When you click on an observation in the list it will open the *Observation Details* page.

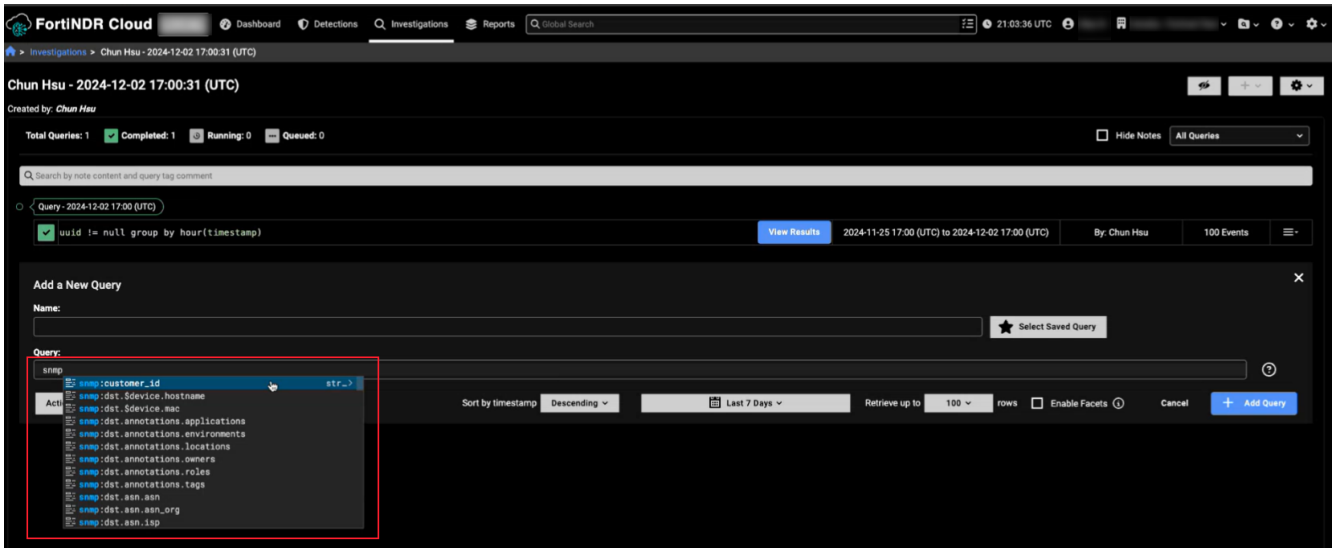
An *Observations* table was also added to the *Entity Lookup* page which shows the observations for the IP within the specified time range. When you click on the observation name in the table it will open the *Observation Details* page preserving the time range and confidence level.



Investigations

SNMP queries

FortiNDR Cloud now supports SNMP event queries.

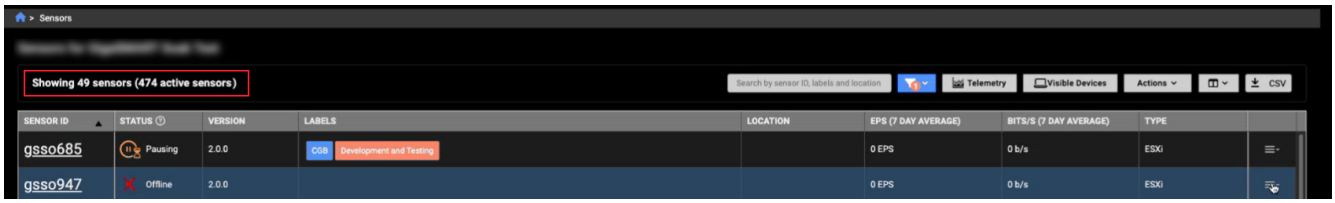


Improved functionality

Sensors

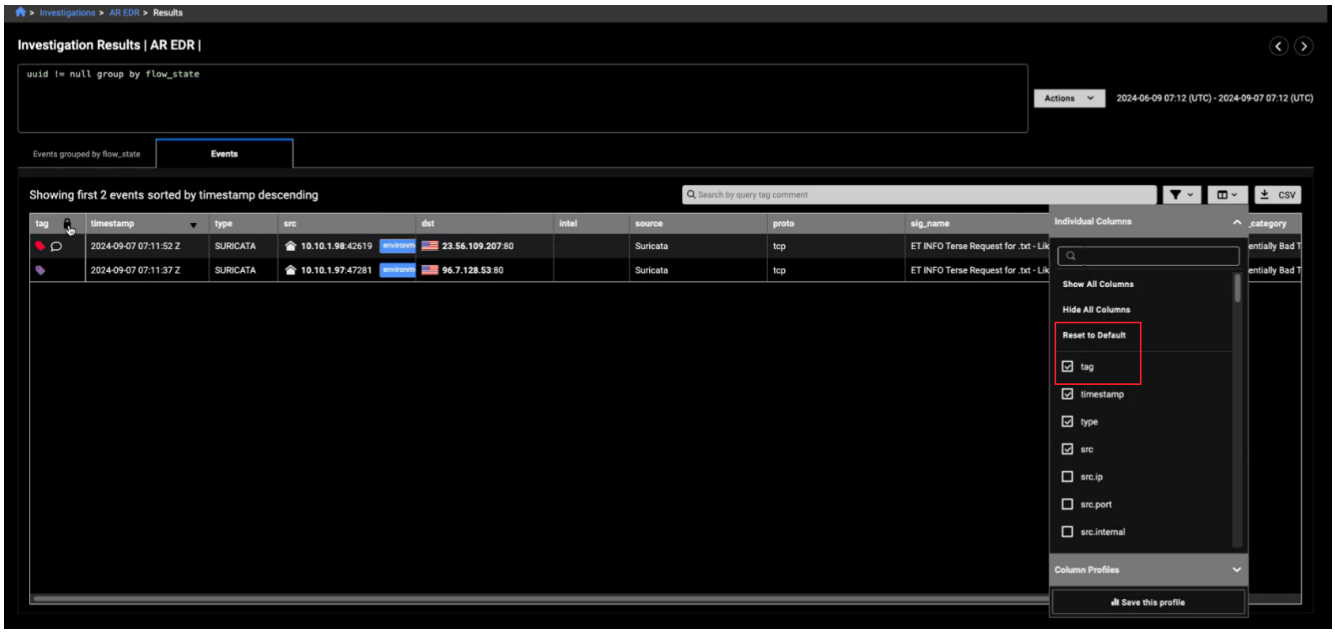
In sensors running version 2.0 or later, we have introduced a *Pausing* and *Resuming* state to indicate the sensor is in the process of being paused or resumed.

We have also added context to the number of sensors to indicate the number sensors and the number of active sensors.



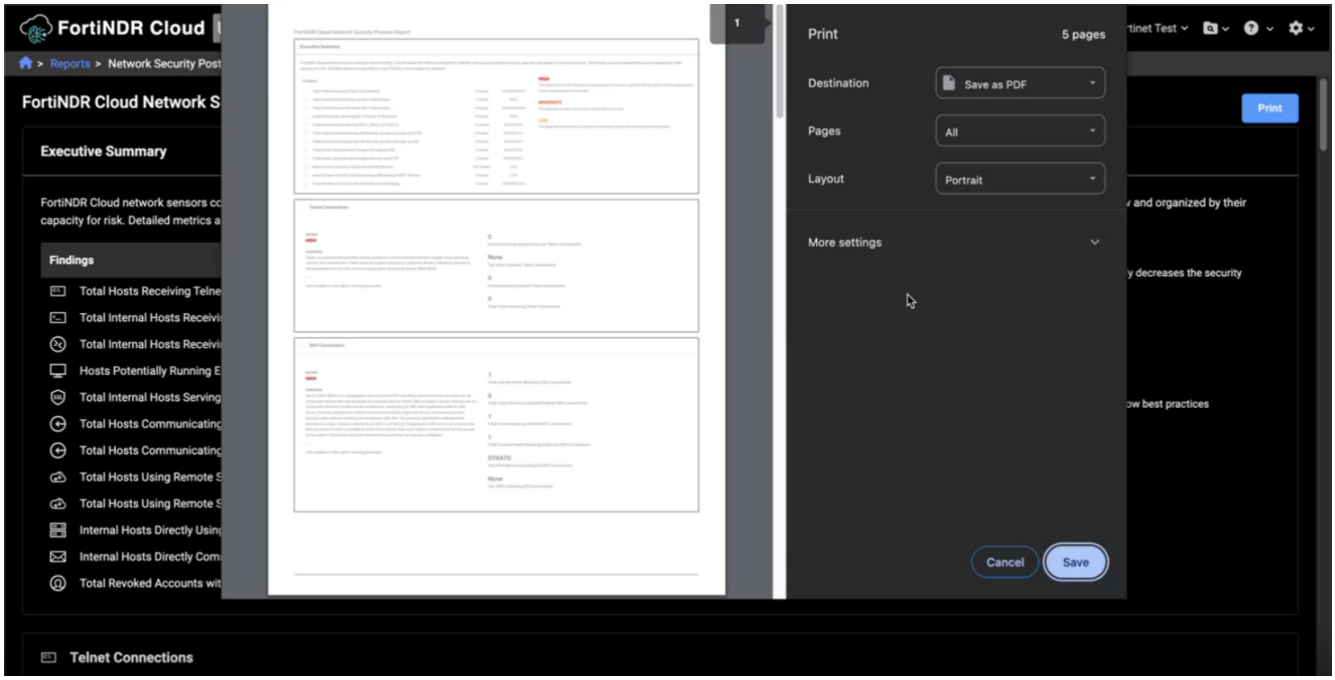
Tags

We have improved the behavior of the *Tags* column in *Investigations* to make it is easier to find. To lock the *tag* column to the left side of the table, in the *Individual columns* filter under *Individual Columns*, select *Reset to Default* or *tag*. You can also lock the column by selecting *Default* under the *Column Profile* in the same menu.



Reports

We have added a *Print* button and print dialog with preview for PDF reports.



Other improvements / changes

- The *Default width* setting has been renamed *Header width* in the *Investigations* tab in the column headers.
- You can now sort all the columns in the *Annotations* table by clicking the column header.

- We redesigned the tooltip in the *Entity Lookup* to include a scroll bar to fit the page.

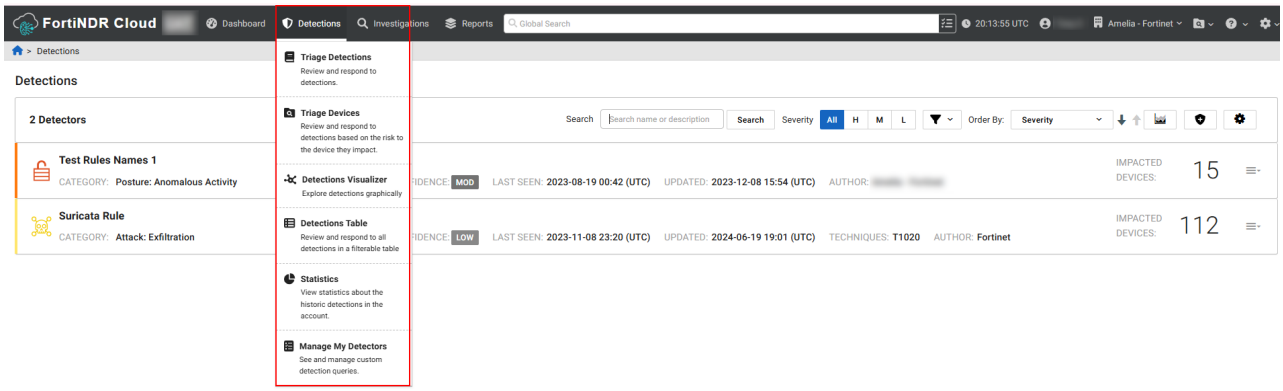
05 November 2024 version 2024.10.0

New terminology

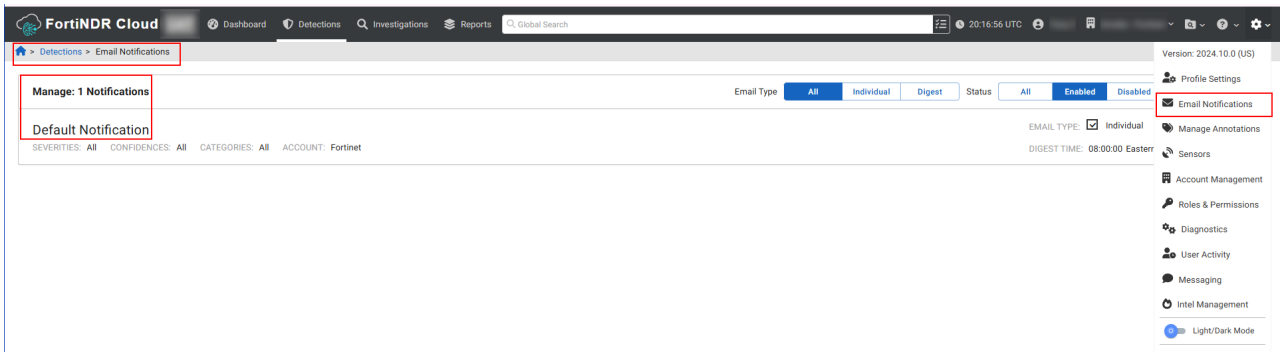
We have updated our terminology to be consistent with standard industry terms so that our documentation and user interface is more intuitive and accessible.

Please be aware we have changed the names of several modules in the portal:

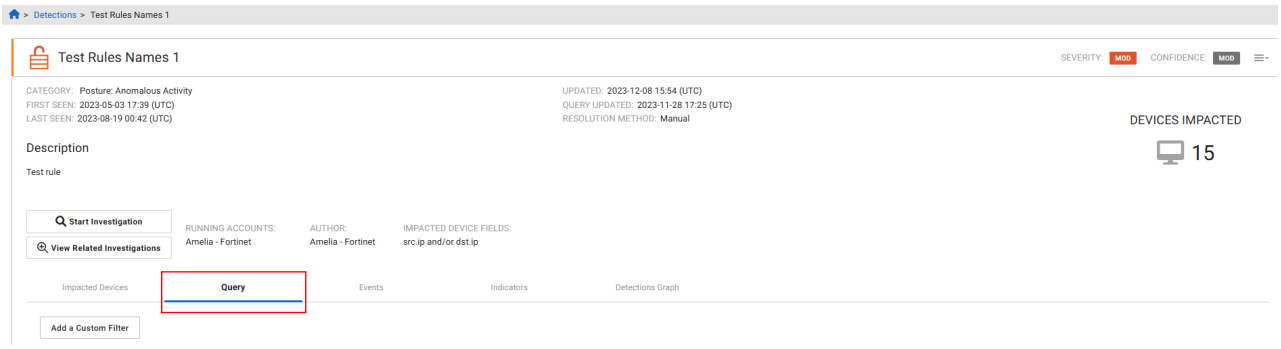
- *Rules* are now referred to as *Detections* or *Detectors*.



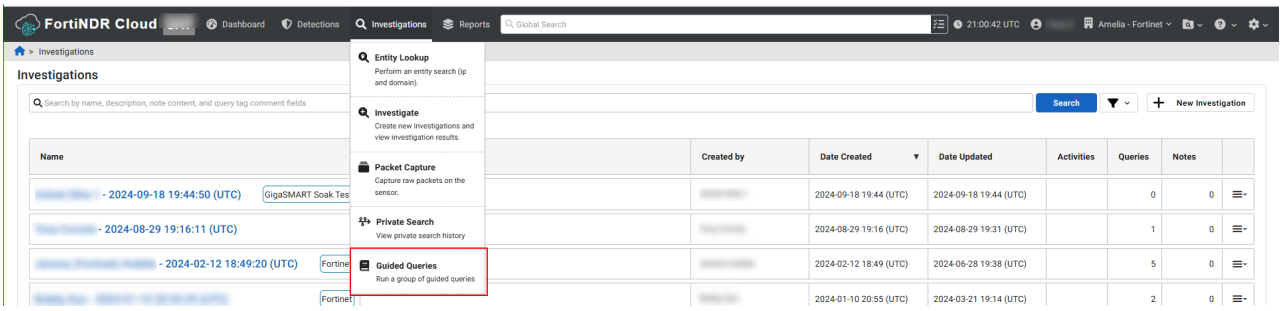
- *Subscriptions* are now *Notifications*.



- *Signatures* are now referred to as *Query* or *Queries*.



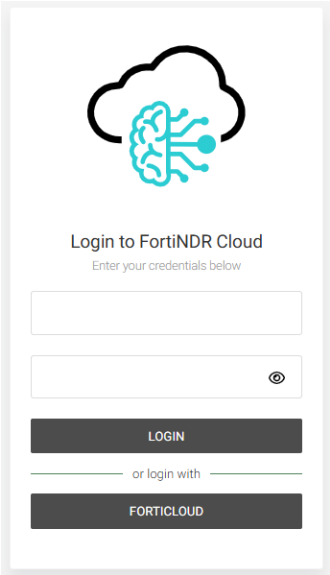
- *Playbooks* are now named *Guided Queries*.



New functionality

Login with FortiCloud

You can now log into the FortiNDR Cloud portal using your FortiCloud account. You must have a valid FortiCloud account that matches an existing FortiNDR Cloud account to use this option.



Improved functionality

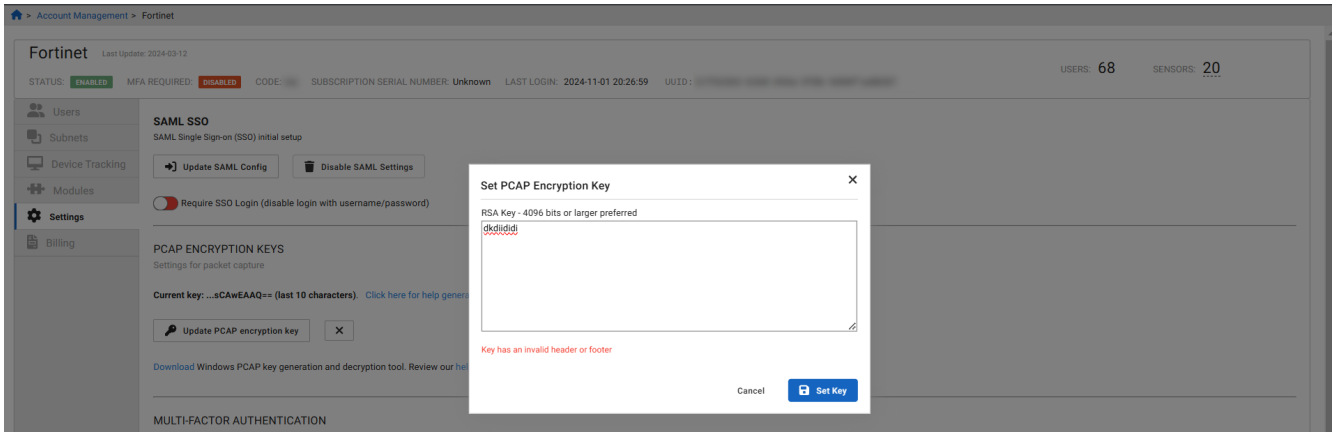
Sensors

We have also added a new *Decommission Pending* status to the *Sensors* page.

Account Management

PCAP encryption keys

PCAP encryption keys are now validated in the *Account Management* > *Settings* page.

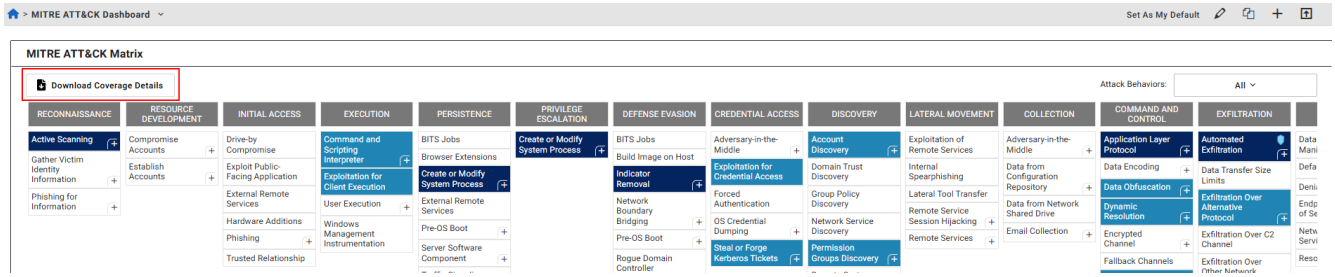


Accounts

A *Last Login* filter has been added to the *Accounts* page. This feature is only applicable to users with access to multiple accounts. You can use this filter to view which accounts are in use to determine if an account should be deleted.

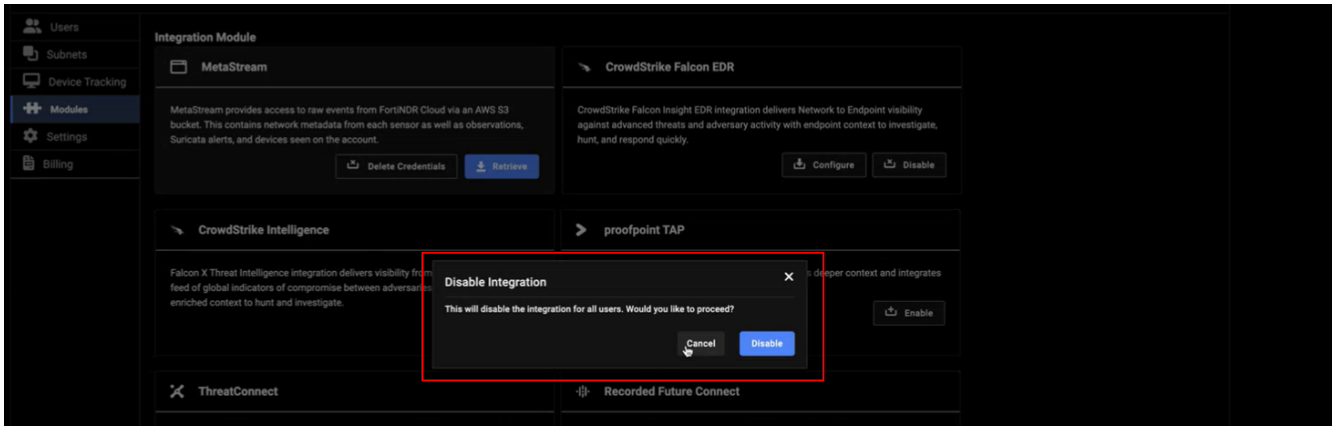
MITRE ATT&CK Matrix

We have added a *Download Coverage Details* button to the *MITRE ATT&CK Matrix* dashboard. Click the button to download the coverage details as a CSV file which contains the *Date Updated*, *Name*, *Primary Attack ID*, *Secondary Attack ID* and *Description*.



Modules

We have added a confirmation message when disabling an integration to prevent disabling an integration by accident.

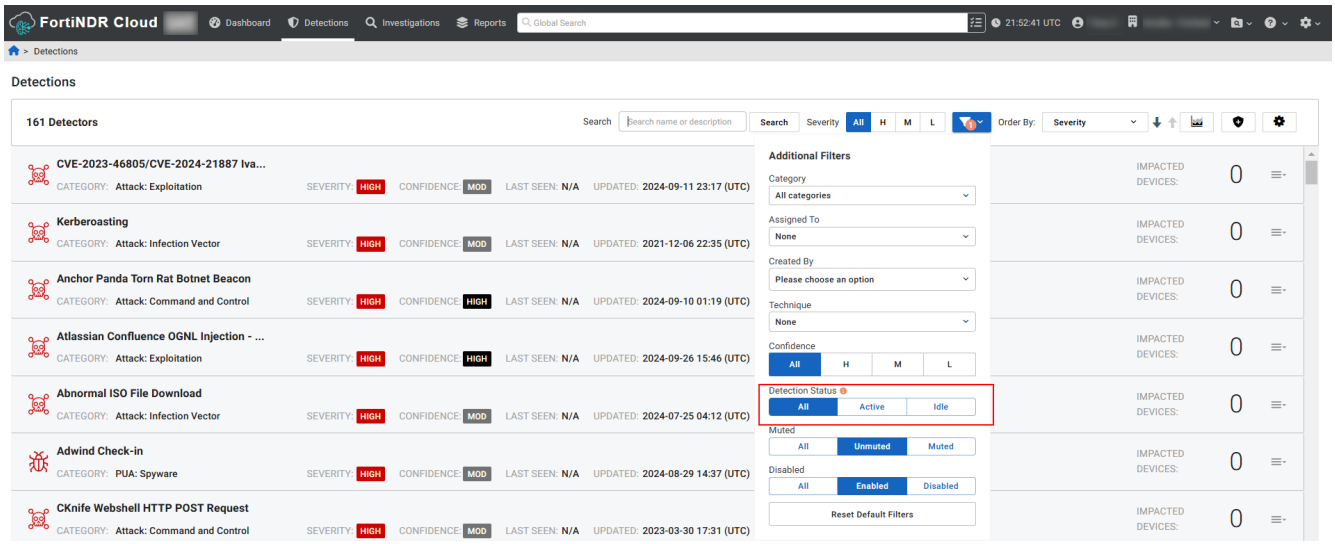


Detections

Triage detections

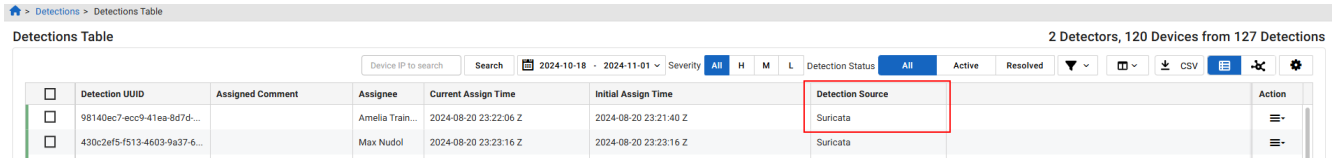
We have updated the *Detection Status* filter logic in the *Triage Detections* page:

- *All*: Returns all detections the user has access to regardless of whether or not it was triggered in the current account.
- *Idle*: Returns all detections that have been triggered in the current account but are not currently active.
- *Active*: Returns all active detections.

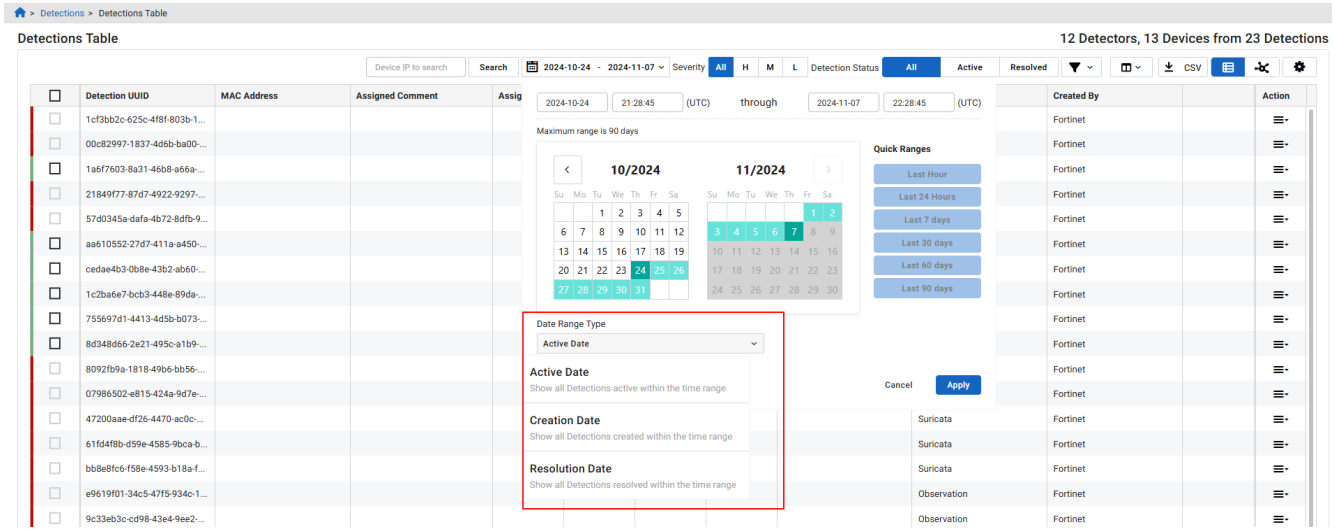


Detections table

We have added a *Detection Source* column to the *Detections Table* which is determined by the detector's query. Note that *Suricata* and *Observation* are the only sources that are displayed at this time, otherwise the field is empty.

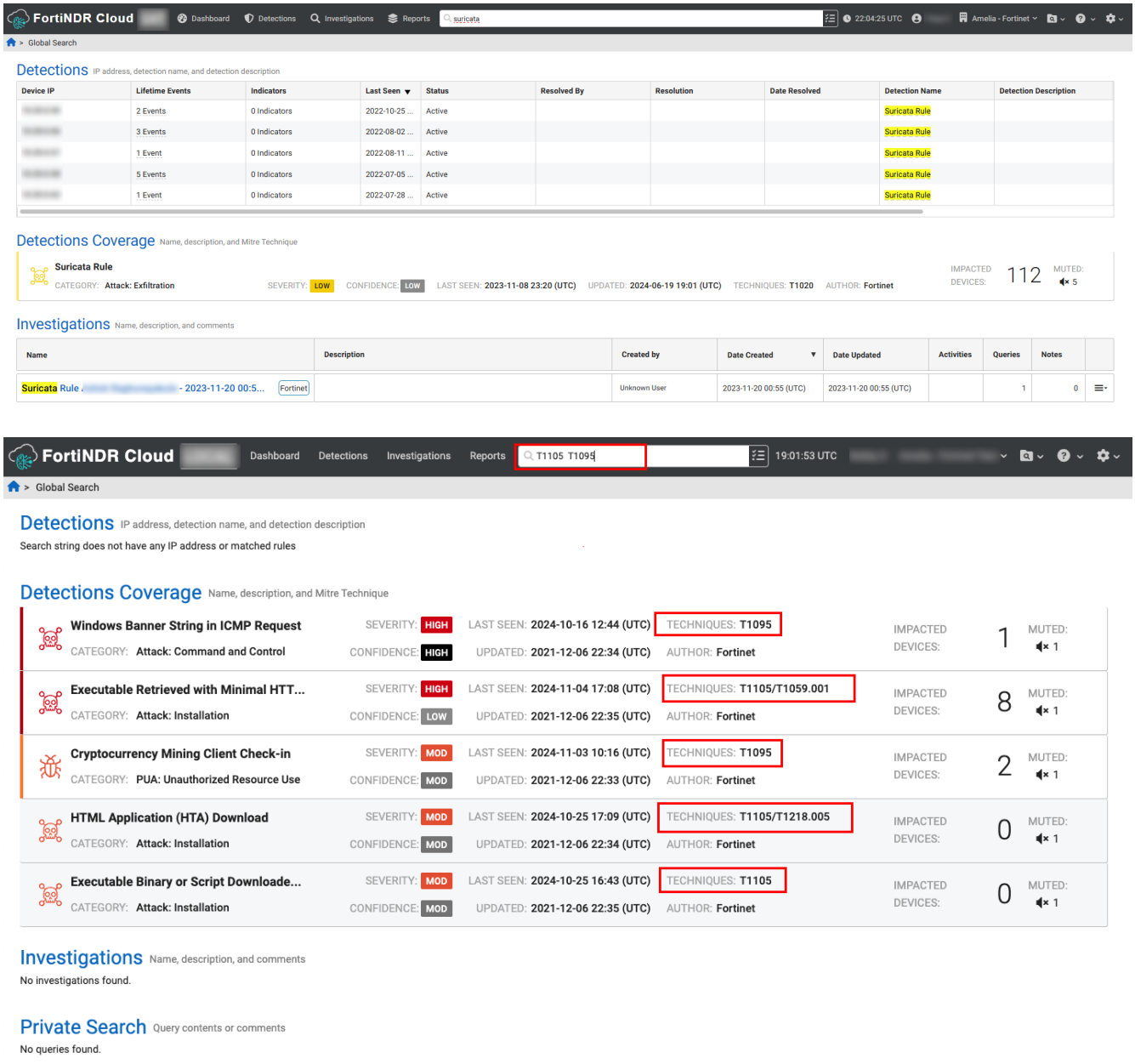


We have also added three new *Date Range Type* options (*Active Date*, *Creation Date*, and *Resolution Date*). The date displayed in the date picker will be displayed in the *Entity Panel*.



Global Search

We have added a *Detections Coverage* section to the Global Search results which shows matches in the detector name, description or technique ID regardless of the detector status.



Other improvements and updates

- The *Fit Width* options has been added to the following pages:
  - Triage Detections Detail
  - Triage Device

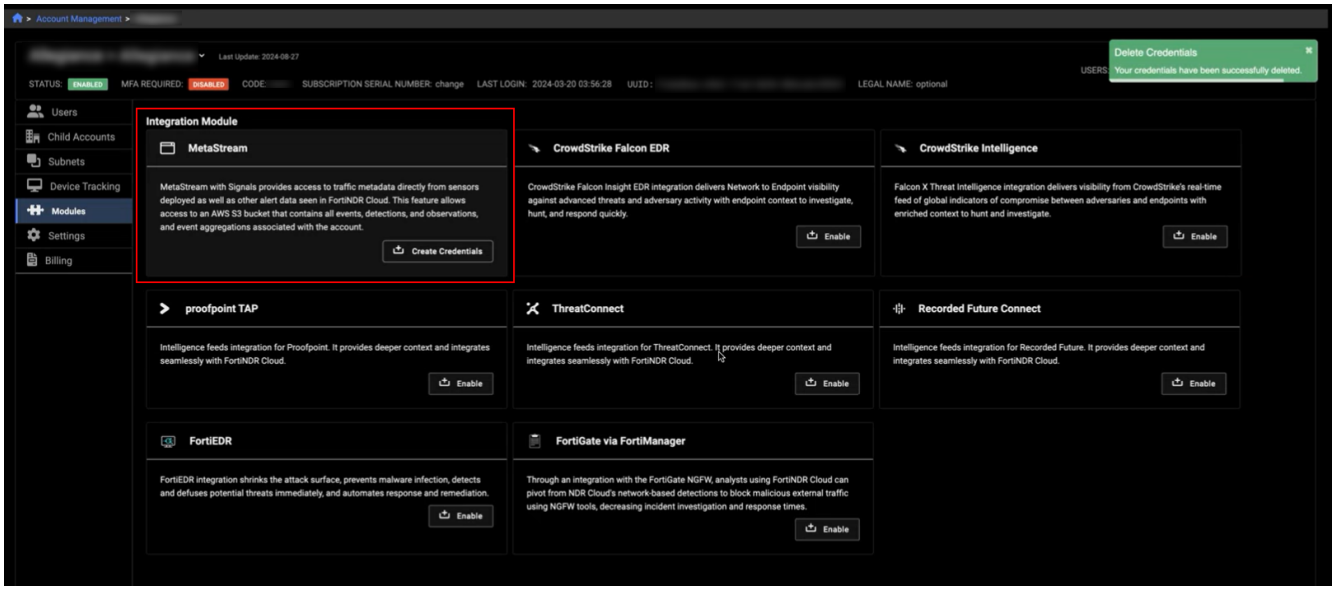
  - Detection Table
  - Sensors
  - User List
- the Zscaler sensor download has been removed. Zscaler integration is now via cloud upload.

25 September 2024 version 2024.9.0

New functionality

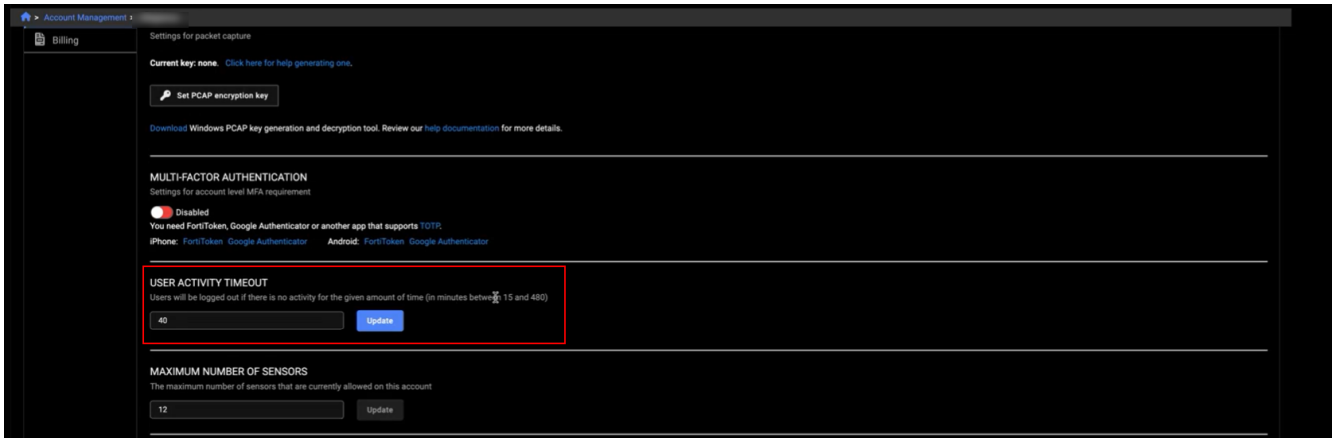
MetaStream Module

The *MetaStream* module is now included with all accounts. Going forward, Admins will only need to create, delete, recreate or retrieve a credential.



User activity timeout

You can now set the amount of inactivity time before a user is automatically logged out of the portal. The new timeout time goes into effect the next time users log into the portal.

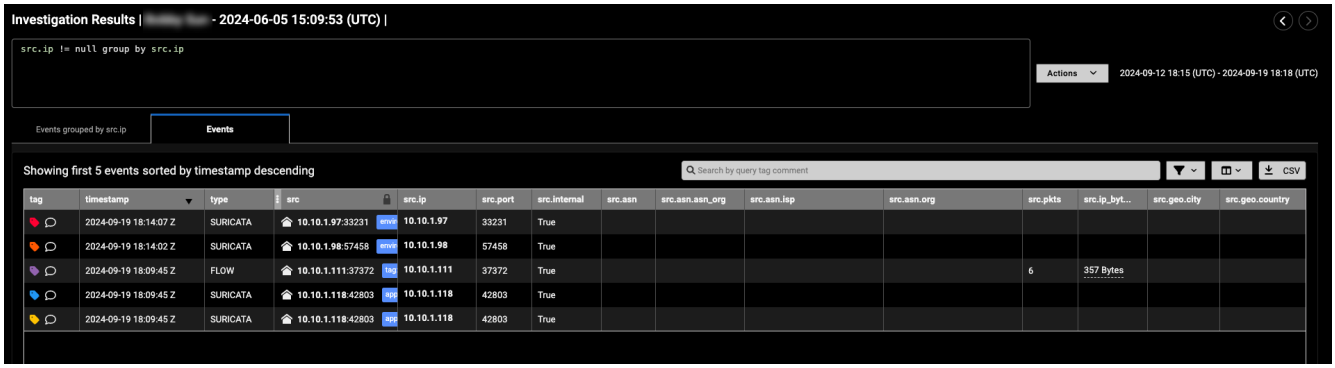


Improved functionality

Pivot to events

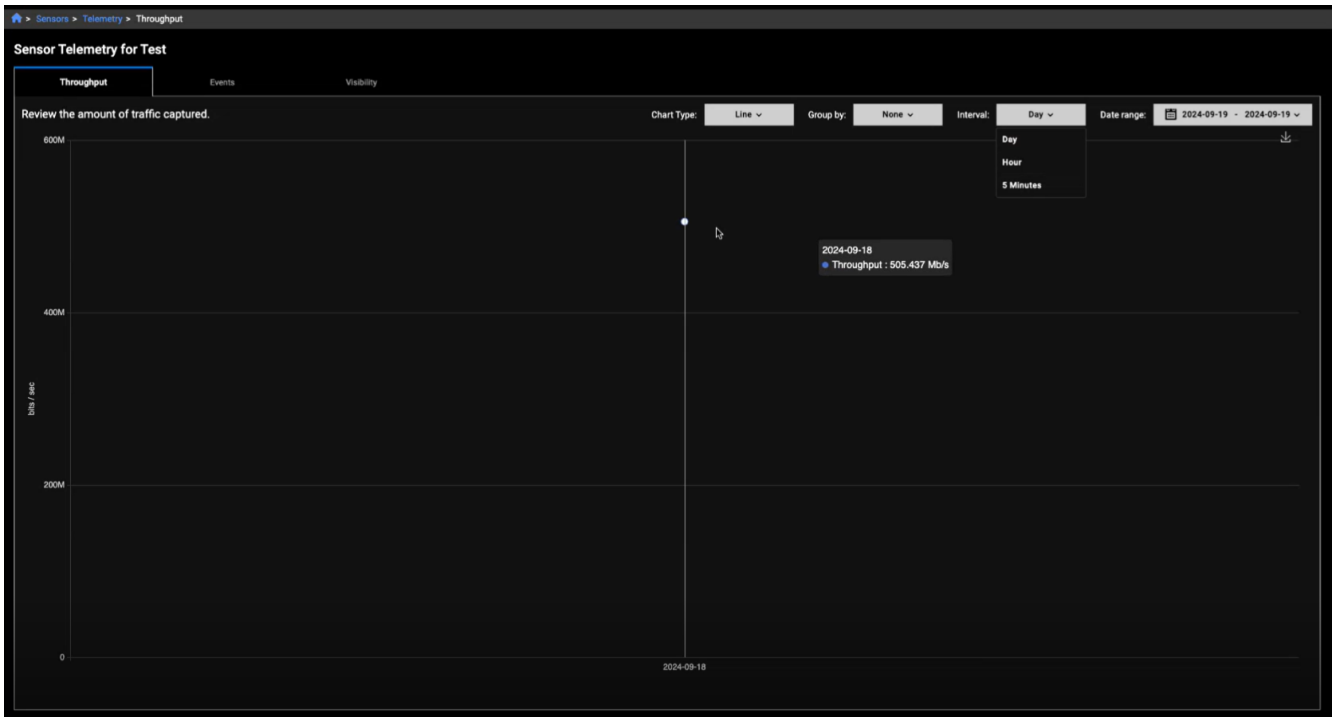
You can now click the tag icon to pivot directly to the *Events* table in an investigation. This saves time navigating to the investigation with the GUI. This function is available on all tags in the investigation tooltip, the investigation detail page, and tagged queries in the *Private Search* page.

The *Events* table will display the same number of events tagged in the investigation dialog.

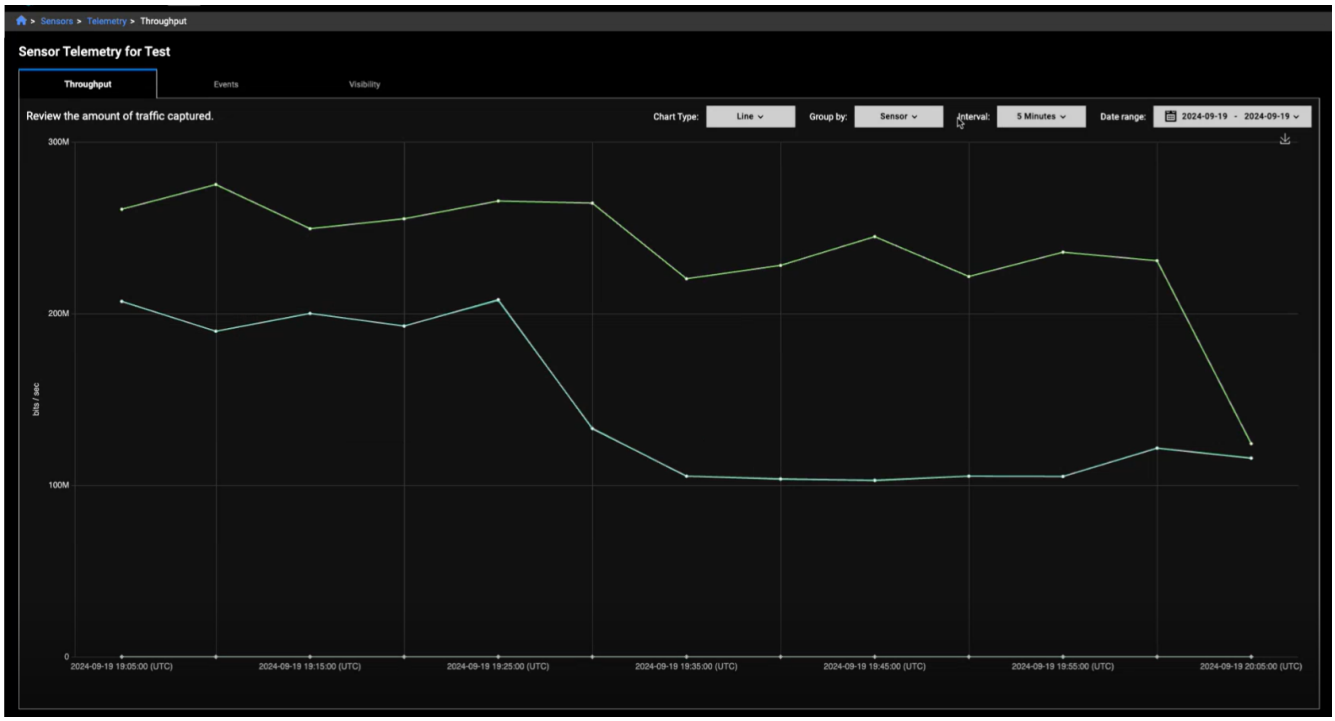


Sensor Telemetry

You can now filter the sensor *Telemetry* data by *Day*, *Hour* and last *5 Minutes*.

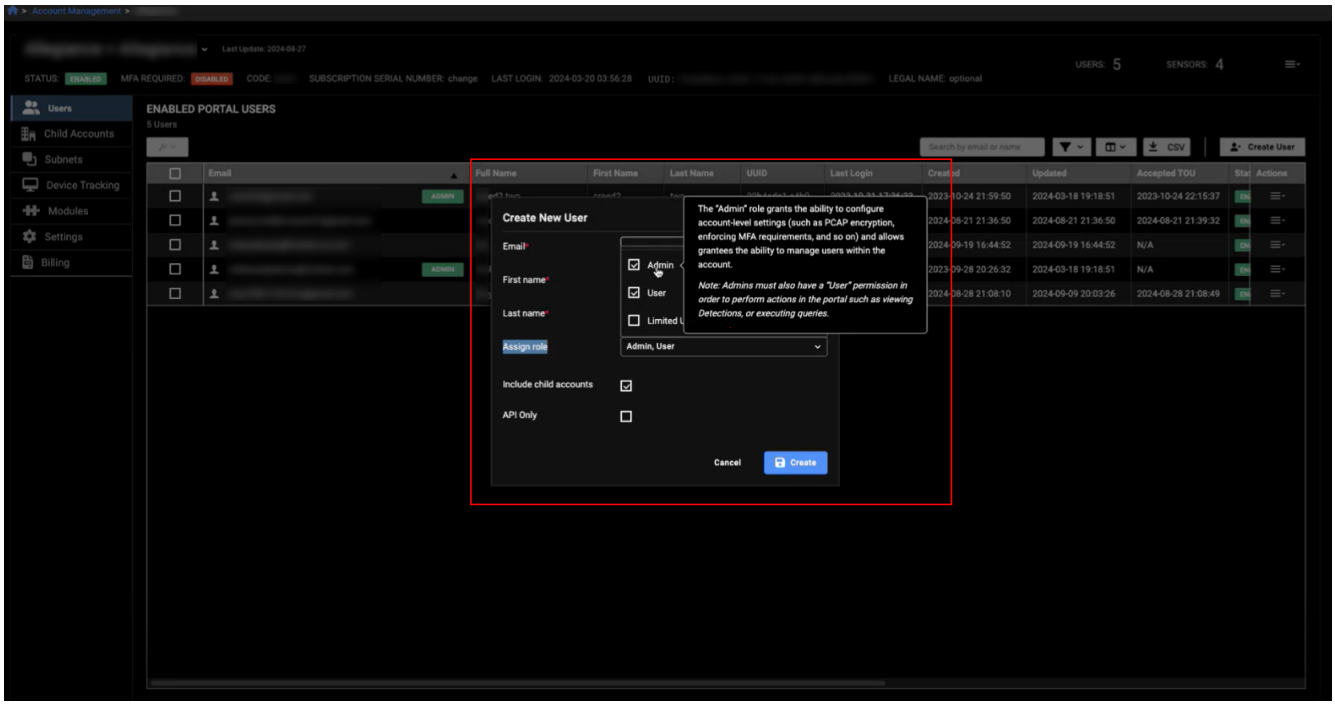


You can also group the page by *Sensor*.

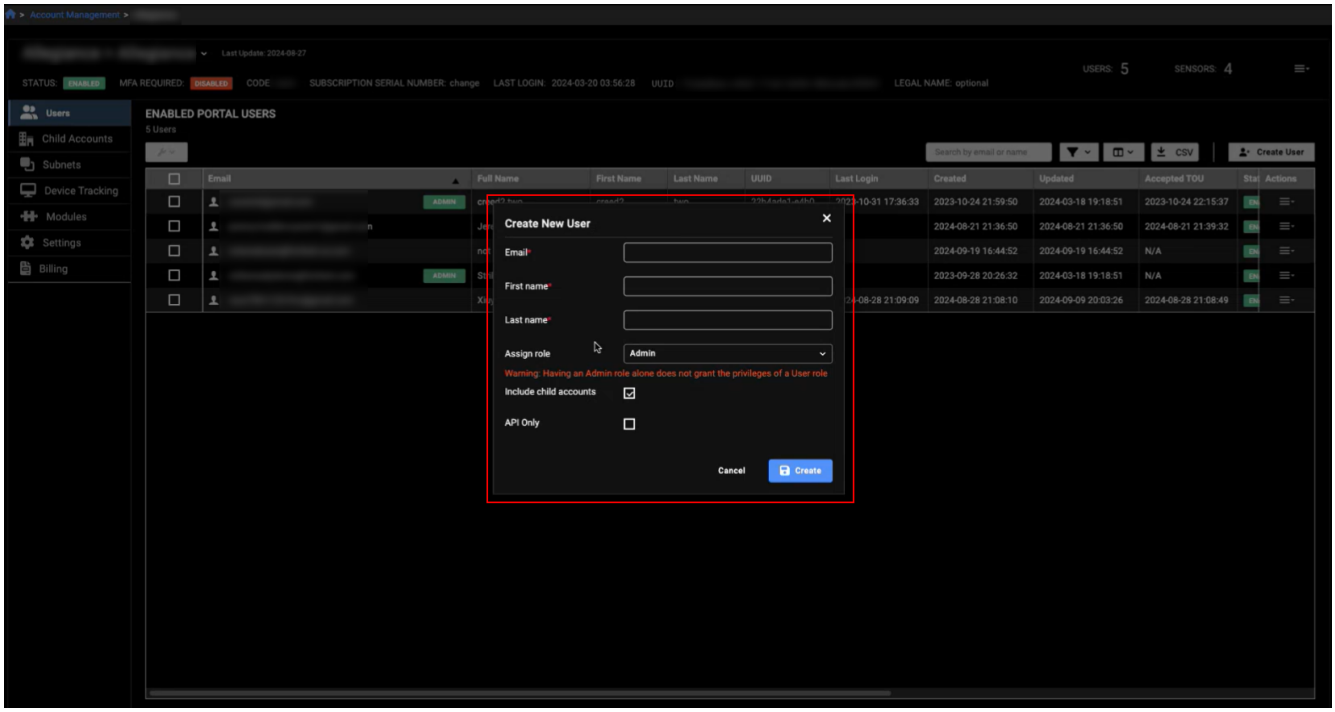


User Roles

We have added a tooltip with a description of each role when you create a new user. The tooltip describes the privileges and limitations of each role and offers suggestions to make sure you are assigning the appropriate role to the user. For example, the new user may need both *Admin* and *User* roles to configure settings and perform queries. To view the description, hover over the name of the role in the dialog.

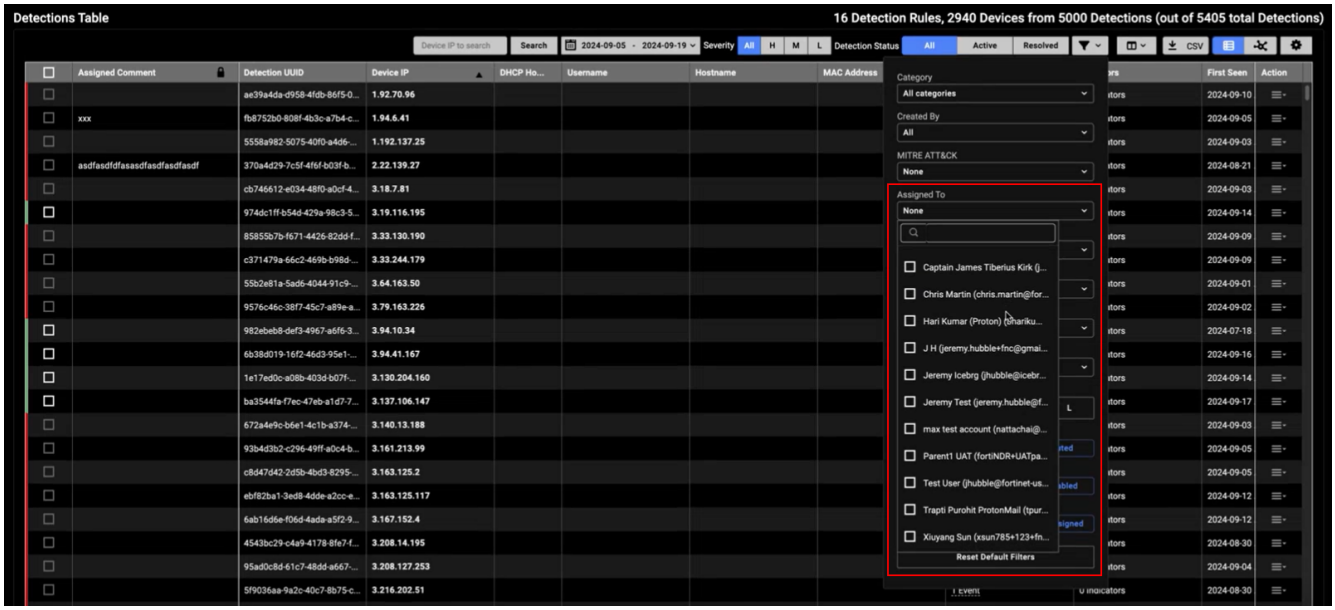


An auto-check is performed when you select the user role. A warning appears to remind you of the limitations of the role. If you choose to ignore the warning, it will not prevent you from creating the new user.



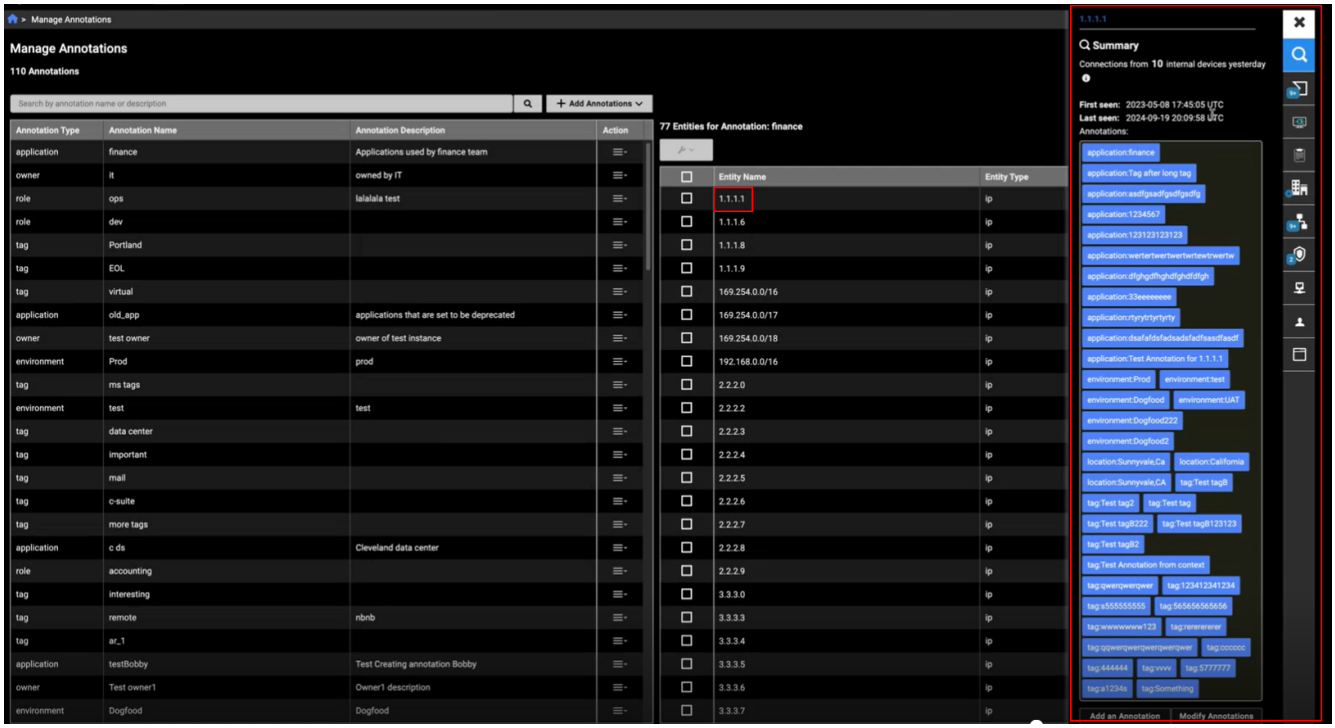
Detection assignment

You can now assign a detection to any active user with any role in the current account. Previously you could only assign detections to active users created in the current account.

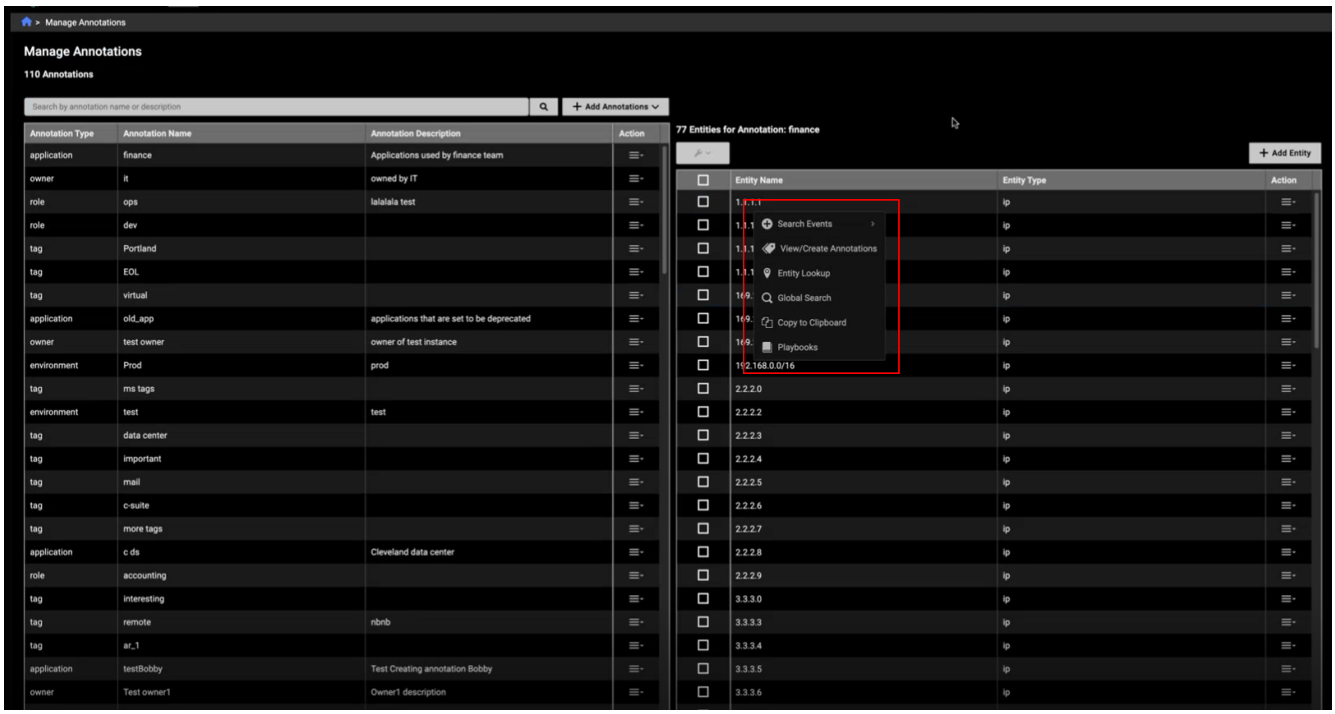


Manage Annotations

You can now open the *Entity Panel* when you click the *Entity Name* in the *Manage Annotations* page when the entity is a valid IP, CIDR, domain, or URL.



You can also right-click the entity with a valid IP to *Search Events*, *View/Create Annotations*, perform an *Entity Lookup* and *Global Search*, or open a *Playbook*.



09 September 2024 version 2024.8.1

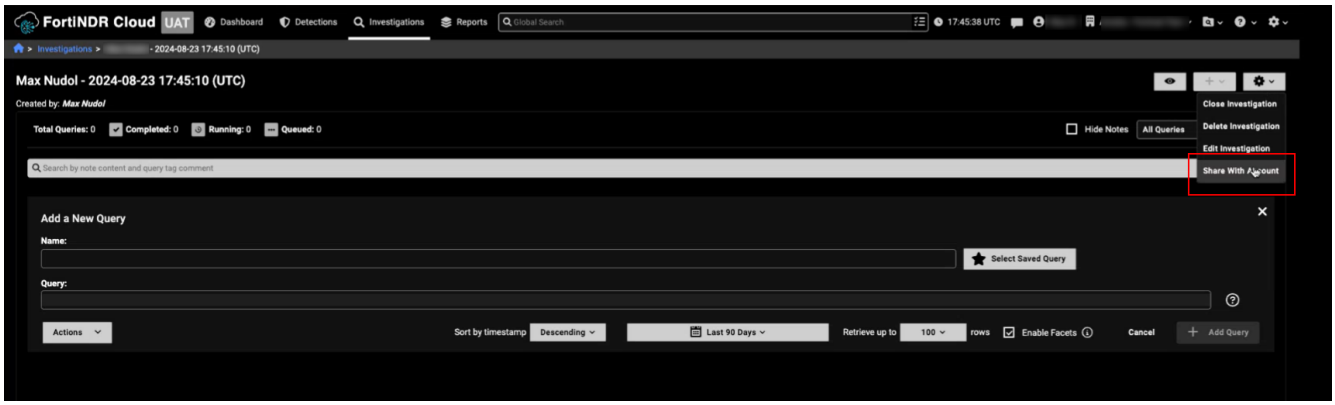
FortiNDR Cloud version 2024.8.1 includes bug fixes, but no new features. See, Resolved issues on page 65.

28 August 2024 version 2024.8.0

New functionality

Share investigations

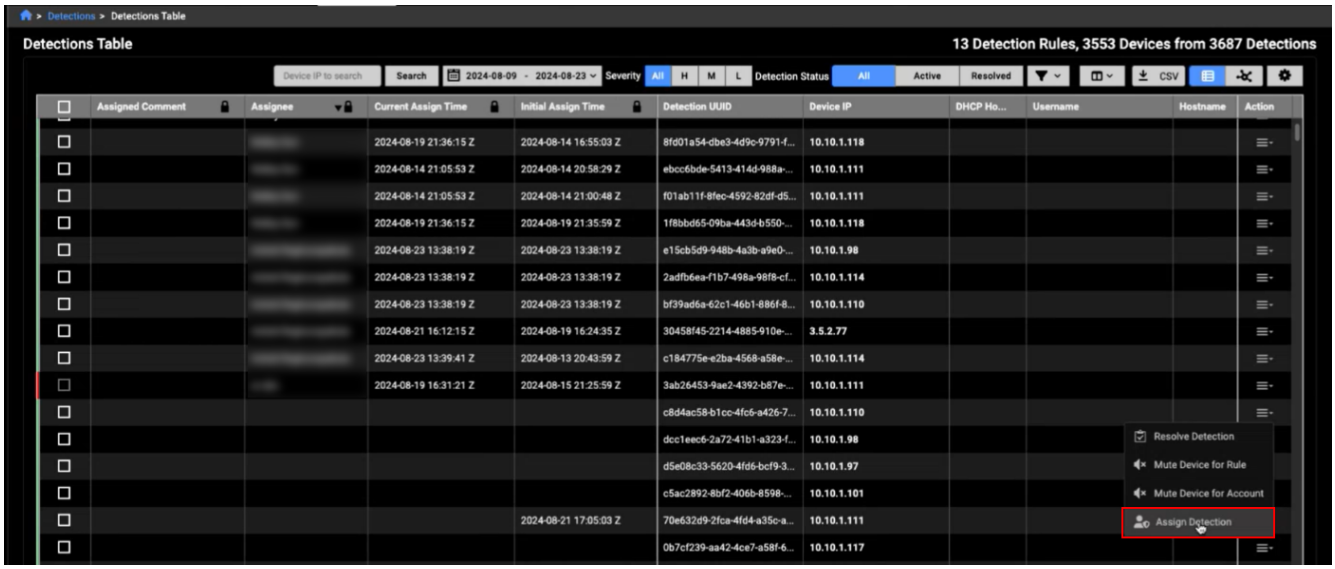
Users with multiple accounts can share investigations in their primary account with users in their secondary account. Sharing an investigation will allow all users with access to the secondary account to see and make changes to the investigation. Once the investigation is shared, it cannot be undone. For more information, see Share investigations.



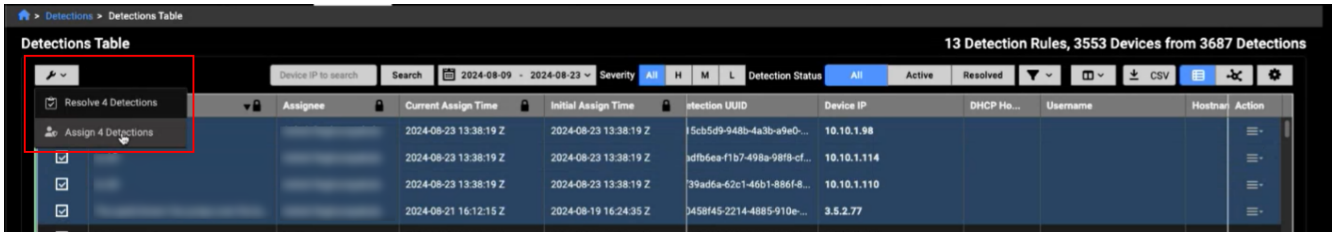
Detection assignment

You can now assign active detections to a user from the *Detections Table*, *Triage Device*, and the *Triage Rules* page. For more information, see Assigning detections.

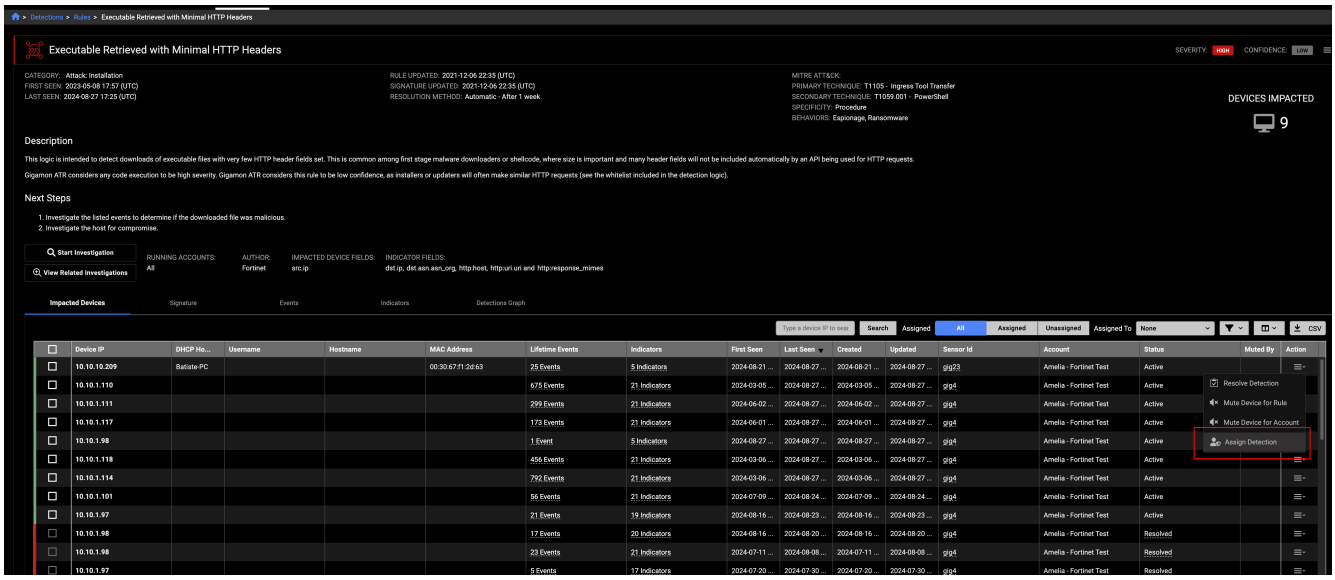
To assign a detection to a user from the *Detections Table*, click the actions menu and select *Assign Detection*.



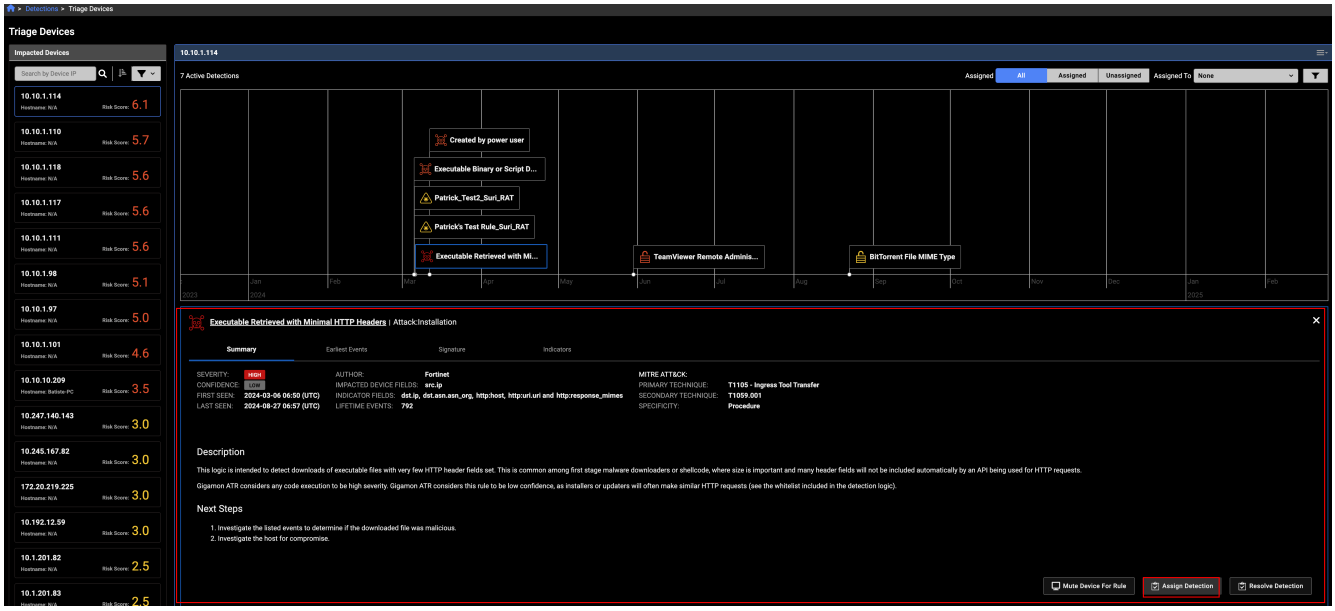
You can bulk assign and unassign detections from the tools menu at the top-left of the table.



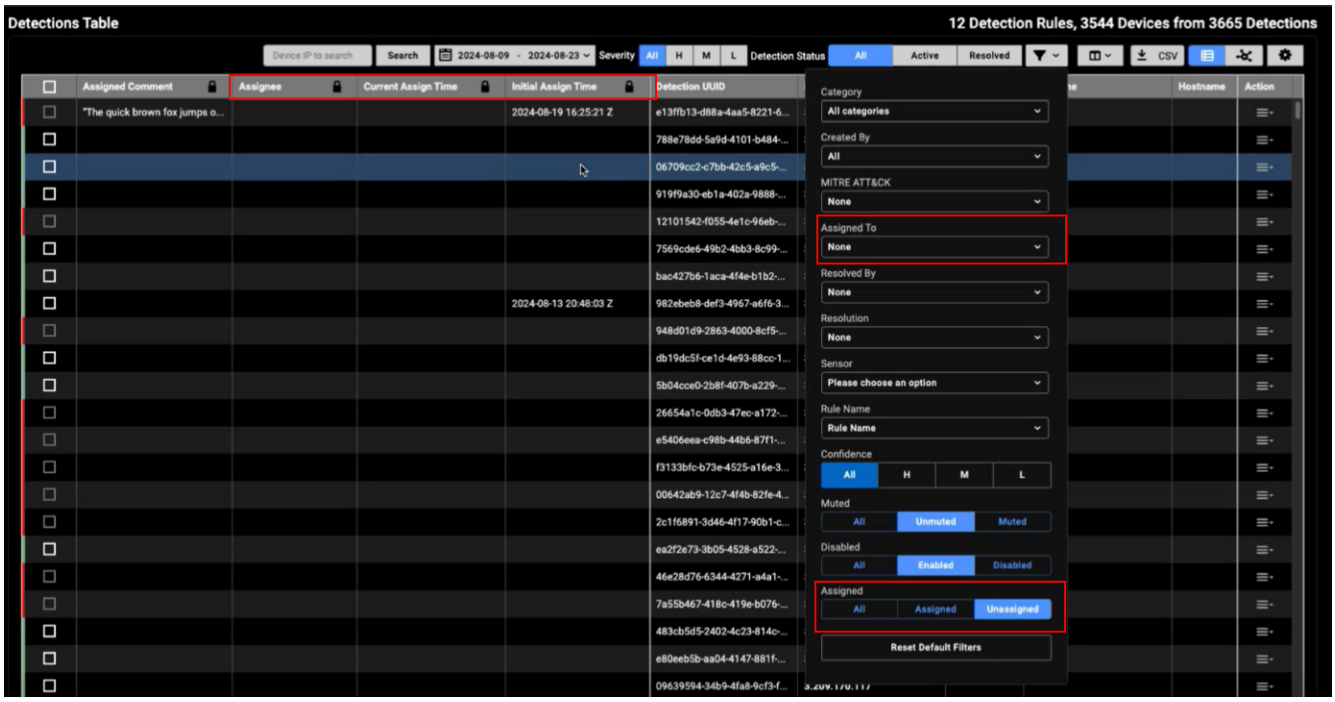
You can also assign a detection from the actions menu in the *Triage Rules* page.



Similarly, you can assign a detection from a rule in the events table in the *Triage Device* page. Select an impacted device, and then select a rule and click the *Assign Detection* button.



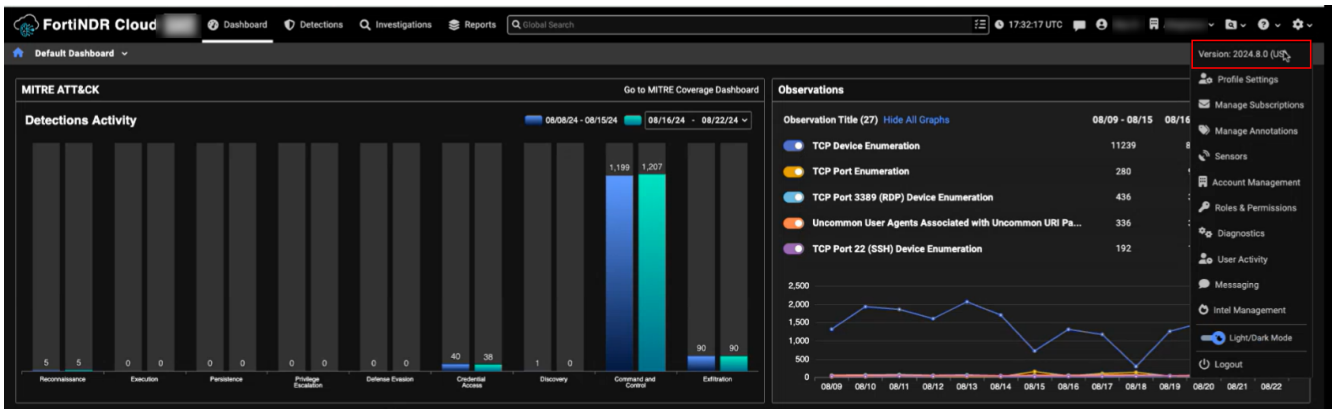
The following new columns were added to the *Detections Table* : *Assigned Comment*, *Assignee*, *Current Assign Time*, and *Initial Assign time*. An *Assigned* / *Unassigned* value was also added to the table filter. You can filter the table based on the user the detection was assigned to.



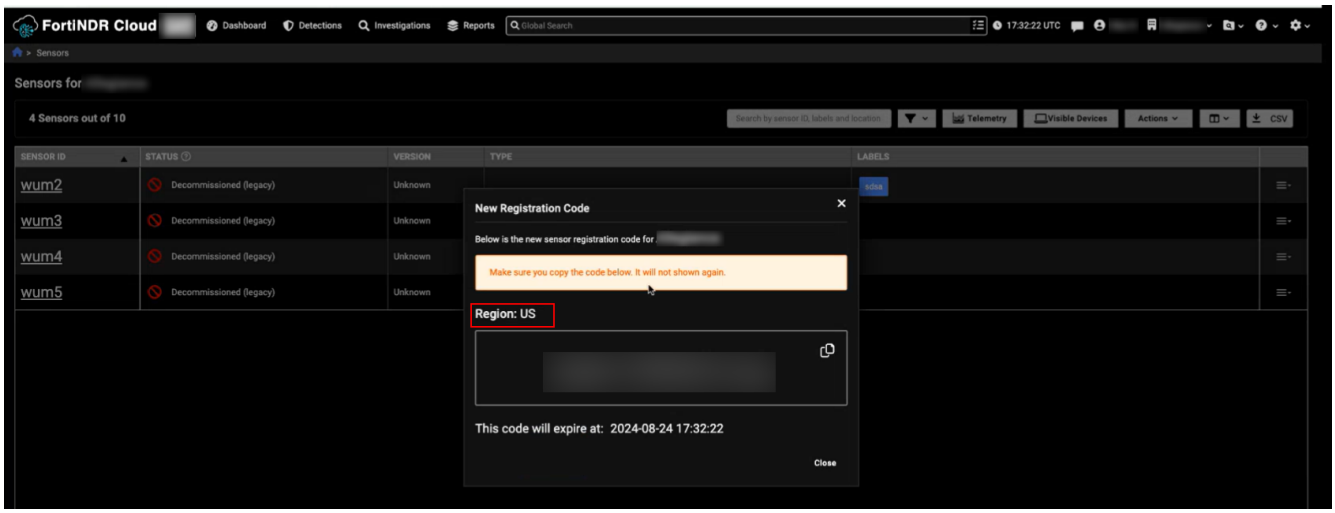
Improved functionality

Account region

The account region now appears at the top of the settings menu and sensor provisioning page.

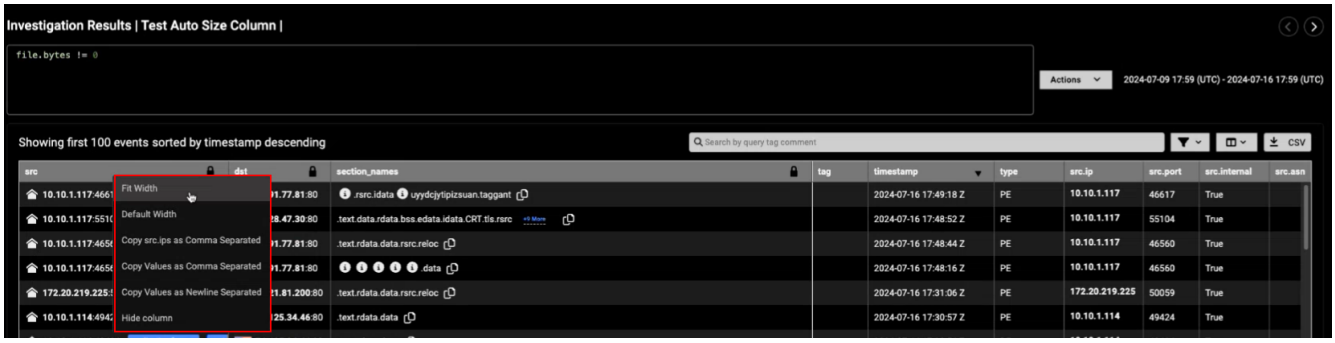


The region can be either *US* or *EU*.



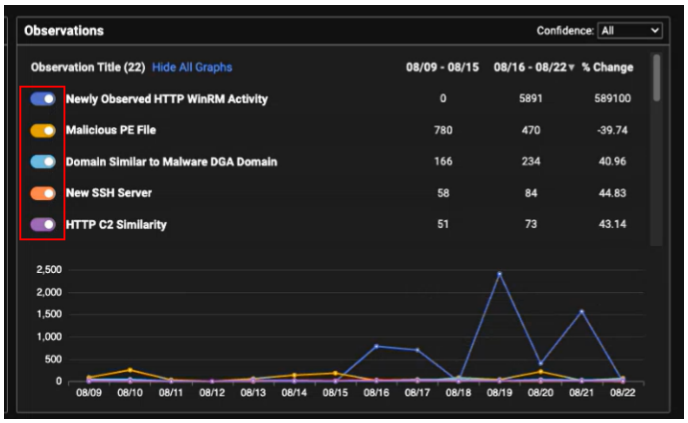
Events table

When you show all columns in the *Events* table, you now have the option to quickly adjust the column width to the widest cell in the table. To adjust the column width, right-click the column header and select either *Fit Width* or *Default Width*.



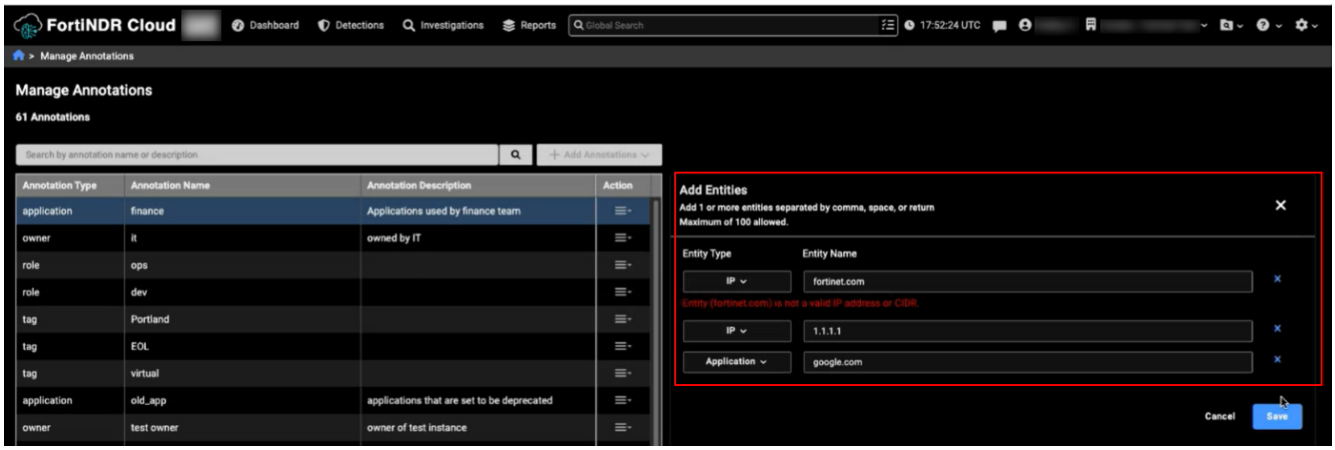
Observations widget

The *Observations* widget in the default dashboard has been enhanced to make it easier to filter and view observations. The filter toggles have been enlarged to make them easier to see and click. The widget also displays all the observations. The total number of observations is displayed at the top of the widget and a scroll bar has been added to scroll through the list. You can also *Hide All Graphs* and toggle the graphs you want to see.

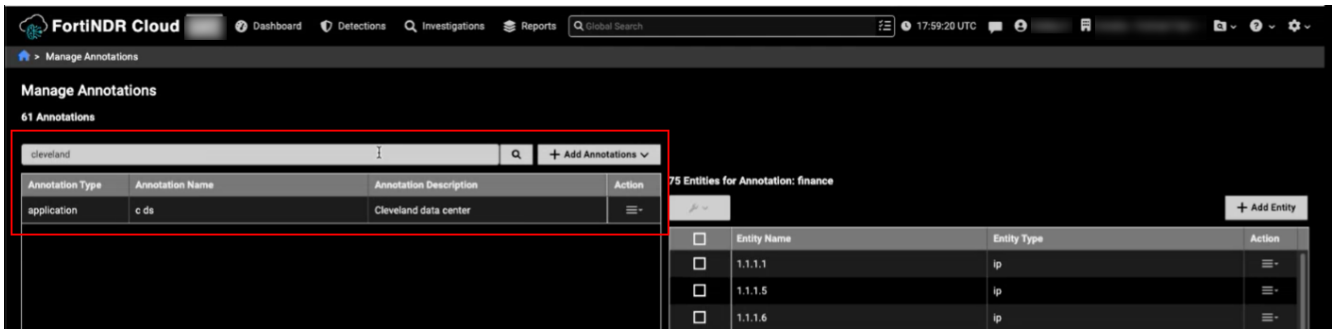


Manage Annotations

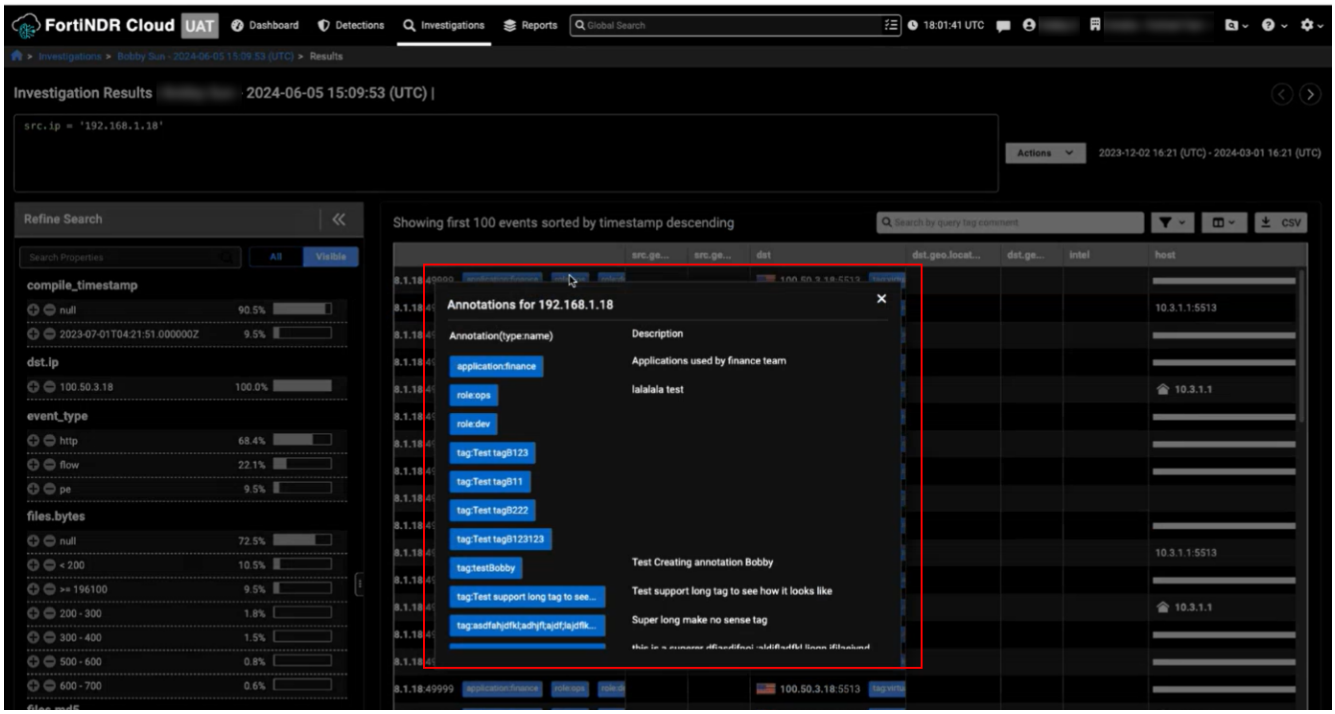
The tables in the *Manage Annotations* page have been enhanced. When you add entities, FortiNDR Cloud will validate the field when you click *Save*.



The search function has also been improved to support searching any text in the *Annotation Name* and *Annotation Description* columns. In previous versions, search was limited to an exact match of the annotation name.

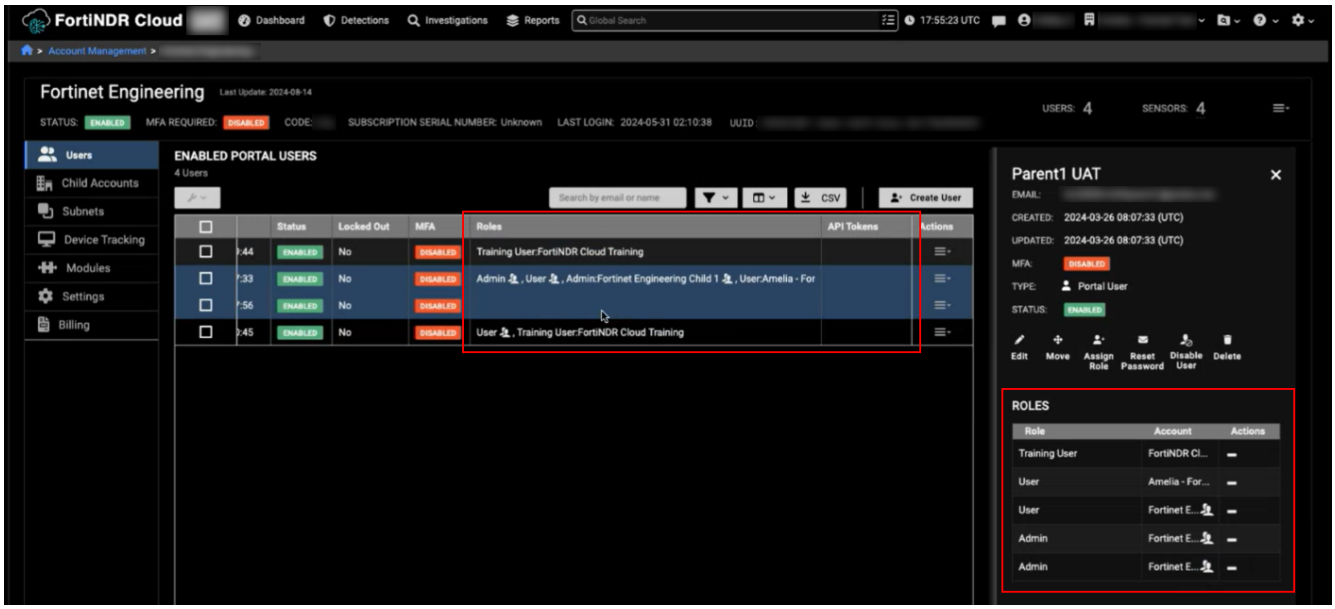


When you hover over an annotation in the Event table, it will show a tooltip with the annotation name and description. When you click the annotation, all the annotation details are displayed in a pop-up window.



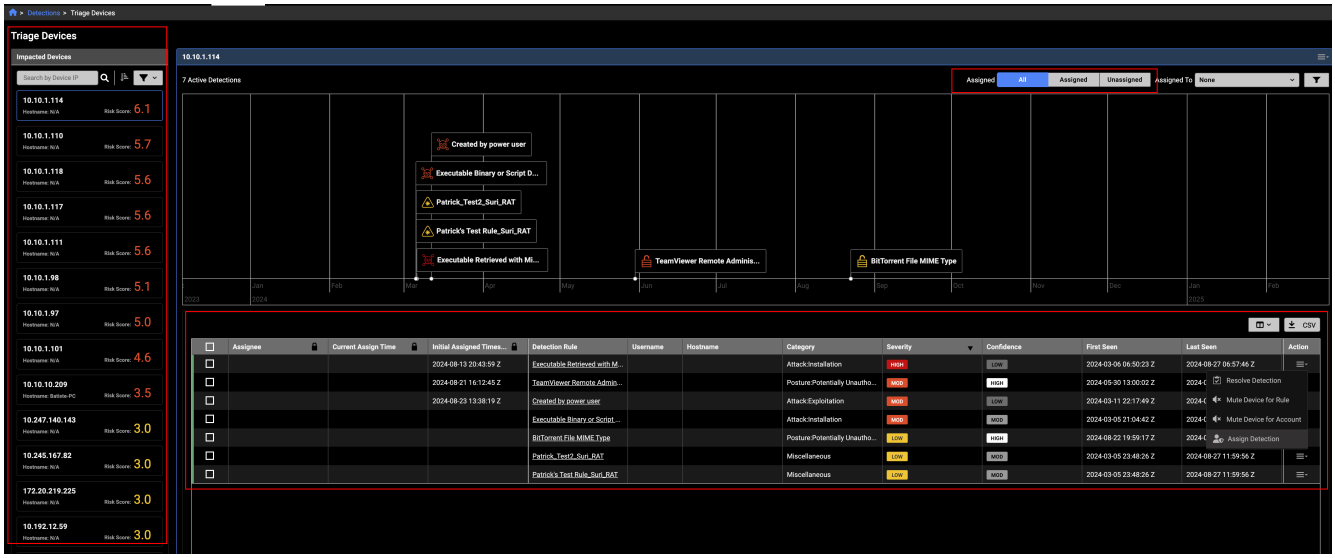
User management

The *Roles* column in the *Users* page, now mirrors the roles and icons in the user details pane. When you download the table as a CSV file, the roles are assigned a column for each role.

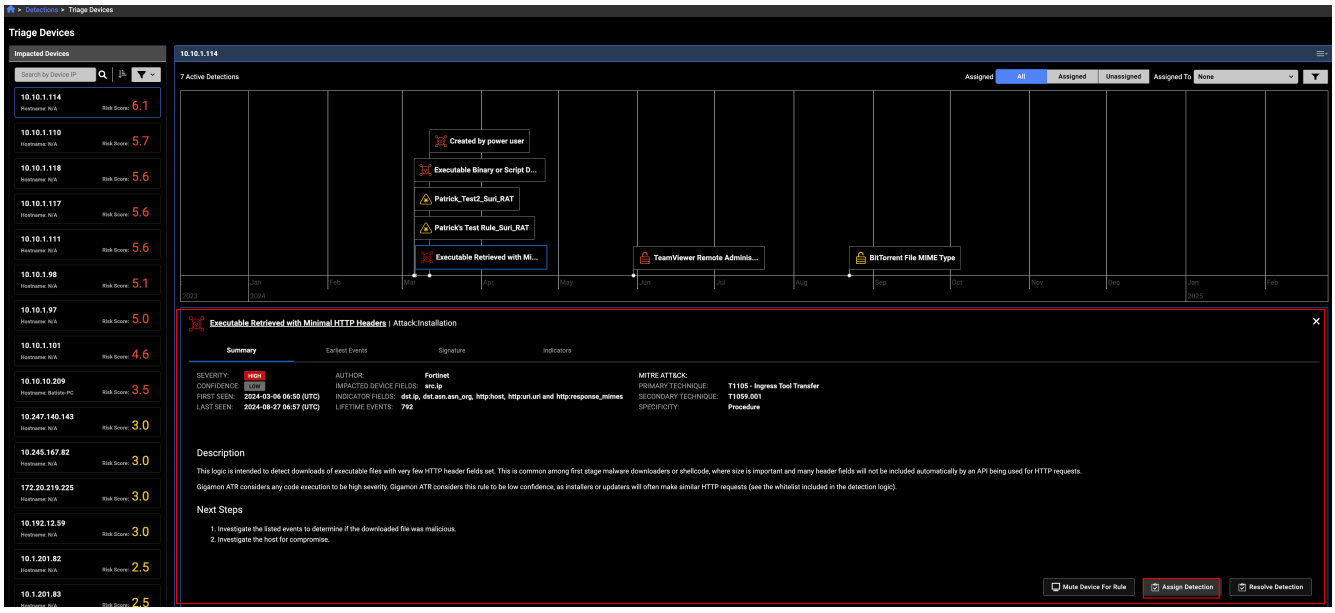


Triage devices

The *Triage Devices* page has been improved, with a scrollable *Impacted Devices* panel at the left side of the page. The device detections table at the bottom of the page has also been replaced with a new scrollable table. All of the filters have been moved to the top of the page.



When you click the link in the *Detection Rule* column the rule details are displayed. and assign a detection. You can use the pane to assign a detection to a user.



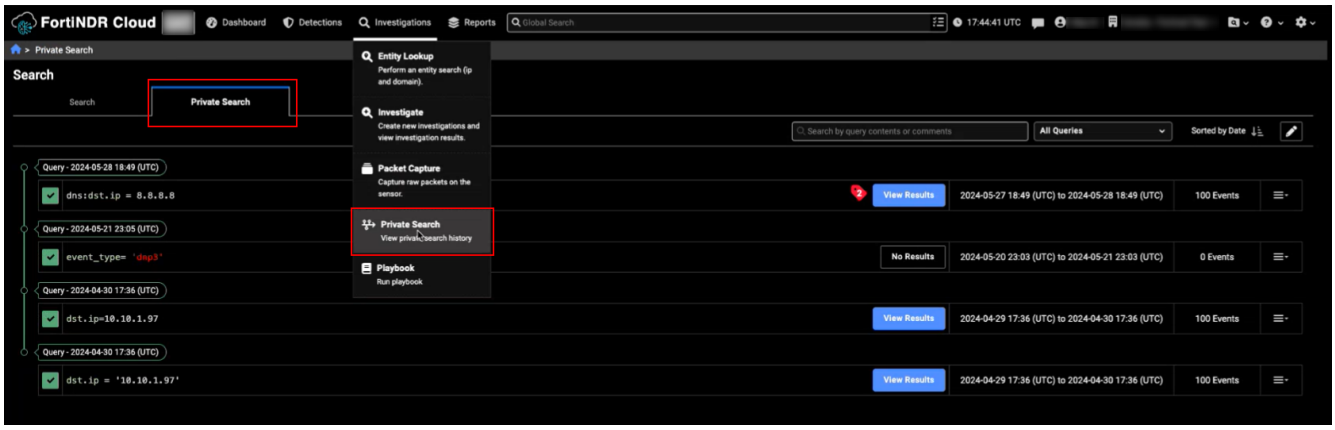
Other improvements

Detections table

The can now use any column header in the *Detections Table* to sort the detections. This enhancement is only available in the Detections Table.

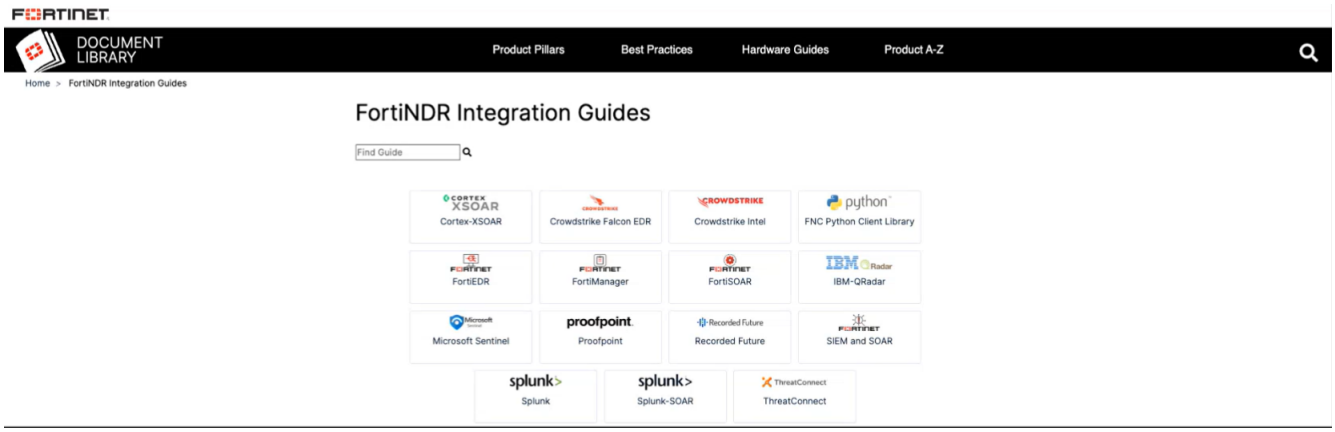
Search Timeline

The *Search Timeline* feature has been renamed *Private Search*.

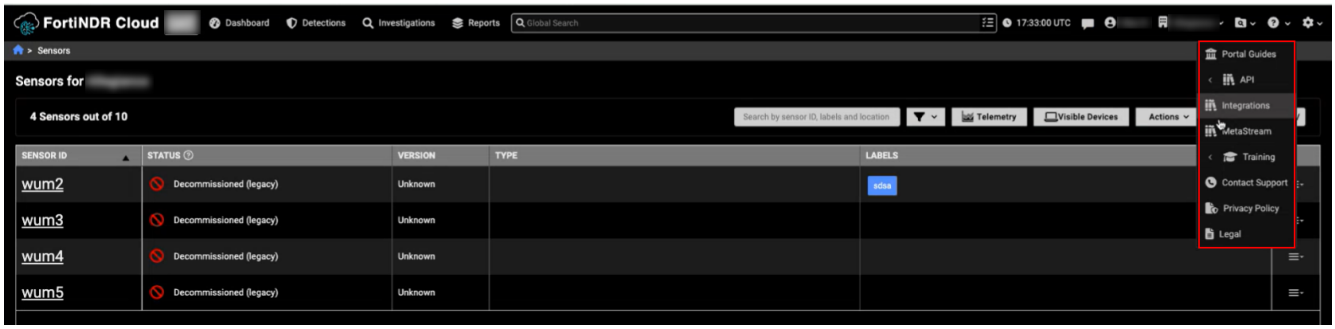


Integrations guides

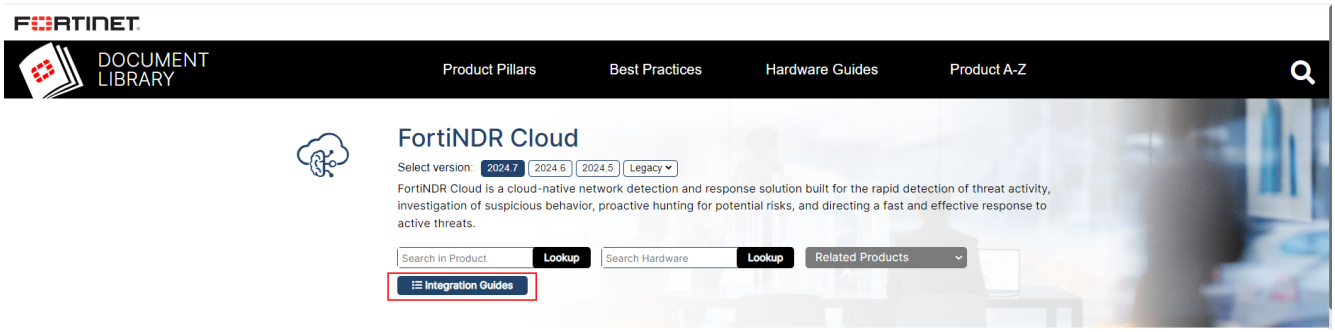
The integrations guides have been consolidated onto a dedicated page.



To access the page, in the Portal, click *Portal Guides* > *Integrations*.



You can also access the page by clicking the *Integration Guides* button in the Fortinet Document Library.

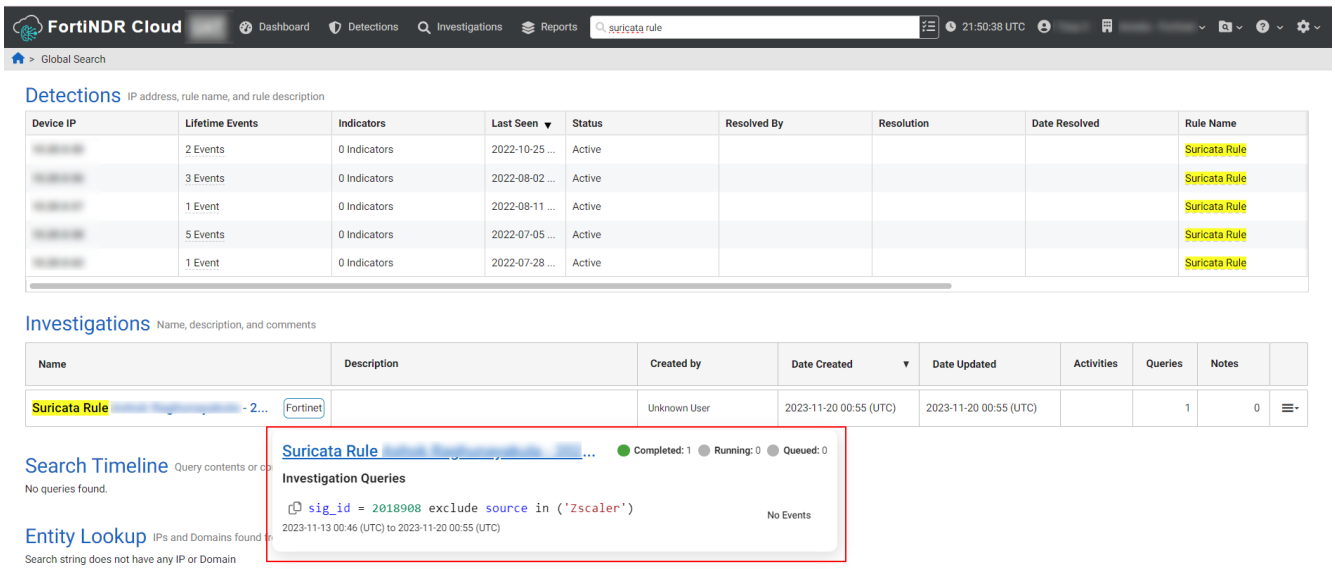


31 July 2024 version 2024.7.0

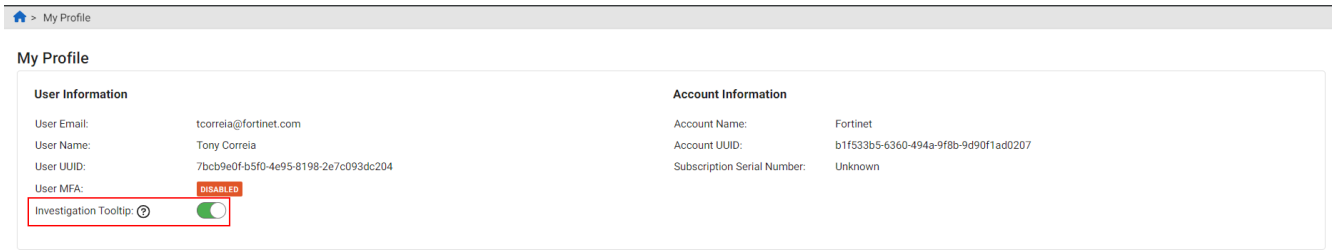
Improved functionality

Investigation tooltip

An investigation tooltip has been added to the *Investigations* widget in the default dashboard, the *Investigations* page, and the search results in global search.



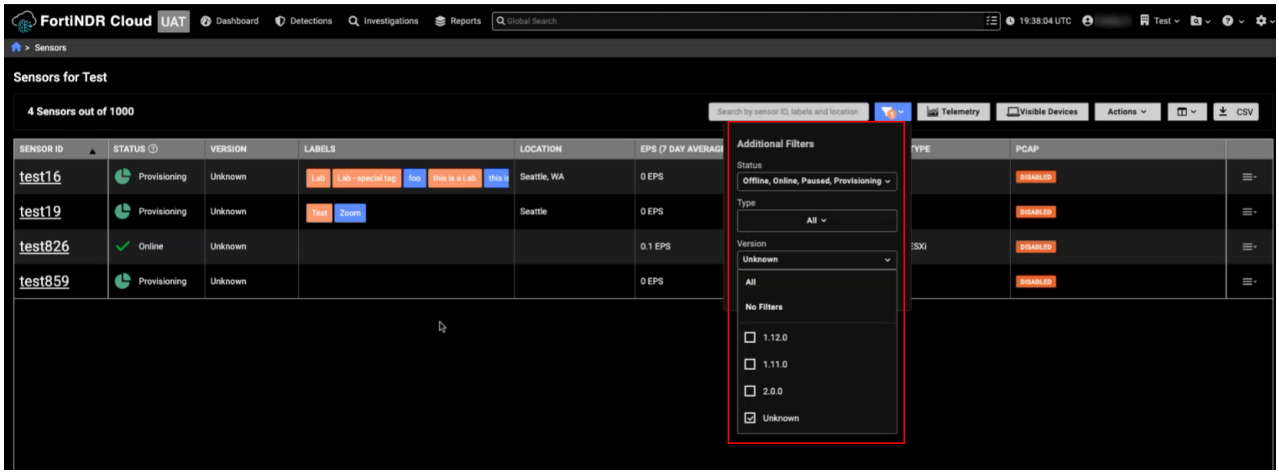
You can also disable the investigation tooltip from the *Profile Settings* page.



Sensors

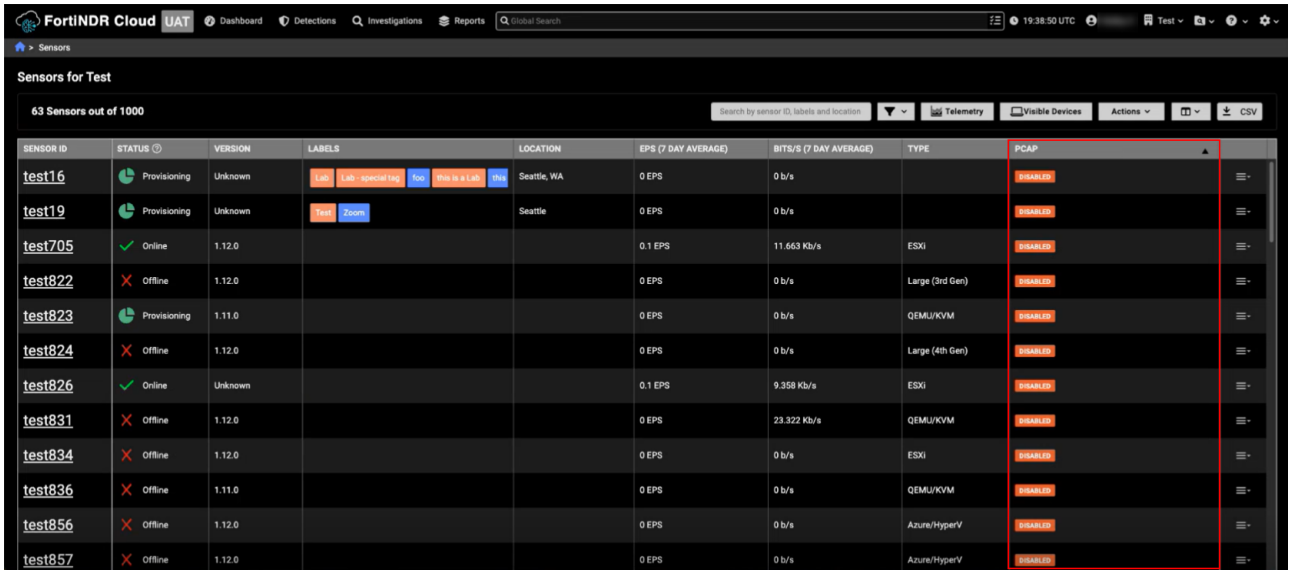
Filter by sensor version

A new filter was added to the *Sensors* page allowing you to filter by the sensor version.



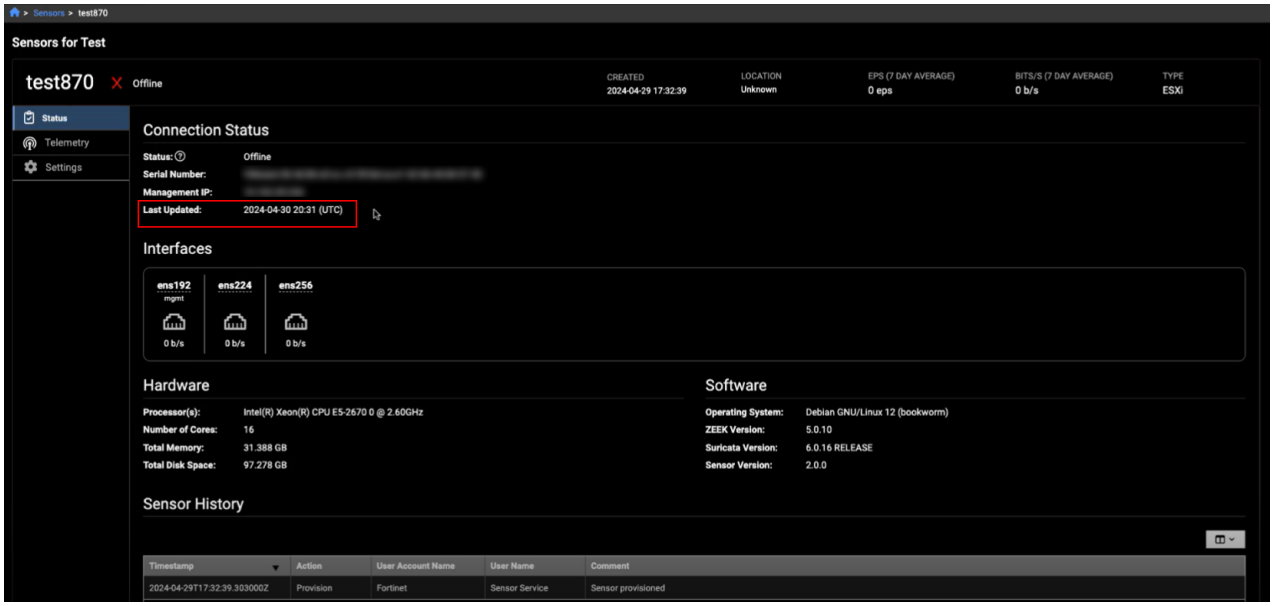
PCAP column

A sortable *PCAP* column was added to the *Sensors* page indicating if *Packet Capture* is enabled or disabled.



Sensor last update

A *Last Updated* field was added to the sensor detail page.

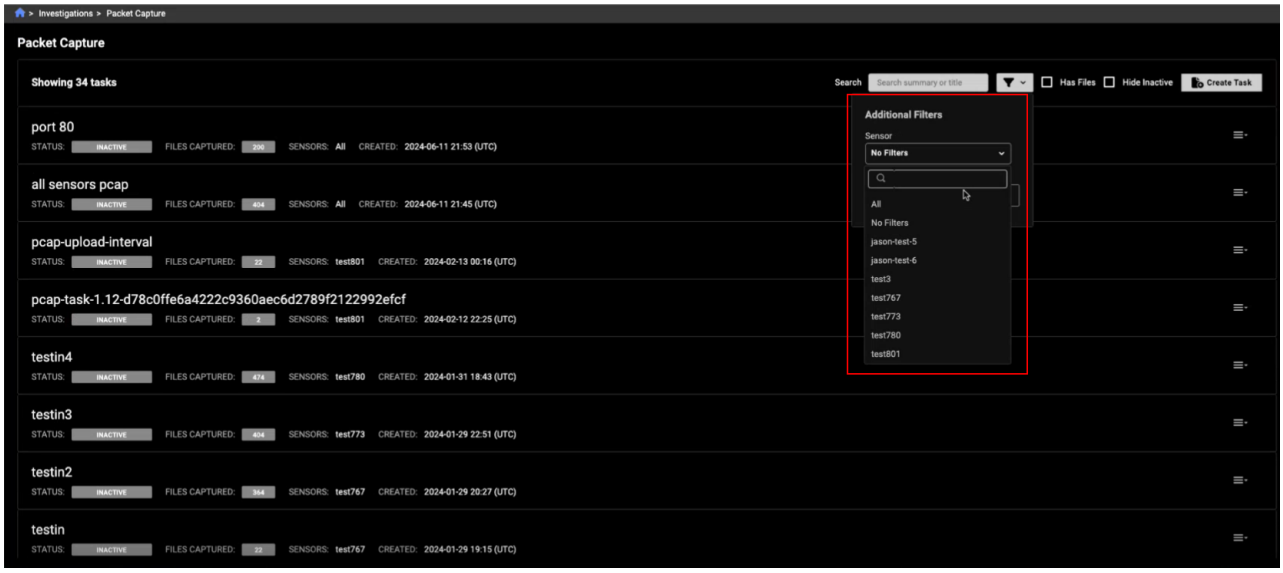


Investigations

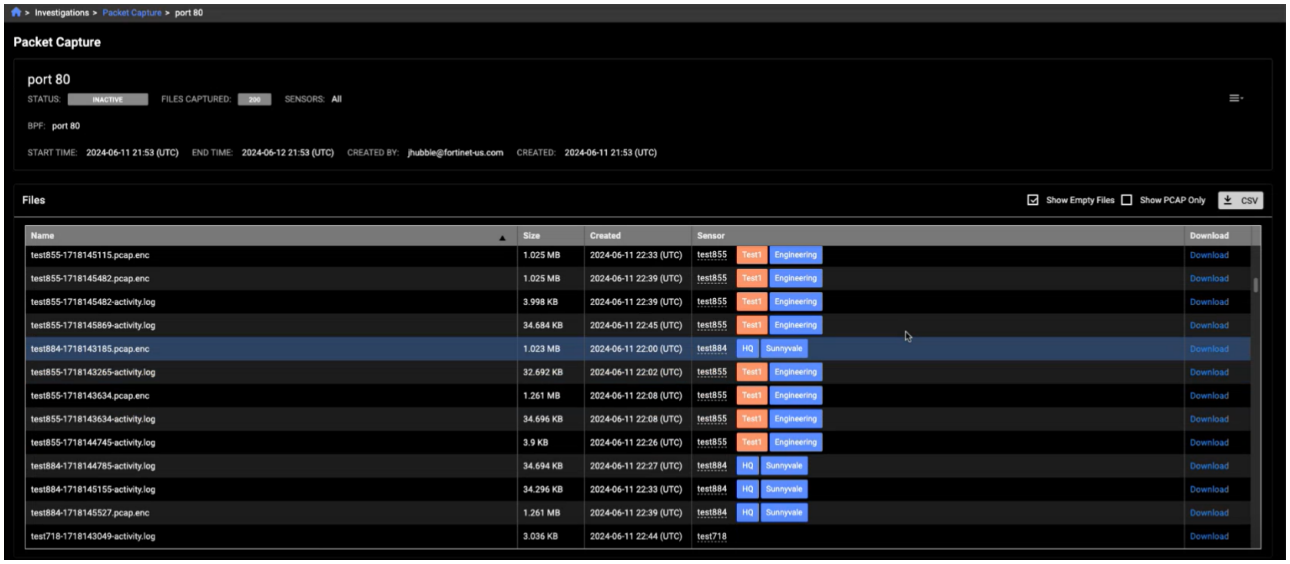
Packet Capture page

The *Investigations* > *Packet Capture* page has been updated.

The sensor filter only shows the sensors that have PCAPs configured. That is, the PCAPs where that sensor is configured and any PCAP that has files from that sensor are shown. If there are any All PCAPs configured, *All* can be selected. By default, *No Filters* is selected.



In the *Files* section, a sortable *Sensor* column that lists the sensor IDs was added. The files table is also now scrollable, instead of paginated.



Other improvements

Metastream module

The *Metastream* module has been redesigned to align with the look and feel of the other integrations on the page. If there is an error while enabling the integration, an error will appear at the top of the page.

Custom Dashboards

Custom dashboards now support default names, allowing users to add a dashboard without a unique name.

GUI

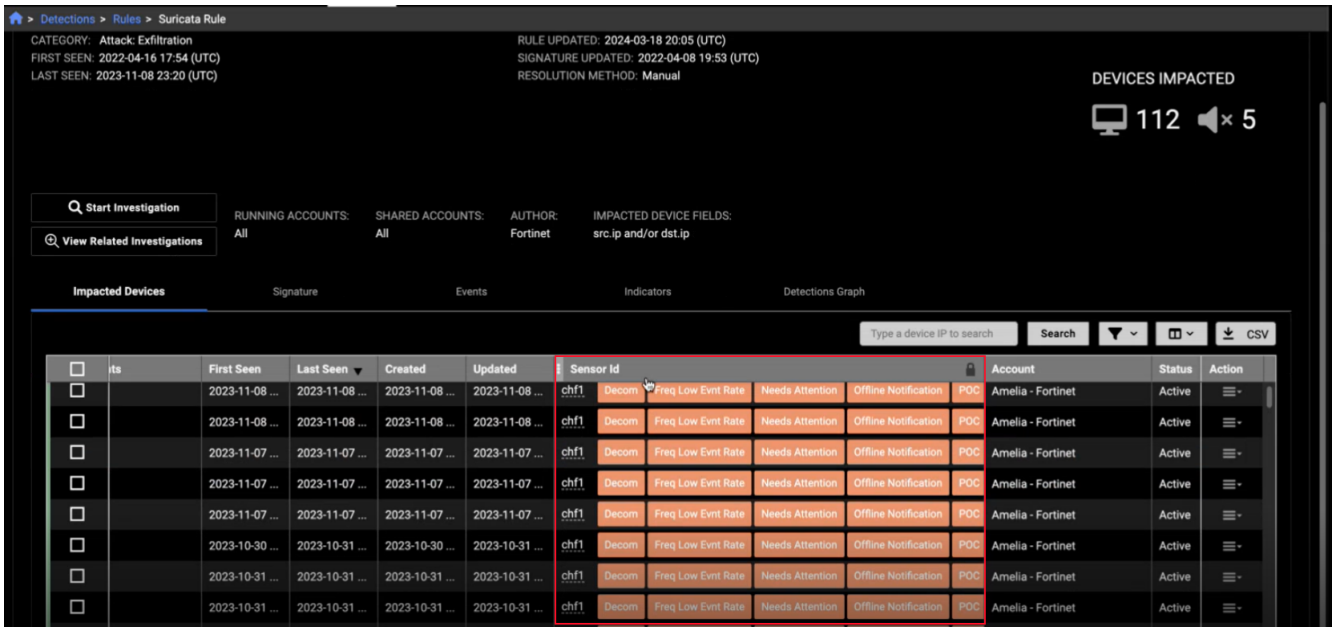
- The *Copy* button has been updated and standardized across the portal.
- A link to the CSV guidelines document has been added on the *Manage Annotations* page.
- In *Reports* > *Network Security Posture Report*, you can now click an event to start an investigation.

26 June 2024 version 2024.6.0

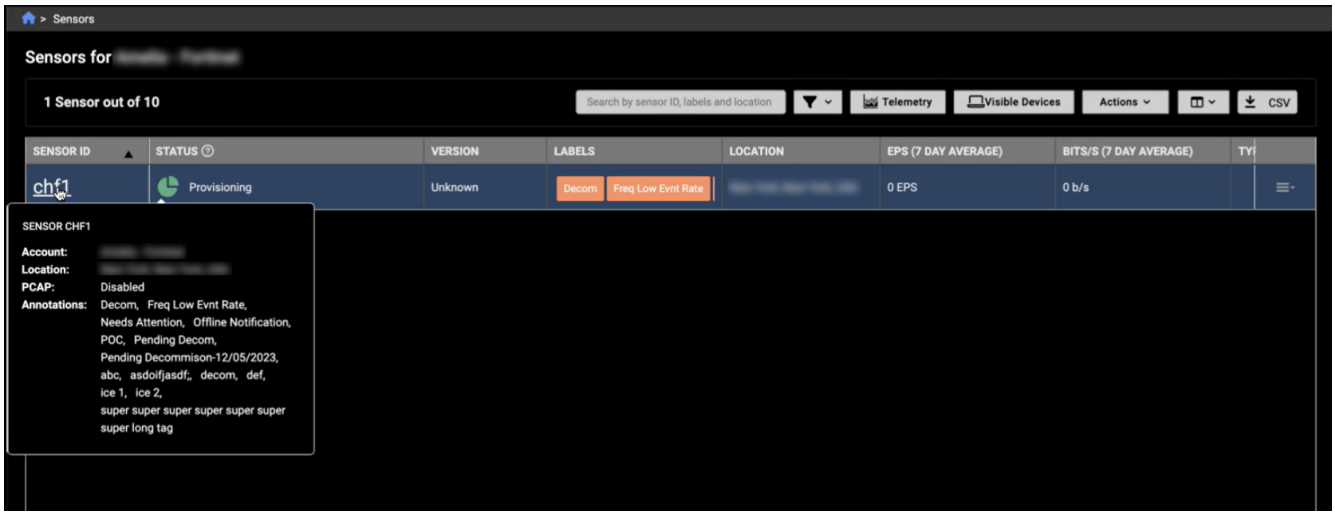
Improved functionality

Sensors

The *Sensor ID* column now displays all the tags within the column. You can also click the sensor ID to open the *Sensor Details* page. When you hover over the Sensor ID, a dialog displays all the annotations for the sensor. With the exception of the *Sensors* page, this change applies to all tables that have the *Sensor ID* column including *Search*, *Search Timeline* results page and the *Events* table.

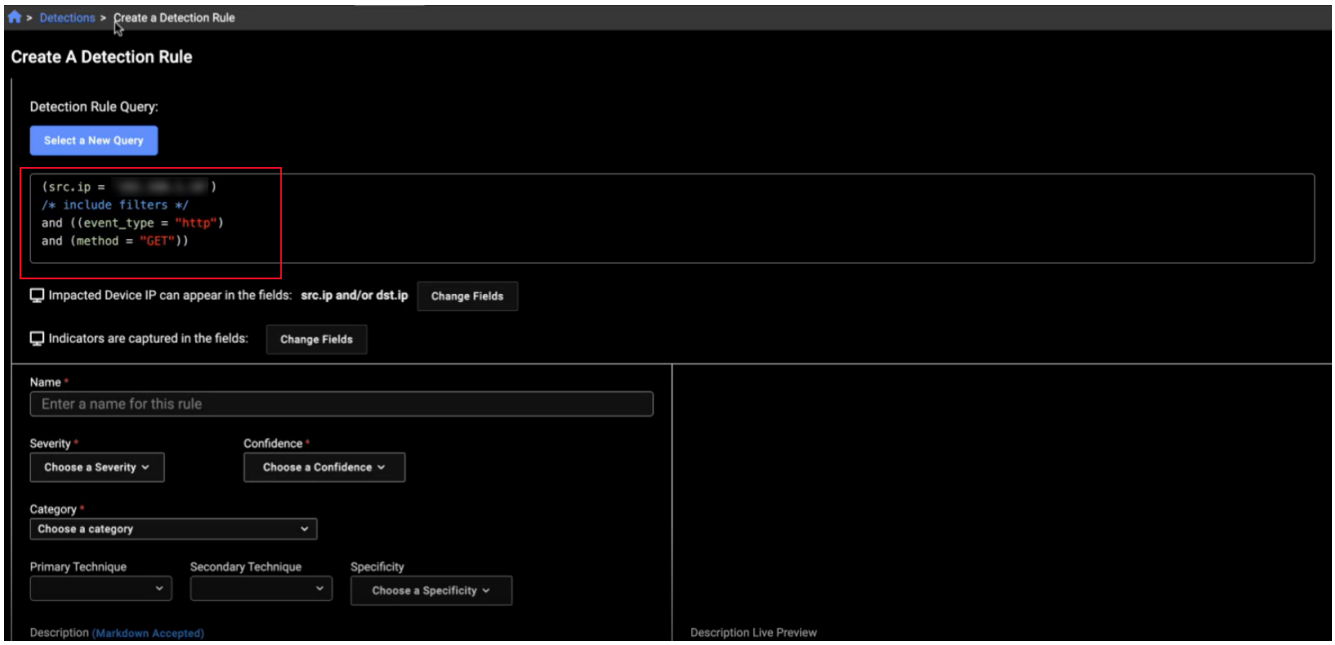


In the *Sensors* page, when you hover over the Sensor ID in the list, a dialog will display the sensor information.



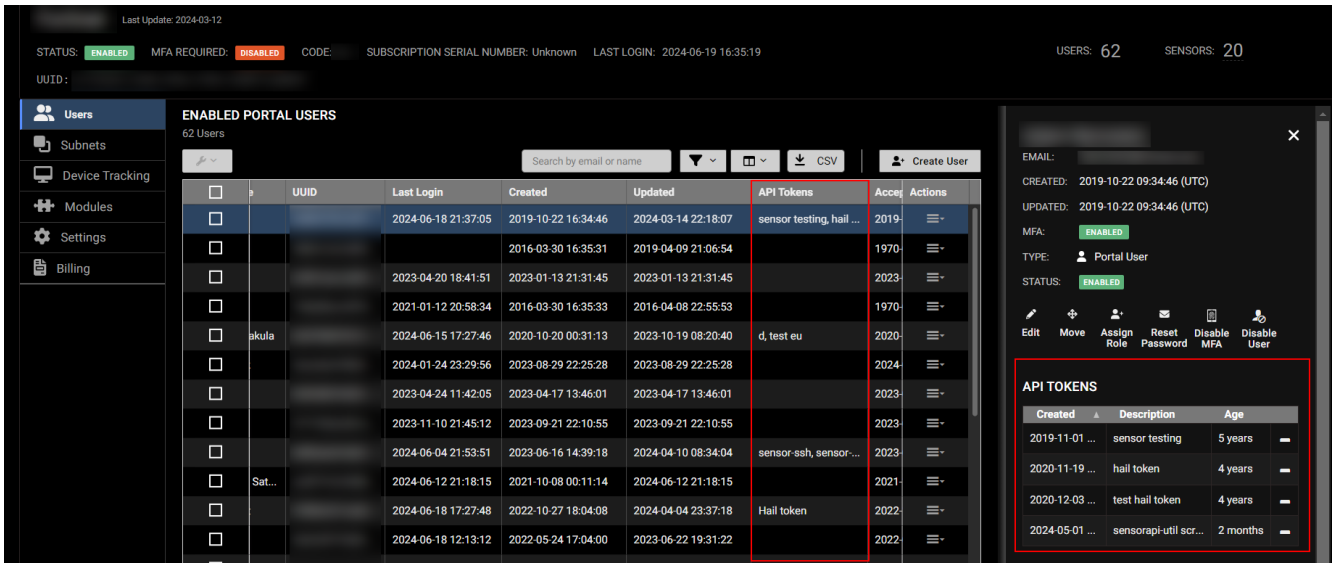
Create new detections

The facet filters are now included in the query field when you create a new detection from the results in the *Search Timeline* page. To try this out, open the *Search Timeline* page and locate an entry with results. Click the actions menu and select *Create Detection*. The facet filters are displayed in the query field.

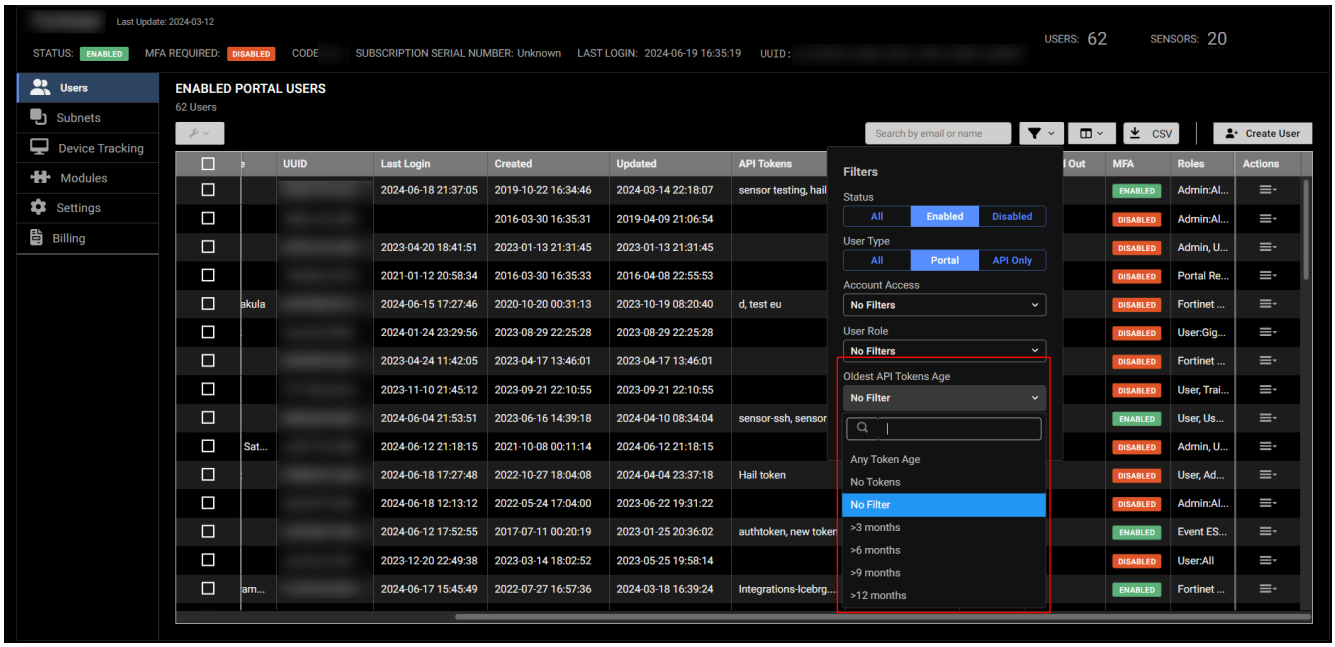


API tokens

The term *Permanent Tokens* has been replaced with *API Tokens*. An *API Tokens* column was also added to the *Users* tab in the *Account Management* page.



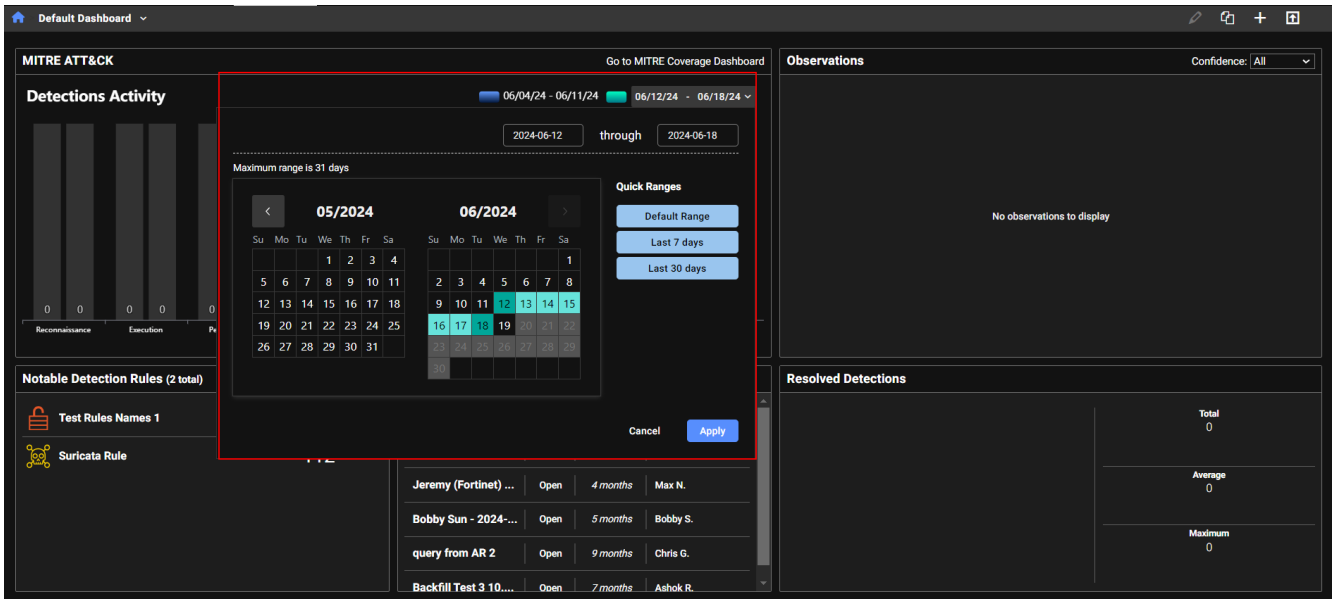
You can also use API tokens to filter the page.



Default dashboard

MITRE ATT&CK widget

A date-range picker was added to the *MITRE ATT&CK* widget in the default dashboard.



Observations widget

You can now filter the graph in the widget by clicking an observation title in the graph's legend.

Other improvements

Detections Rules tab

The *Detections Rules* page no longer displays rules that have never been triggered when you filter the page by *All*. Pagination has also been removed from the page to make it easier to scroll through the results. This change also applies to the detail wheel.

Packet Capture

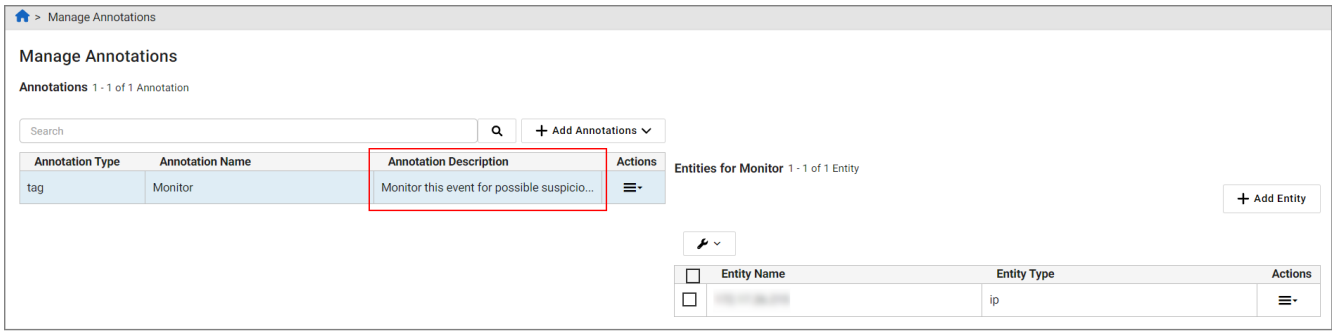
We have removed the option to select the number of rows to view on the page. The page now shows all the tasks on a scrollable page.

29 May 2024 version 2024.5.0

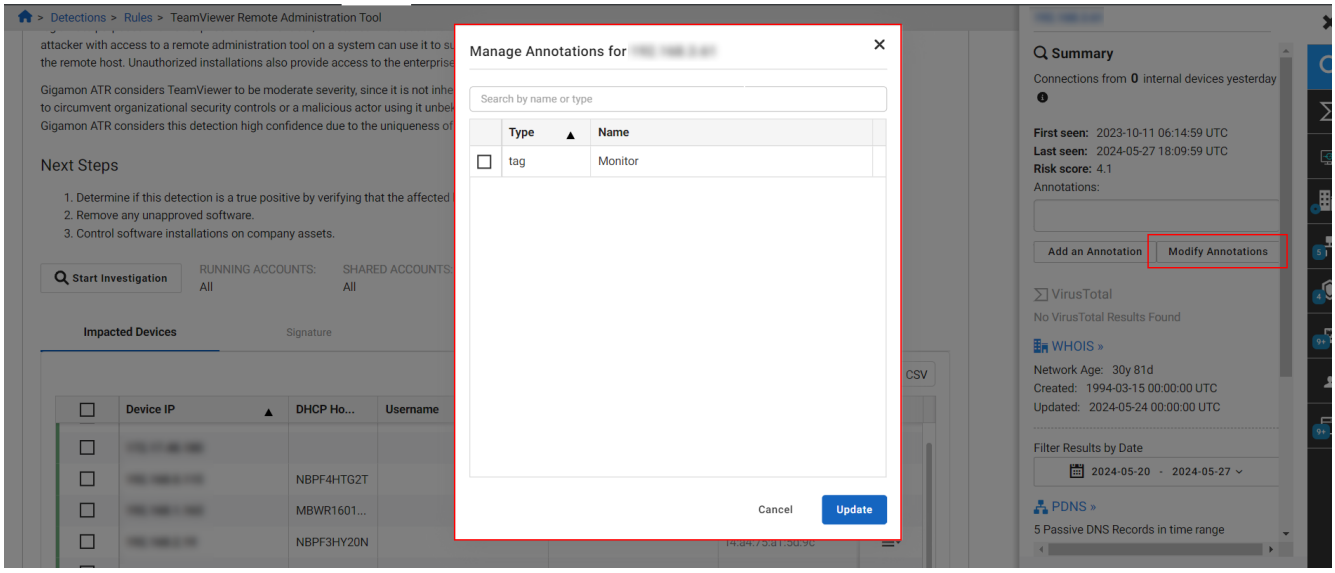
Improved functionality

Manage annotations

A new *Annotations Description* column was added to the *Manage Annotations* page.

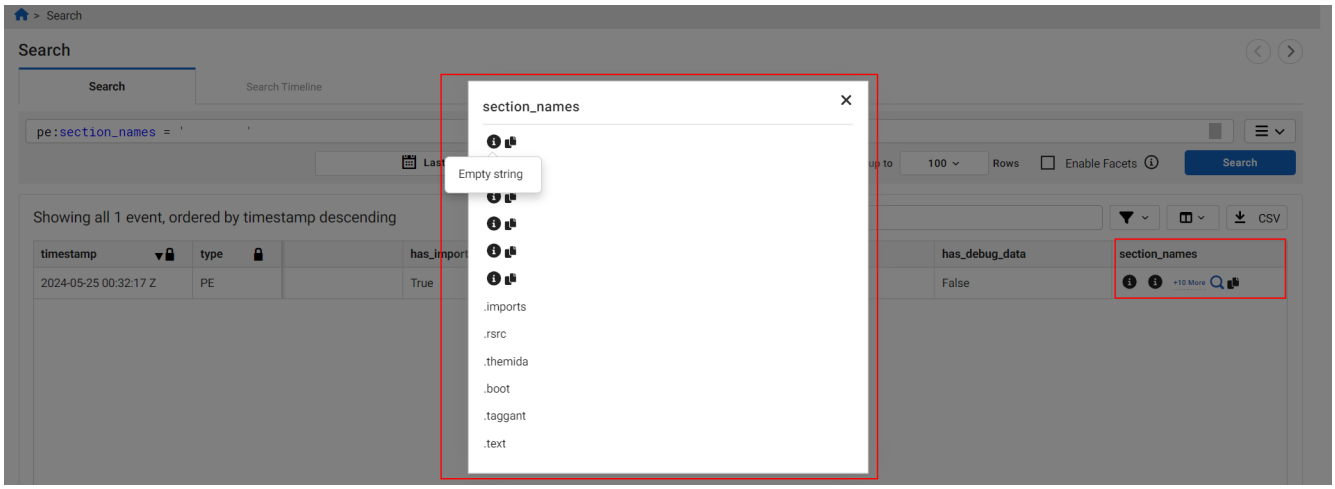


In the *Entity Panel*, the *Manage Annotations* button has been renamed *Modify Annotations* and the GUI was improved so you can search for and quickly add or remove annotations.



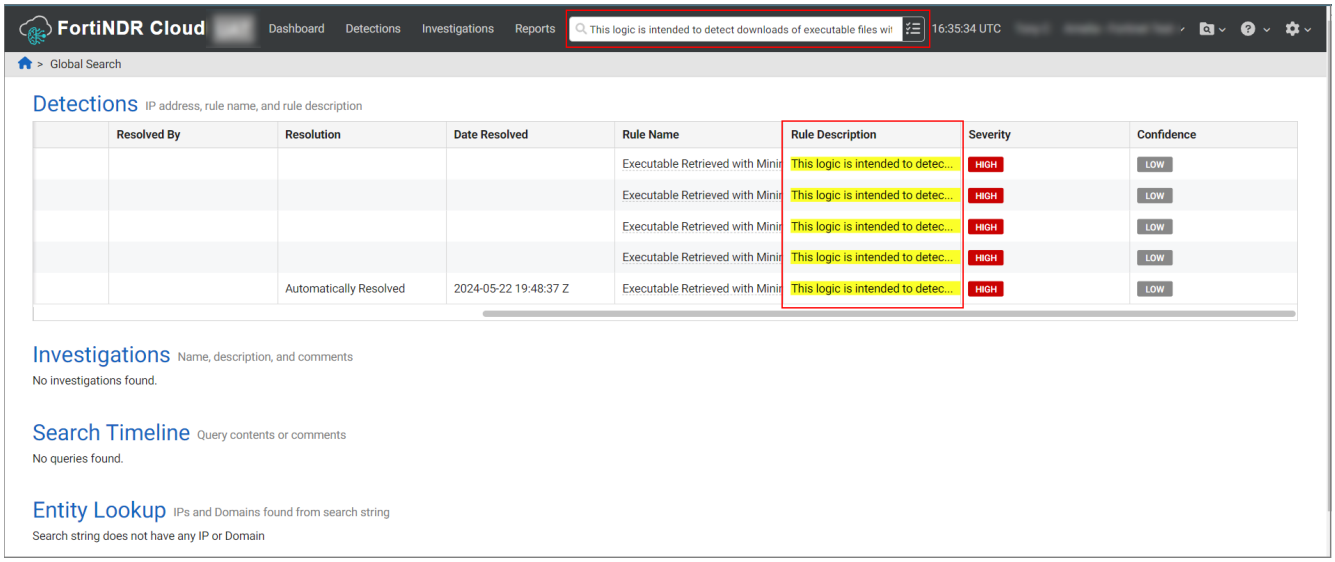
Search timeline

New icons have been added to the *section_names* column to add explanation and functionality to the data. Hover over the information icon to view the number of empty strings and spaces . Use the copy icon to copy the information. You can also click the link to view the values and icons in a dialog box.



Global Search

Global search now supports search Rule descriptions. Copy and paste text from Rule description into the search field. Search results will be highlighted in the *Rule Description* column of the in the *Detections* section. A highlight was also added to the *Device IP* column when you search by IP.



Other improvements

Queries

- The dashboard and report queries have been improved to make them faster.
- You can now query *dnp3*, *dnp3_control*, and *dnp3_object* event types in an investigation.

Investigations

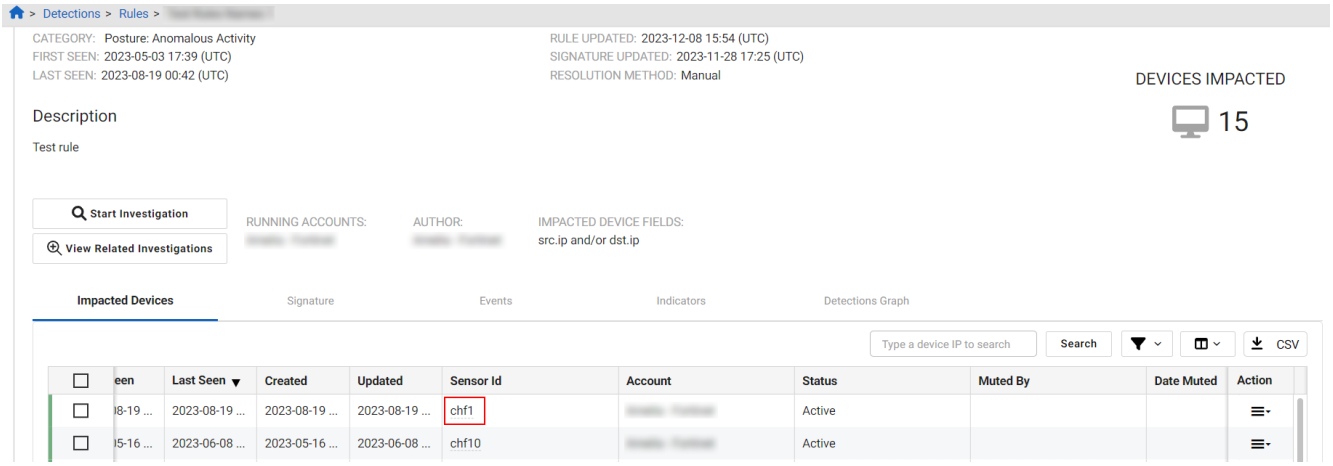
The *scrc* column in the *Events* tab now displays the annotation names (as opposed to the number of annotations).

15 May 2024 version 2024.4.1

Improved functionality

Navigation improvements

You can now pivot to the *Sensor Details* page from the *Sensor ID* column in the *Rules Details*. Go to *Detections* > *Triage Rules* and open a rule. Click a sensor in the *Sensor ID* column. If the sensor is available, the *Sensor Details* page opens.

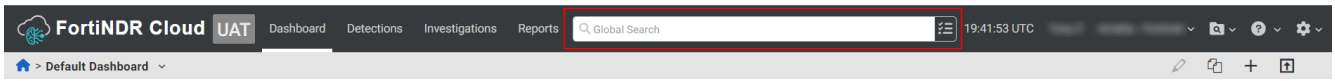


01 May 2024 version 2024.4.0

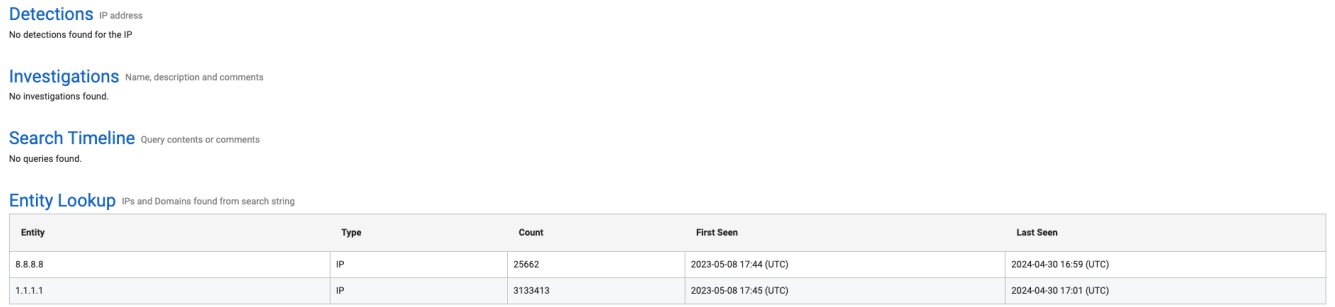
New functionality

Global search

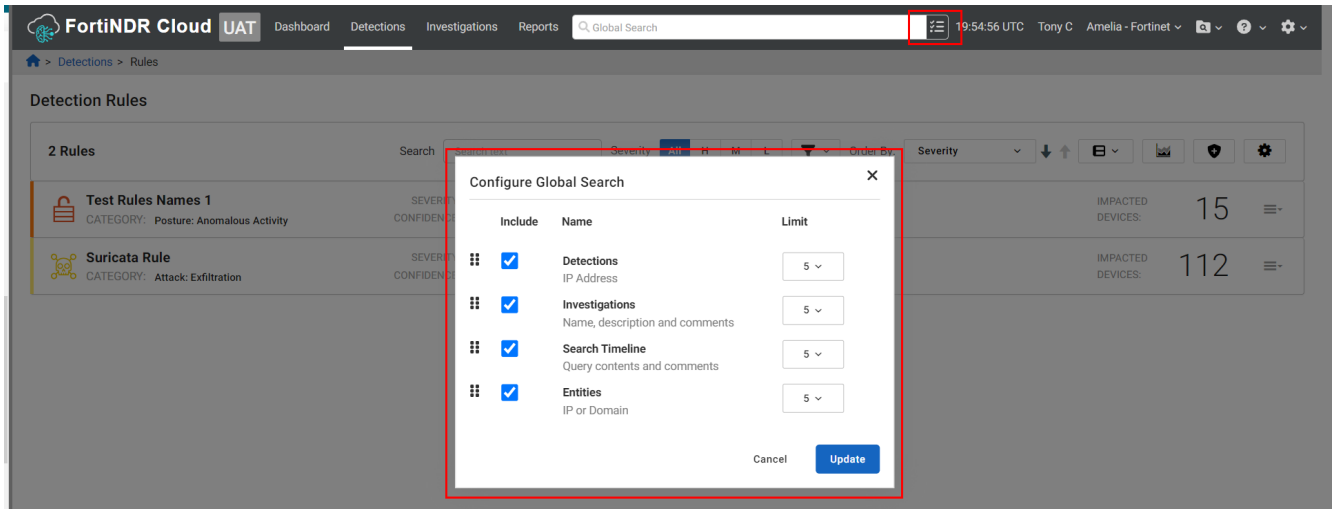
A new Global Search function was added to the navigation banner allowing you to search FortiNDR Cloud with a text string, IP address or domain. You can enter multiple IPs and domains separated by a comma or space.



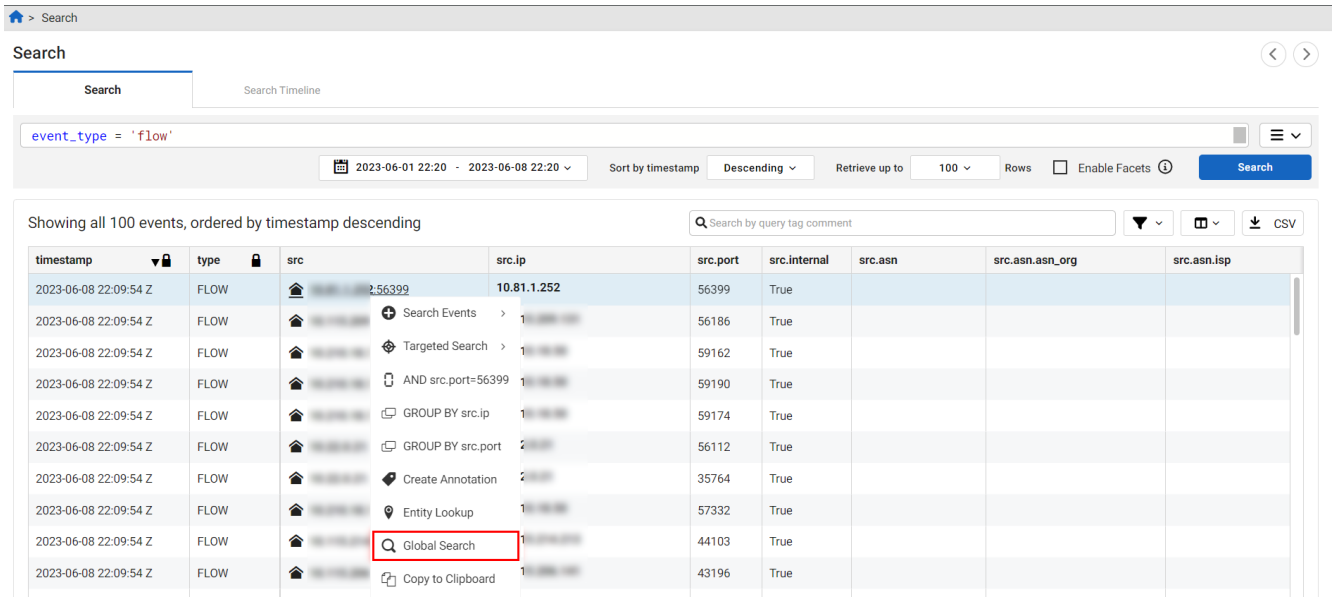
The search results are organized by *Detections*, *Investigations*, *Search Tmeline* and *Entity Lookup*. Global Search does not support searching Rules at this time.



You can configure how the results are displayed by clicking the menu next to the search field. You can show or hide a category, limit the number of results, or arrange the order they appear in the page.

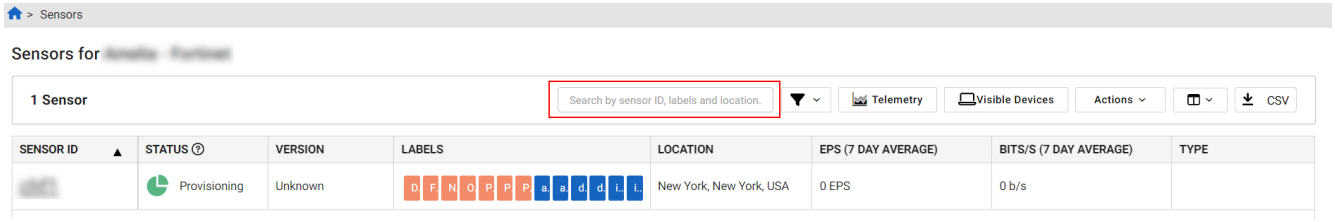


You can also access Global Search when you right-click a *scr* IP.



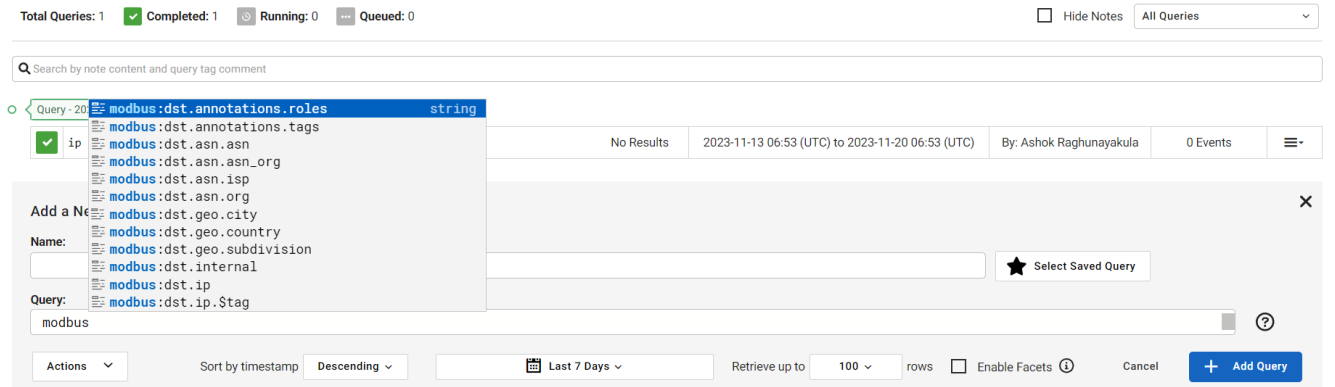
Sensor lookup

A new search function was added to the *Sensors* page allowing you to search the page by *Sensor ID*, *Labels* and *Location*.



Modbus events

You can now query Modbus events in an investigation.



Other improvements

- You can now open and close the date picker by clicking the date-range button. The date picker is responsive so the dates are visible regardless of its position on the screen.
- The subscription serial number is displayed in the *My Profile* page. If the serial number is not displayed, you will see a tooltip informing you the SN is available from your account representative. You can also update the serial number in the *Update account* dialog.
- A banner is displayed when your account is set to expire in less than 90 days.

10 April 2024 version 2024.3.1

Improved functionality

Detections table

A new *Created by* column was added to the *Detections table*.

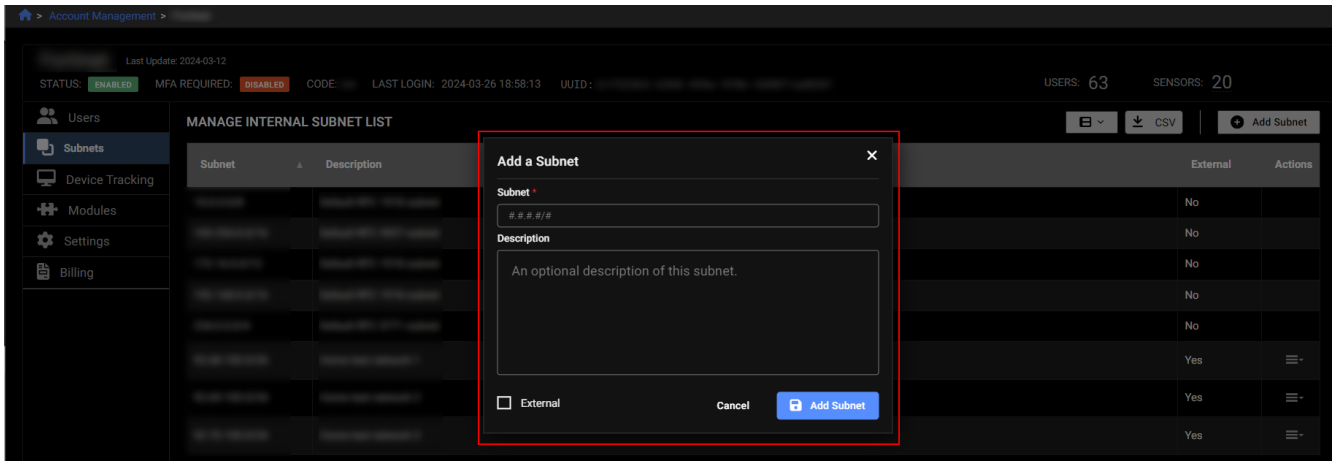
27 March 2024 version 2024.3.0

New Functionality

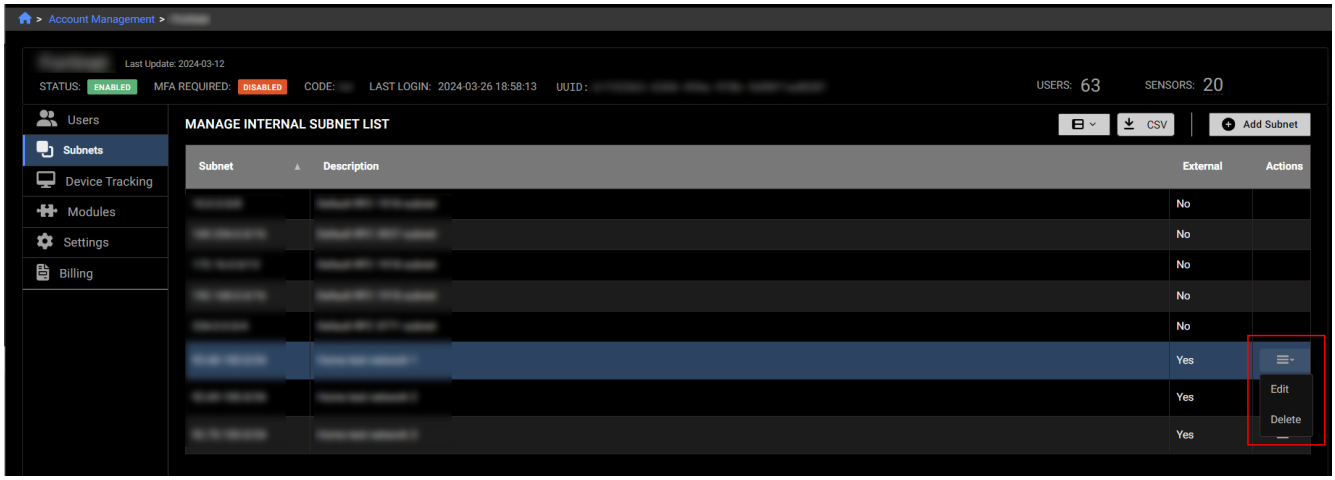
Edit subnets

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*.

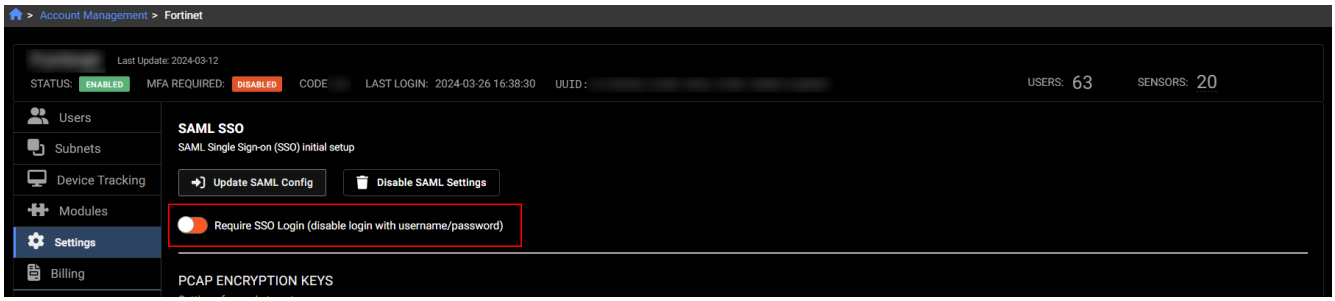


After the subnet is added, you can edit or delete the subnet from the menu in the *Actions* column.

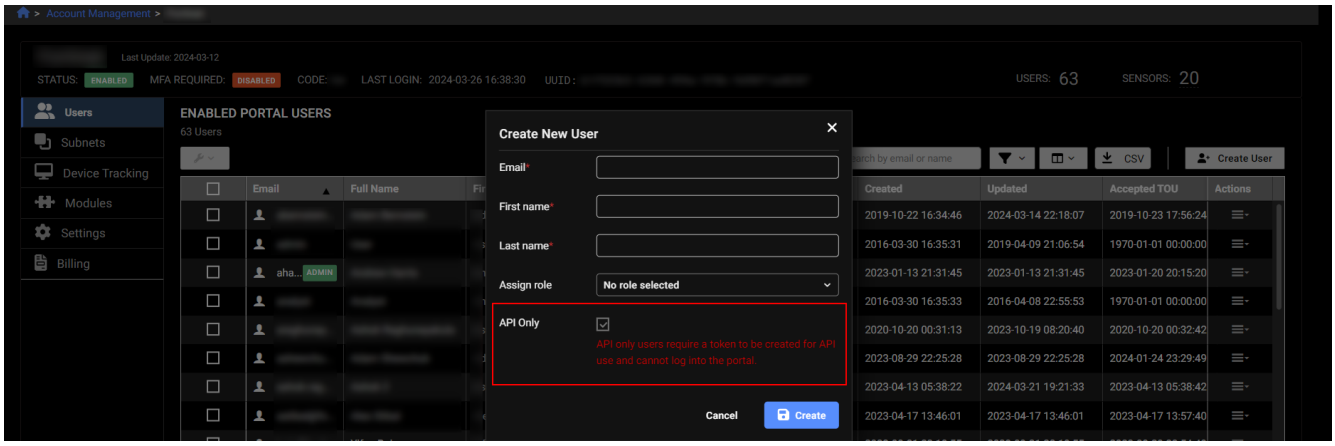


Mandatory SSO

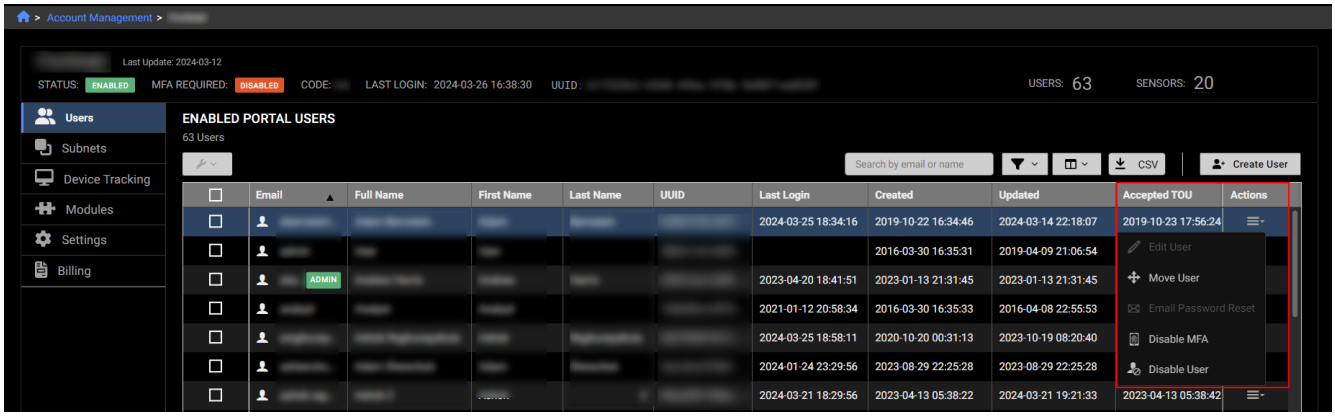
You can now require all users to log in with SSO. Go to *Account Management* > *Settings*. When SAML SSO is enabled the *Require SSO Logging disable login with username/password)* option is displayed. For more information, see Settings (Account Management) > SAML SSO > Mandatory SSO in the FortiNDR Cloud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



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



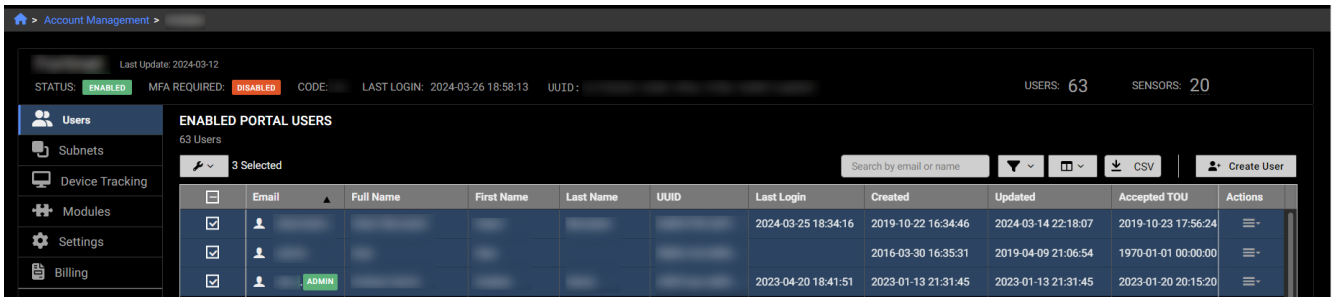
The *Edit User* and *Email Password Reset* options are also disabled in the *Users* page and the user details pane when mandatory SSO is enabled.



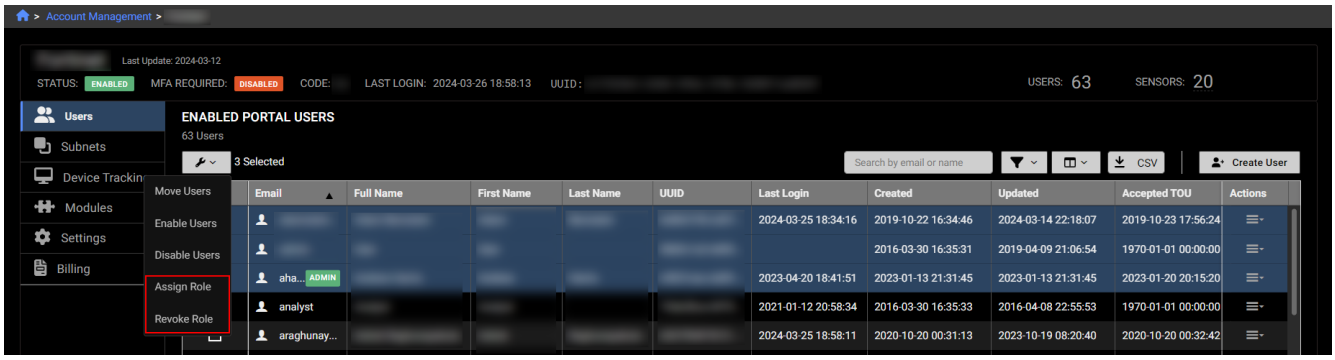
Improved Functionality

User management

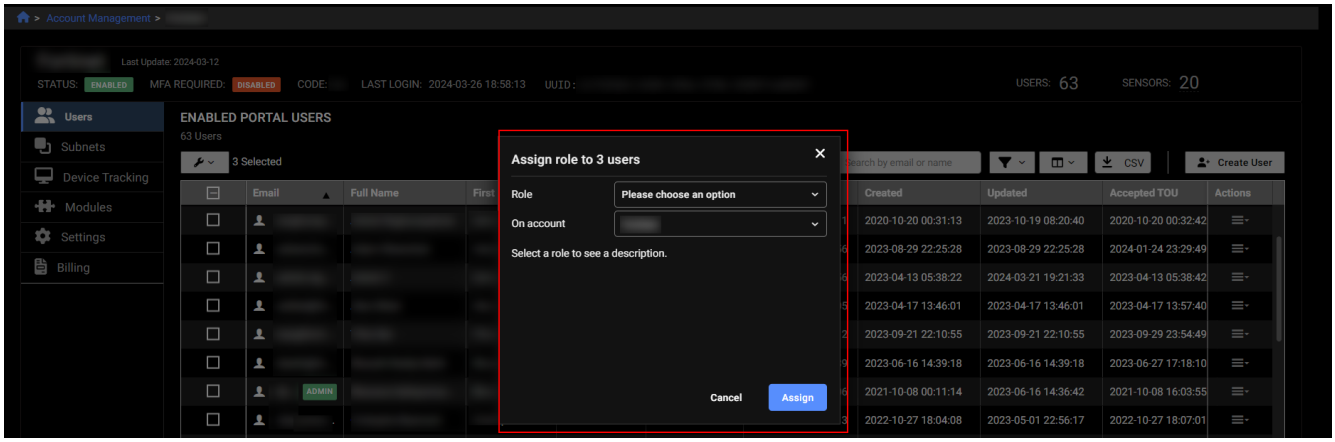
You can now assign or remove roles in bulk from the *User Management* page. Go to *Account Management* > *Users* and select the users you want to assign roles to.



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

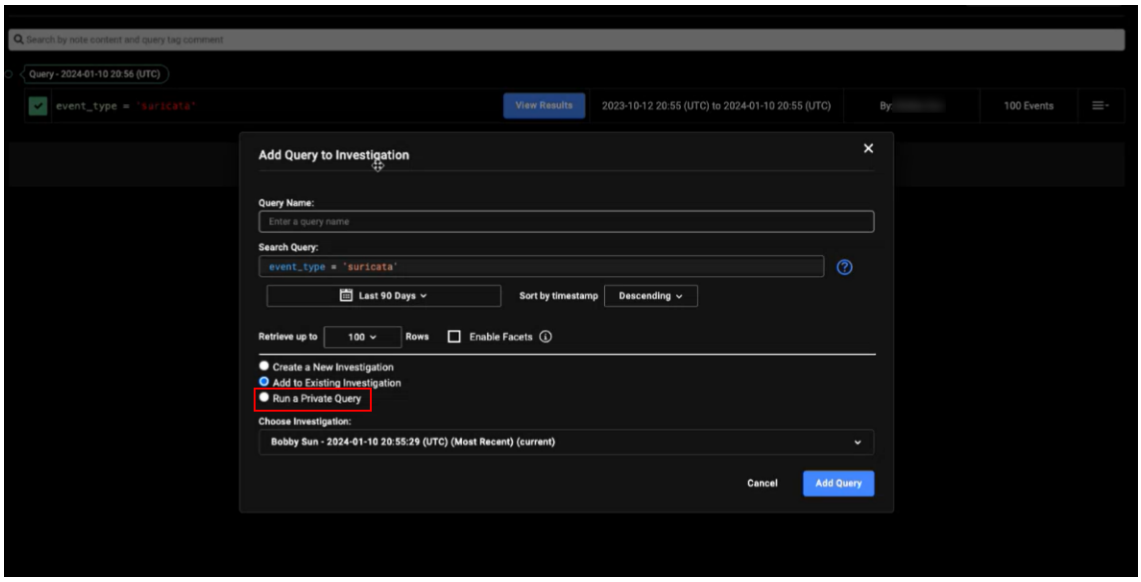


Select an option from the list and the click *Assign* or *Remove*. If the user has access to more than one account, you will see an *On Account* dropdown.



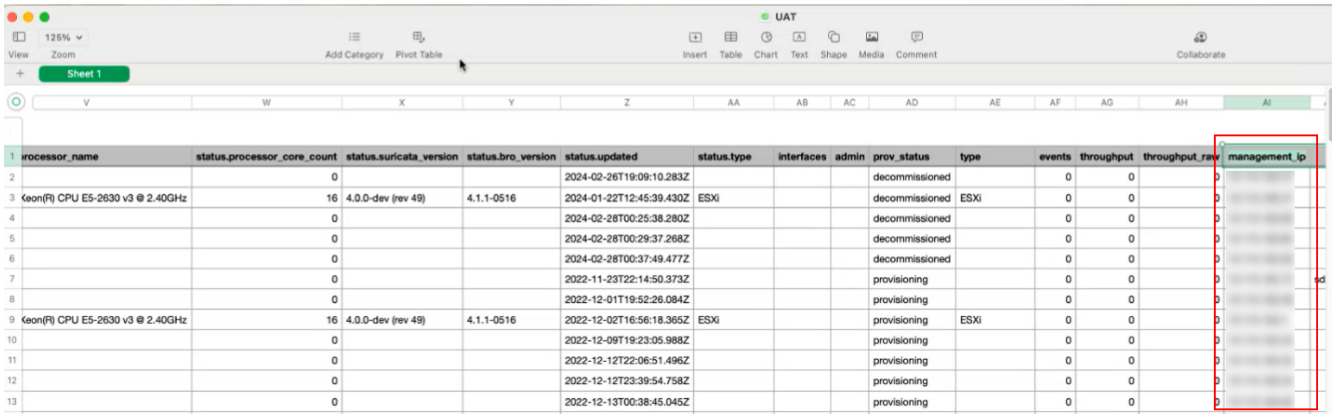
Run a private query

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 he Sensor CSV export. If the 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
	0			2024-02-26T19:09:10.283Z				decommissioned		0	0		
Xeon(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			2024-02-28T00:25:38.280Z				decommissioned		0	0		
	0			2024-02-28T00:29:37.268Z				decommissioned		0	0		
	0			2024-02-28T00:37:49.477Z				decommissioned		0	0		
	0			2022-11-23T22:14:50.373Z				provisioning		0	0		
	0			2022-12-01T19:52:26.084Z				provisioning		0	0		
Xeon(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			2022-12-09T19:23:05.988Z				provisioning		0	0		
	0			2022-12-12T22:06:51.496Z				provisioning		0	0		
	0			2022-12-12T23:39:54.758Z				provisioning		0	0		
	0			2022-12-13T00:38:45.045Z				provisioning		0	0		

13 March 2024 version 2024.2.1

Improved Functionality

Sensors

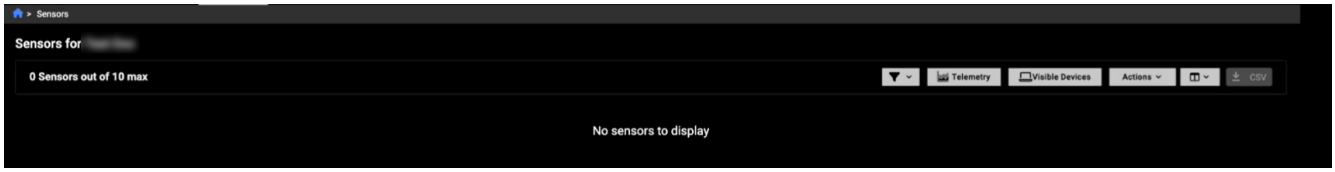
- A link to the Sensors topic in the *FortiNDR Cloud User Guide* was added to the *Status* column header in the *Sensors* page. This topic contains a description of each status.
- The *Sensor History* table in the *Sensor* detail page is hidden when there are no records to display.

29 February 2024 version 2024.2.0

New Functionality

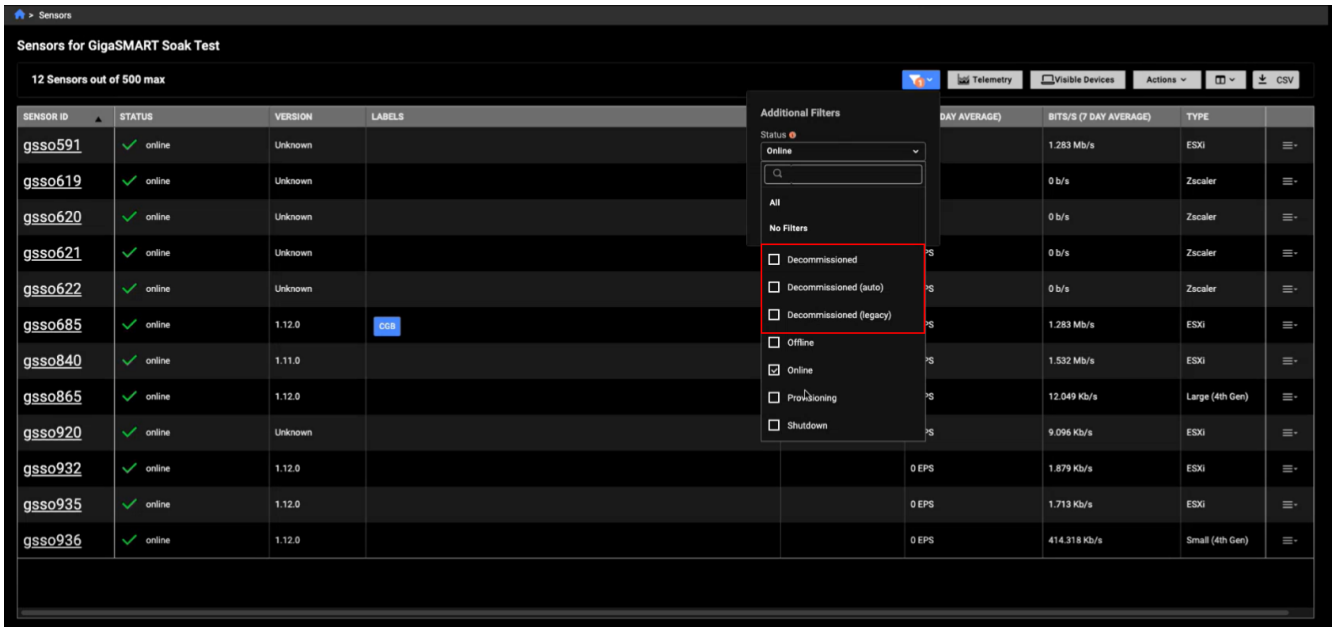
Sensors page

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



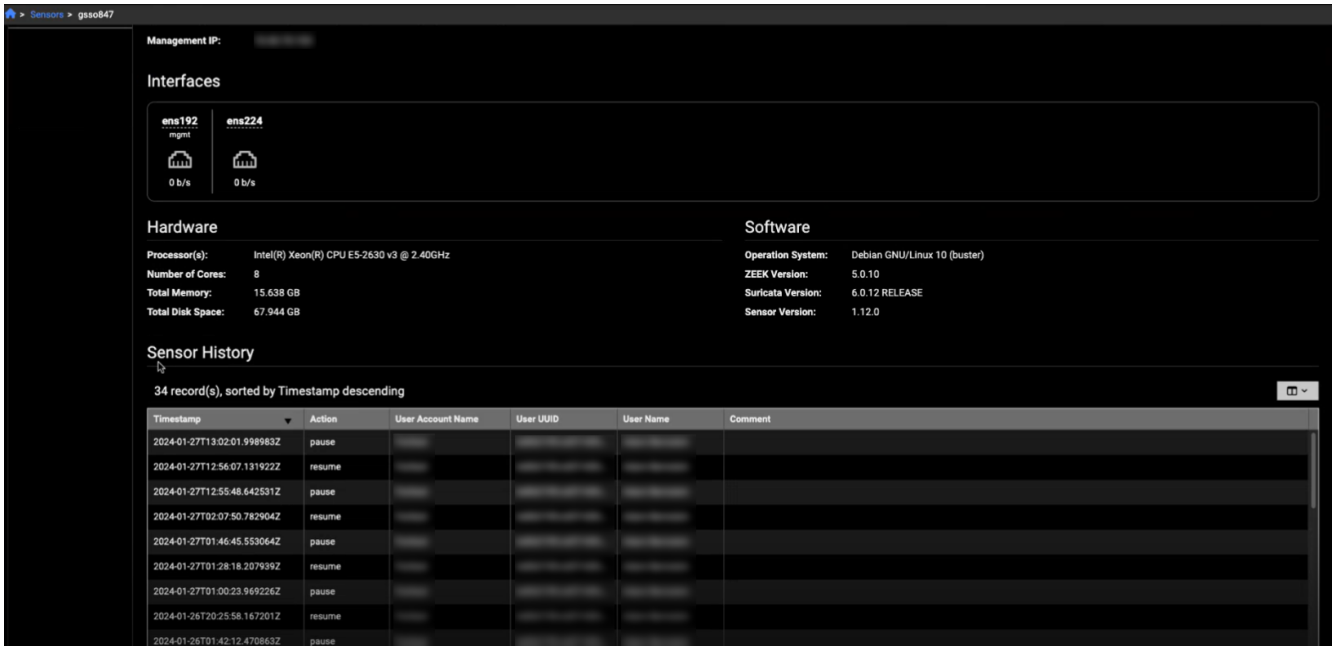
A new *Decommissioned* status was added. You can use this status to filter the page. The *Decommissioned (legacy)* status indicates a sensor that was previously disabled.

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.

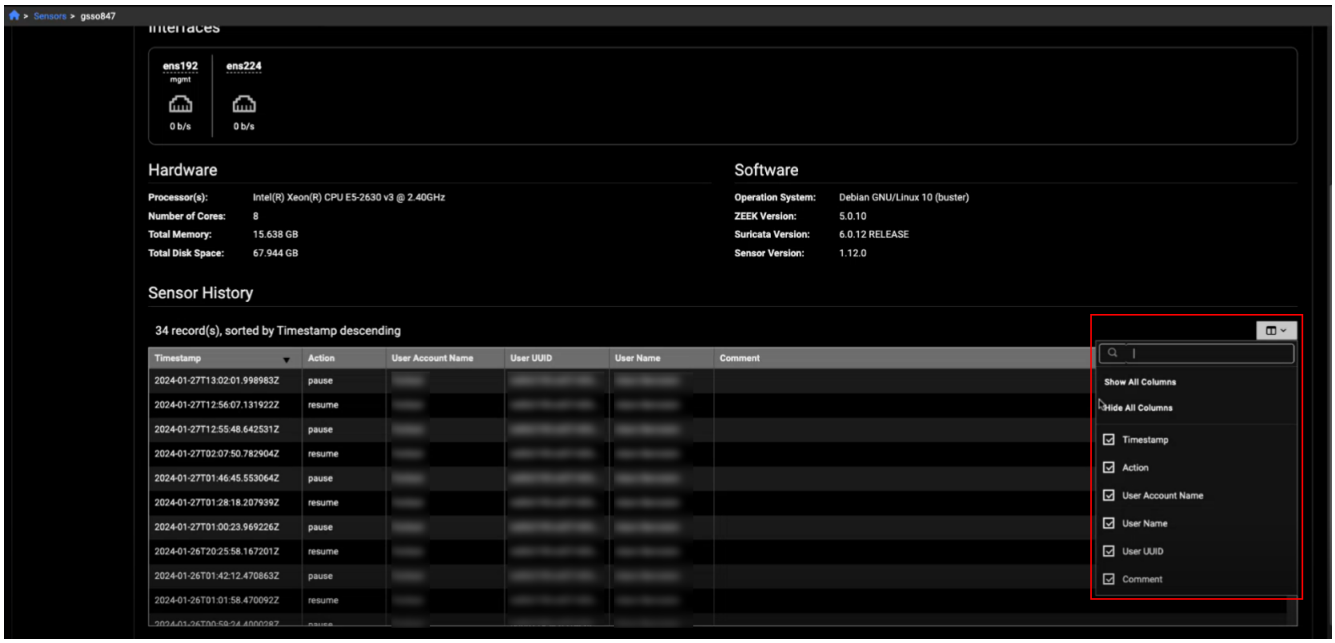


Sensor history

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.

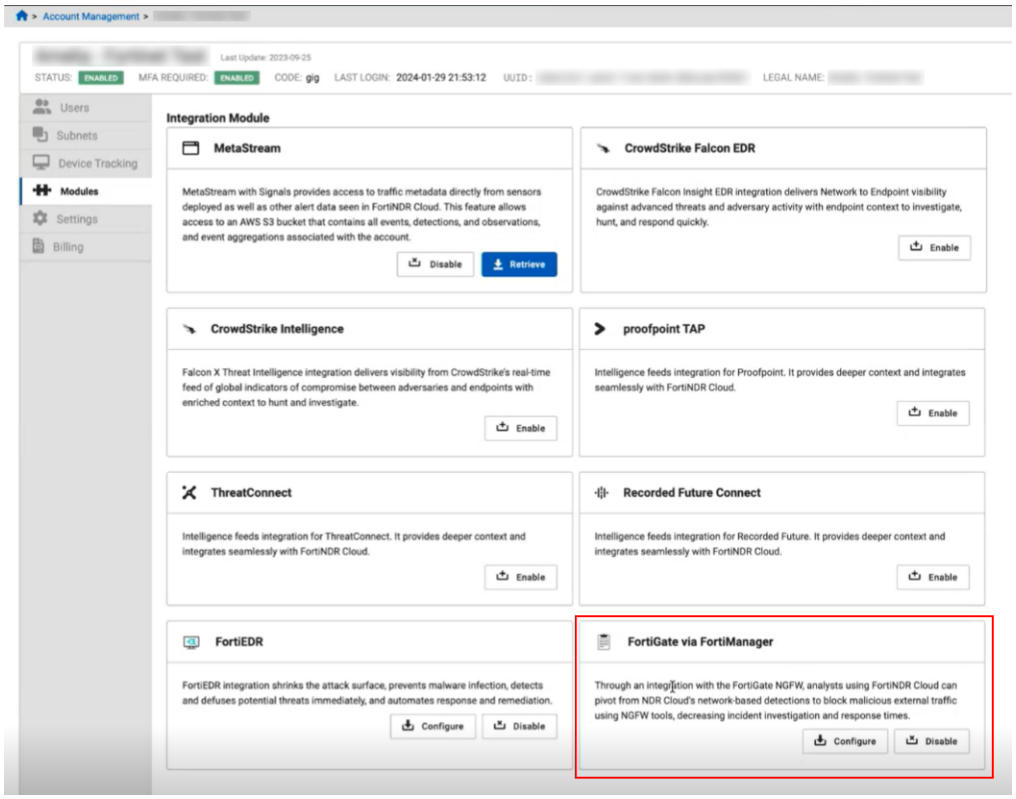


The table supports filtering. However, you cannot sort the *Timestamp* column in ascending order and you cannot fix the columns.

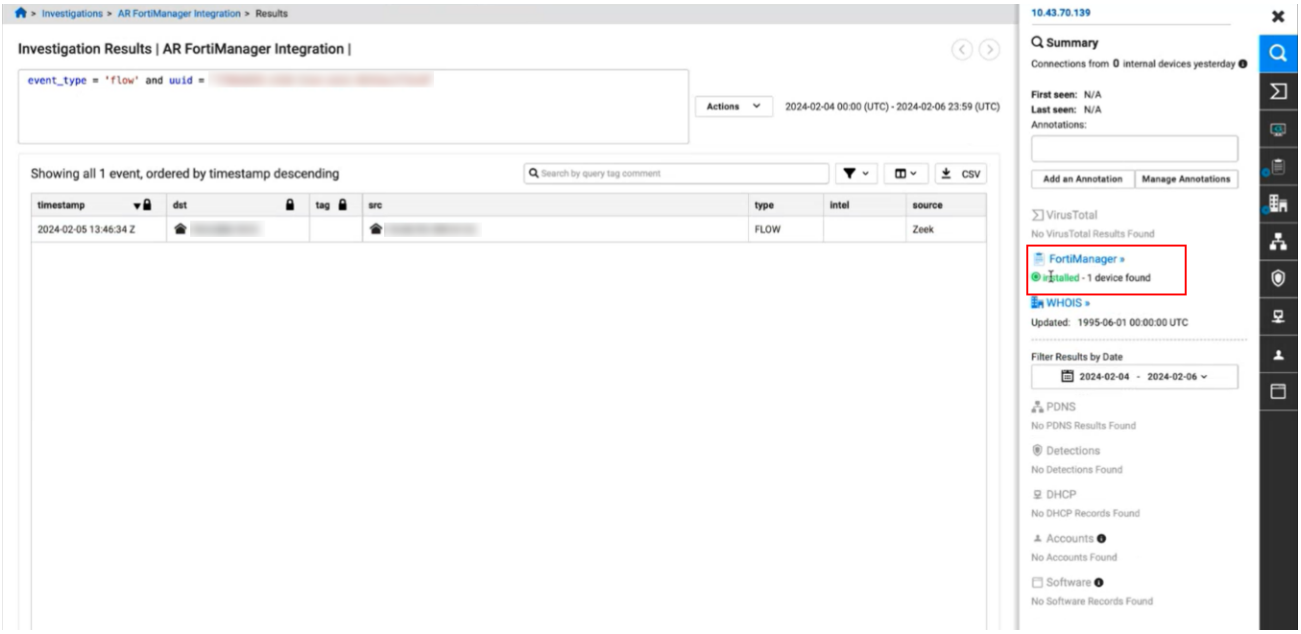


FortiGate integration

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.



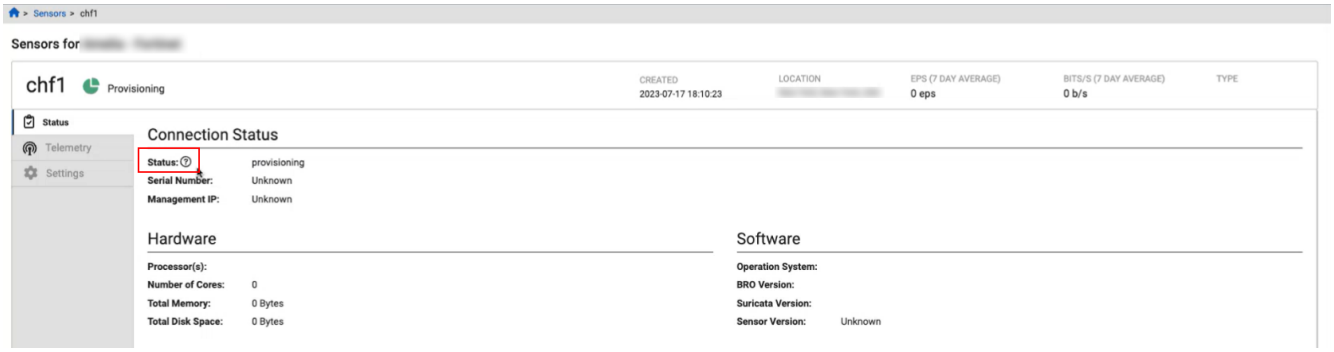
You can view the data collected by the integration and perform FortiGate actions in the *Entity Panel* when you click on an IP in the portal.



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*.



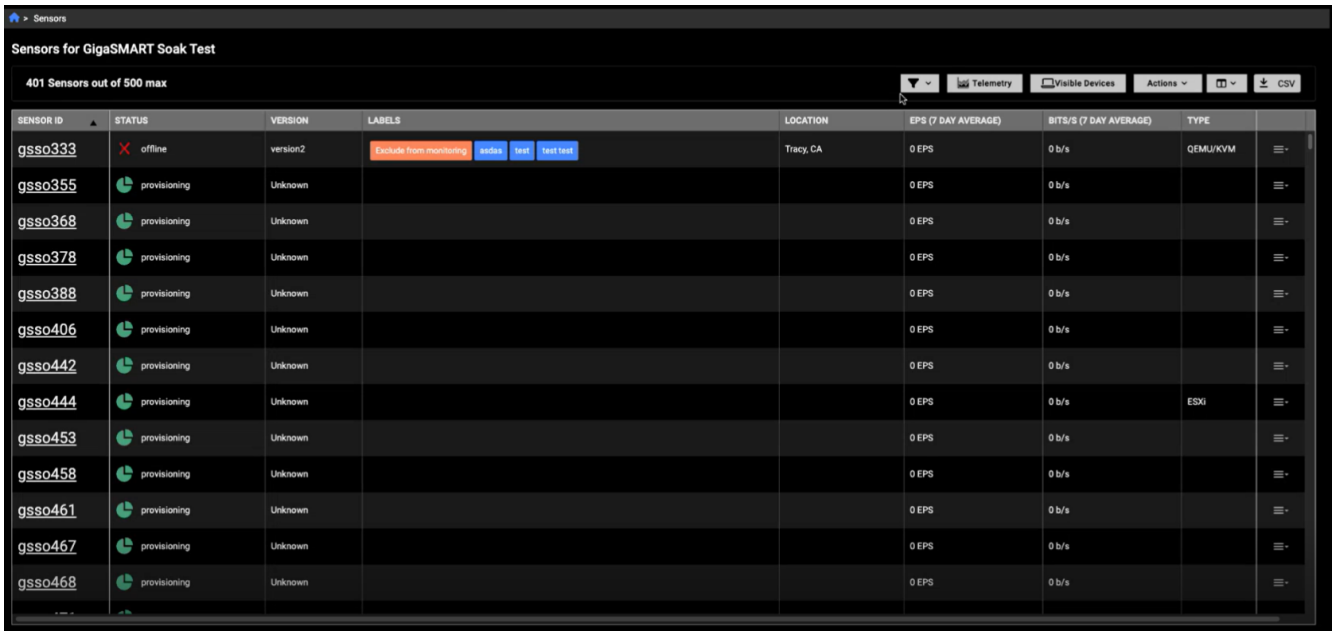
Other improvements

- 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*.

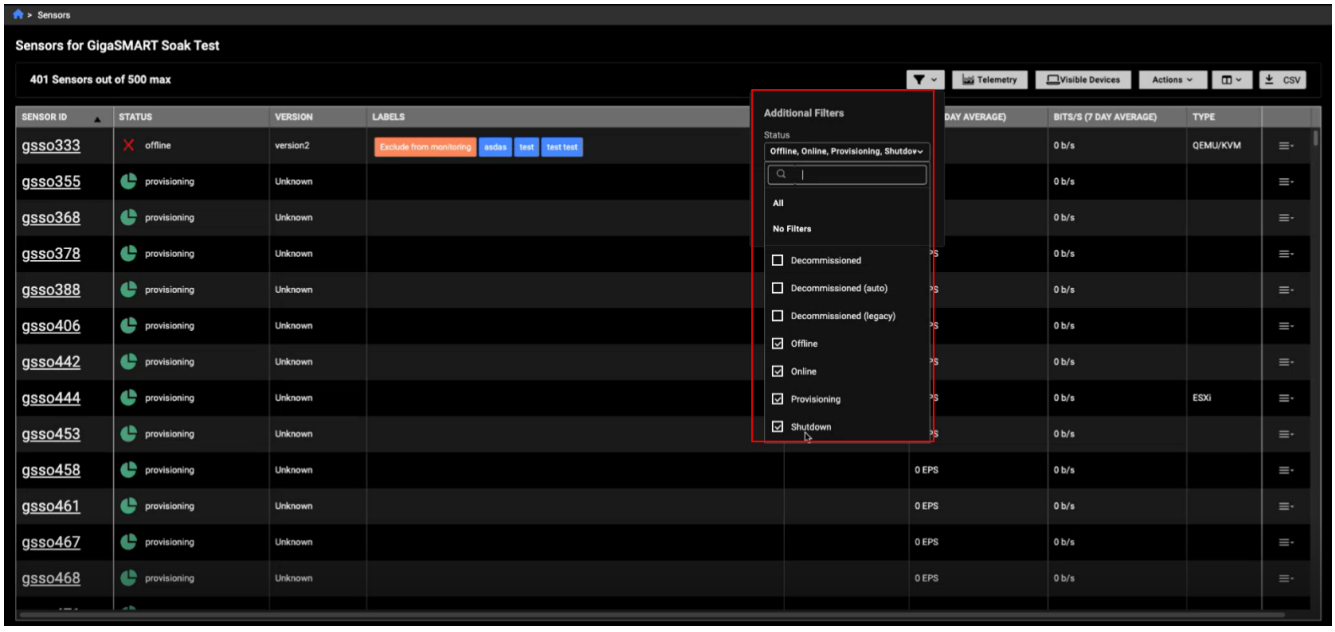
Discontinued Functionality

Enabled column

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



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.



14 February 2024 version 2024.1.1

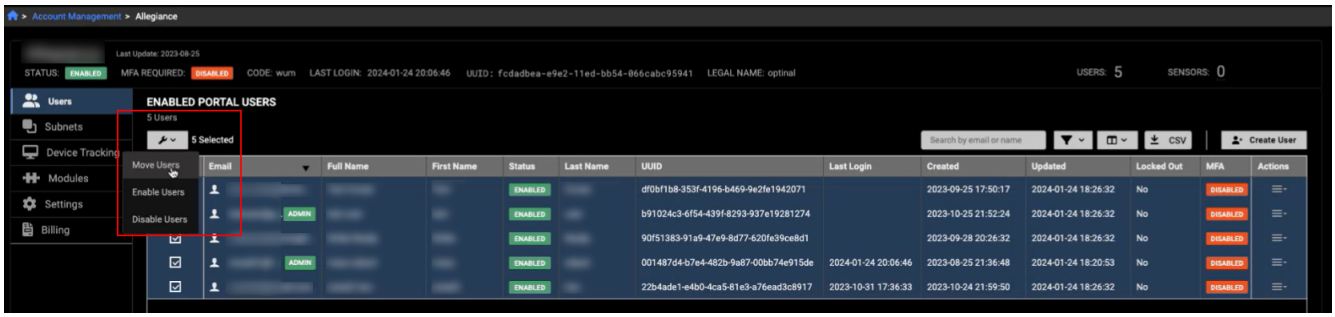
FortiNDR Cloud includes bug fixes, but no new features. See Resolved issues on page 65.

31 January 2024 Version 2024.1.0

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.

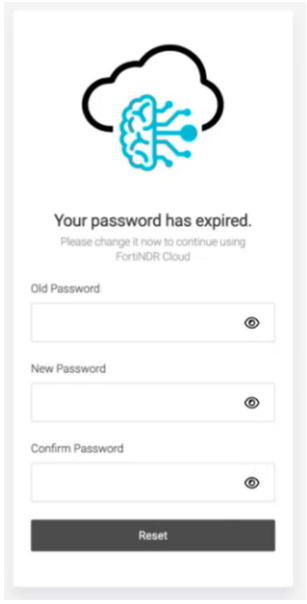
Sensor table

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 as been split into two columns: *EPS (7 Day average)* and *BITS/S (7 Day average)*. This allows you to sort each column individually.

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.



New detection rules and observations

This page lists the new detections rules and observations in FortiNDR Cloud. New rules are created every month; however, it possible that a rule is created in a category that already exists.

2024.11.0

Primary ATT&CK Name	ATR Category
Application Layer Protocol	Attack:Command and Control > HTTP(S) Beaconing
Exploit Public-Facing Application	Attack:Exploitation > Exploit Public-facing Application

2024.10.0

Primary ATT&CK Name	ATR Category
Application Layer Protocol	Attack:Command and Control > Connectivity Check
DNS	Attack:Command and Control > DNS Tunneling
Ingress Tool Transfer	Attack:Installation > Remote File Copy from External
LLMNR/NBT-NS Poisoning and SMB Relay	Posture:Anomalous Activity
Remote Access Software	Posture:Potentially Unauthorized Software or Device > Remote Admin Tools
Symmetric Cryptography	Attack:Command and Control > Other Protocol

2024.9.0

Primary ATT&CK Name	ATR Category
Abuse Elevation Control Mechanism	Attack:Exploitation
Application Layer Protocol	Attack:Command and Control > Web Shell
Exploit Public-Facing Application	Attack:Exploitation > Exploit Public-facing Application

Primary ATT&CK Name	ATR Category
Non-Application Layer Protocol	Attack:Command and Control > Custom Protocol
Web Protocols	Attack:Command and Control > HTTP(S) Beaconing

2024.8.0

Primary ATT&CK Name	ATR Category
Application Layer Protocol	Attack:Command and Control > Other Protocol
Domain Account	Attack:Discovery > Remote System Scanning
Domain Controller Authentication	Attack:Miscellaneous
Exploit Public-Facing Application	Attack:Exploitation > Exploit Public-facing Application
Exploitation for Client Execution	Attack:Exploitation
Exploitation for Privilege Escalation	Attack:Miscellaneous
Network Denial of Service	Attack:Impact > Network DoS
Non-Application Layer Protocol	Attack:Command and Control > Custom Protocol

2024.5.0

Primary ATT&CK Name	ATR Category
Exploit Public-Facing Application	Attack: Command and Control > Other Protocol
Non-Application Layer Protocol	Attack:Command and Control > Other Protocol

2024.4.0

Primary ATT&CK Name	ATR Category
Network Denial of Service	Attack: Impact > Network DoS
Exploit Public-Facing Application	Attack: Exploitation > Exploit Public-facing Application
Network Denial of Service	Attack: Impact > Network DoS
Network Denial of Service	Posture: Anomalous Activity
Network Denial of Service	Attack: Impact > Service DoS
Network Denial of Service	Attack: Impact > Network DoS

2024.3.1

Primary ATT&CK Name	ATR Category
Application Layer Protocol	PUA:Adware
Command and Scripting Interpreter	Attack:Exploitation > Exploit Public-facing Application
Exfiltration Over Web Service	Attack:Exfiltration > C2 Server Upload
Exploit Public-Facing Application	Attack:Exploitation > Exploit Public-facing Application
Non-Application Layer Protocol	Attack:Command and Control > Custom Protocol
Web Protocols	Attack:Command and Control > HTTP(S) Beaconing

2024.3.0

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

2024.2.0

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

2024.11.0

Description
Fixed the CSV download of users in Account Management to honor the Account Access filter.
Resolved a UUID issue when updating an account.

2024.10.0

Description
Fixed the CSV download of users in Account Management to honor the Account Access filter.
Resolved a UUID issue when updating an account.
Fixedt he resizing in the Event Type field.
Resolved issues affecting PCAP tasks.
Fixed a Crowdstrike containment issue.

2024.9.0

Description
Fixed an issue where clicking Resolve deselected the items in a bulk action.
Sharing investigations in the EU portal no longer fails.
The legend in the detections Visualizer no longer overlaps with the data.

2024.8.1

Description
Three vulnerability bugs have been resolved.
Resolved an issue where the buttons on the Investigation Detail page were missing for some users.
Resolved an issue where certain columns were empty when viewing a query grouped by result.

2024.8.0

Description
Fixed a performance issue with the Search field in the Detection Triage Rules Page.
Fixed the Roles & Permissions page to display properly in Firefox.
The Notable Detection Rules widget is displayed when there are no rules as designed.
Fixed inconsistencies between menu names and the breadcrumb.
Resolved an issue where the Entity Panel was not loading the Summary panel.
Fixed the columns and rows to fit the Files dialog.
Fixed inconsistent title case for the Source Device list.

2024.7.0

Description
Fixed the MetaStream module.
No feedback was provided when a password reset failed.
The All Accounts option was sometimes missing in the Run on Accounts dialog.
Resolved a bug in the Default Dashboard. The Go back to dashboard link works as designed.
The sensor status updated timestamp is now visible on the sensor detail page.
Dashboards can be saved.
The count of visible devices had significant variations.
Fixed the security posture report query.
Fixed the New X.509 Certificates From VPS dashboard query.

Description
Fixed the DCE/RPC Over Time dashboard query.
The correct IQL and Druid queries are used for the security report query Total Internal Hosts Serving TLSv1.1

2024.6.0

Description
Resolved an issue in the Detections List where the Resolution filter was missing Automatically Resolved.
Auto-closing characters in the IQL editor no longer disables the Search button.
Users can no longer disable themselves via the user details pane or with bulk actions.
The icons in the Entity Panel are no longer obscured by the scroll bar when viewed in Safari.
Disabled accounts no longer appear in the account list when you assign a role, move a user. or perform bulk actions.
Resolved an issue in Reports where users could not select dates older than the supported backlog.
The undo function has been fixed in the Add Query field in Investigations.
Fixed an error in the Hosts Potentially Running EOL Versions of Windows query.
The security posture report shows the correct IQL version of Total Hosts Using Remote Storage Services via SSL and Total Hosts Using Remote Storage Services via HTTP.
Resolved an issue with the Users list where API users could not be deleted.
Fixed a malformed URL and error message when logging in and out of FortiNDR Cloud from the Rules details page.

2024.5.0

Description
Account Management no longer displays two copies of an API token.
Fixed the example CSV file in the Manage Annotations page.
Fixed the All option in the Account dropdown menu.
Fixed the delete function in Modify Annotations in the Entity Panel.

2024.4.1

Description
The detection counts in the Mitre Attack dashboard widget match the Detections Table as intended.
When a user clicks a link in an email, they no longer land on the Dashboard after they log into the portal.
When searching the Detections Table with the device IP, the search box displays the IP after the page is refreshed.
Modifying the search in adhoc search results no longer clears the IQL query box.
The items in the notifications dropdown no longer blink.

2024.4.0

Description
Fixed the formatting in the Sensor detail page.
Clicking the Filehash indicators opens the Entity Panel as expected.
The Lifetime Events column in the Detections List no longer displays a Null value.
Fixed the Create button when creating a token.
Resolved an error message issue when resetting the password.
Resolved a navigation issue when creating a playbook.
Fixed the scroll bars in playbooks with a large number of queries.

2024.3.1

Description
Fixed the Isolate Device feature in the FortiEDR integration.
The filters in the Sensors list no longer persist when you pivot to an account that does not have any sensors.
Fixed a styling issue in Account Management that caused errors to overlap with the page content.
Resolved an error handing issue in the FortiManager integration configuration.

2024.3.0

Description
Power users can see the labels in the Sensors 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 Account error page no longer appears when a page is refreshed.
Resolved an issue where all accounts displayed telemetry data in the Sensor page.

2024.2.1

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

2024.2.0

Description
Users with multiple accounts will see the Edit button for the accounts with Admin permissions.
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

Copyright© 2025 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.