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

TABLE OF CONTENTS

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
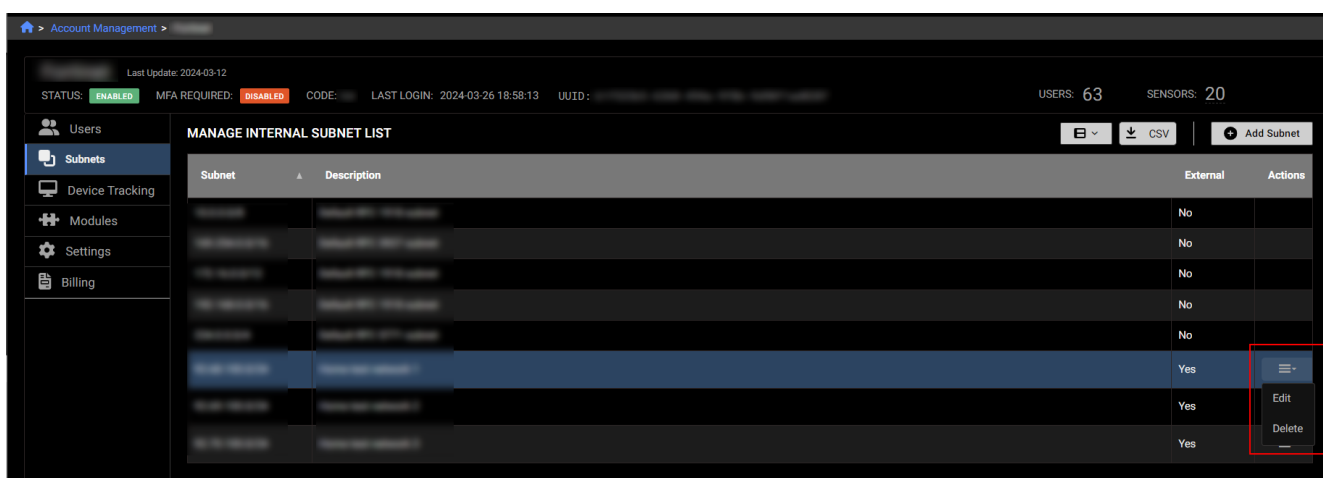
New Functionality

Edit subnets

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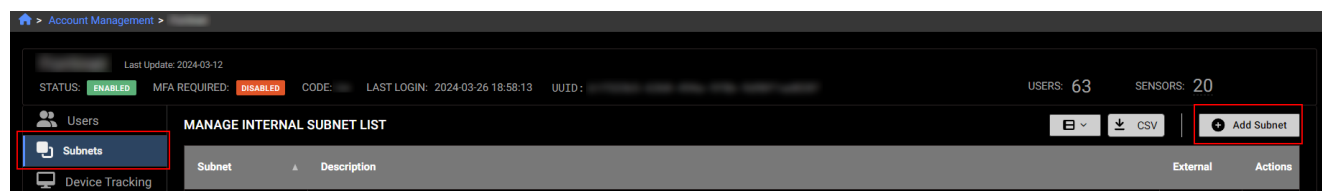

Configure the subnet and click *Add Subnet*.
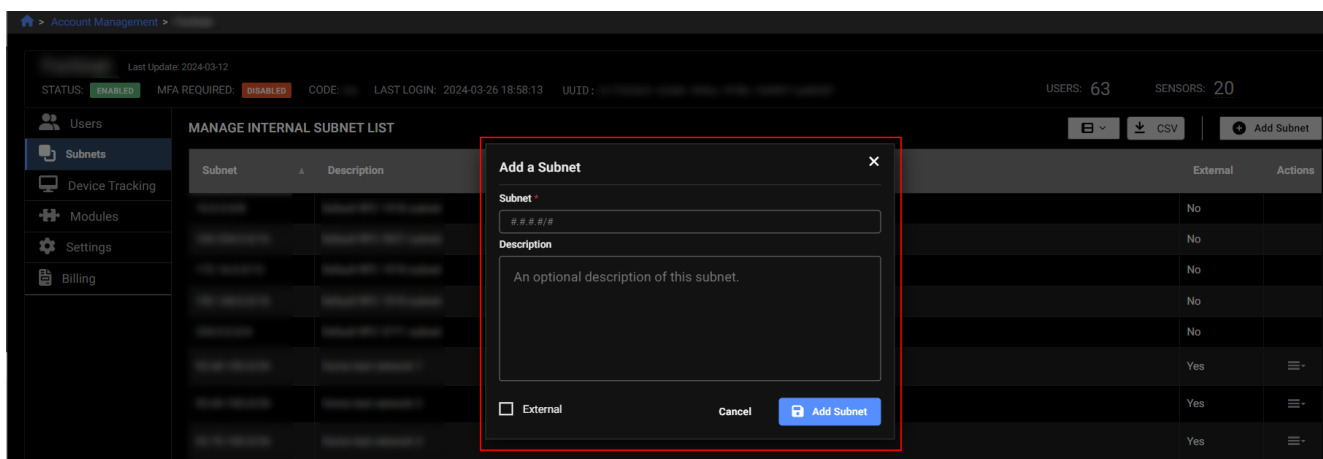
After the subnet is added, you can edit or delete the subnet from the menu in the *Actions* column.
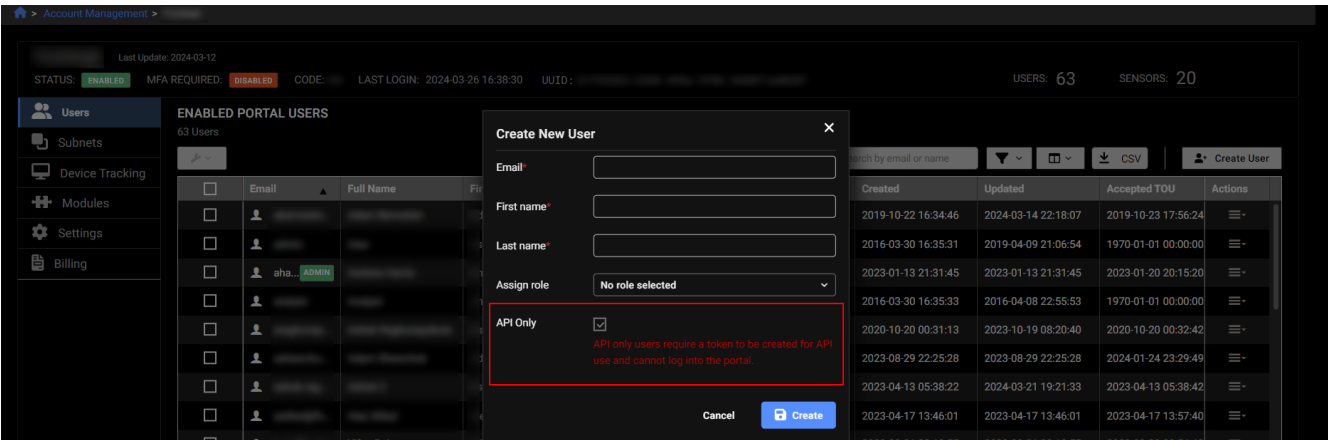

Mandatory SSO

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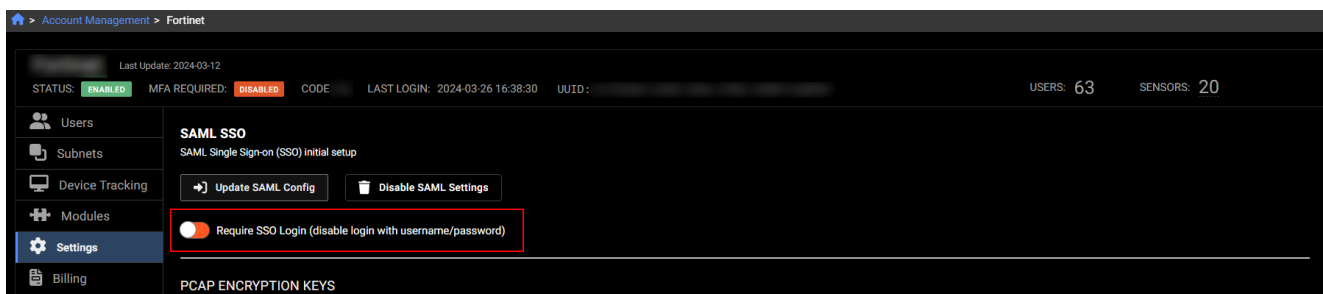
When mandatory SSO is enabled, *API Only* is selected by default when you create a new user.

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.
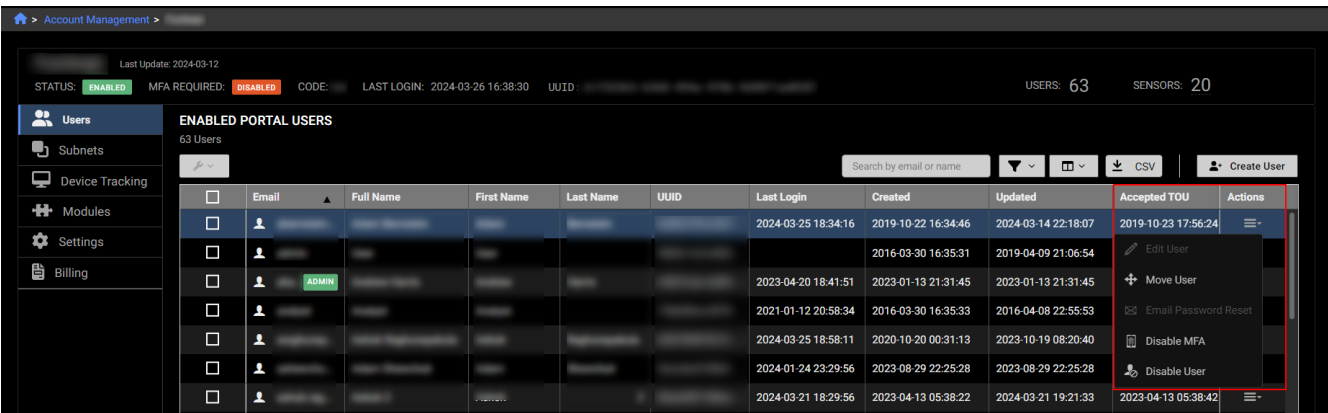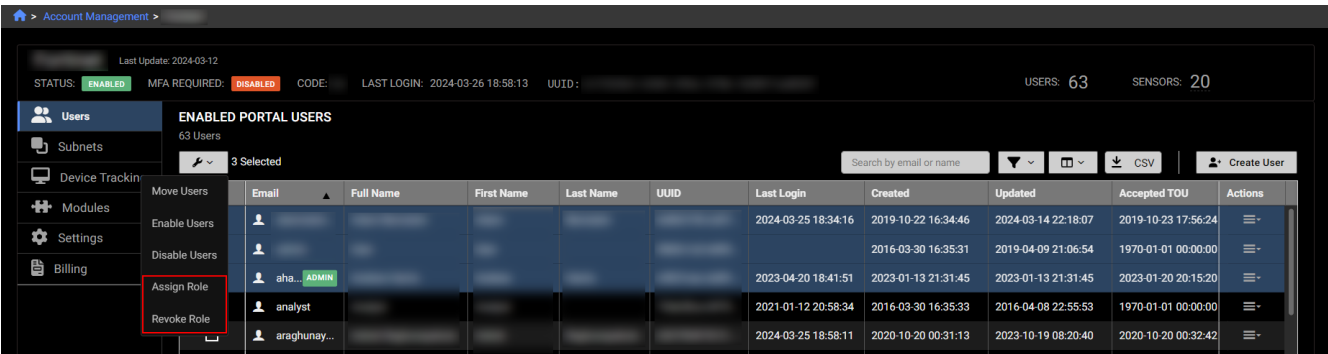

Improved Functionality

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.
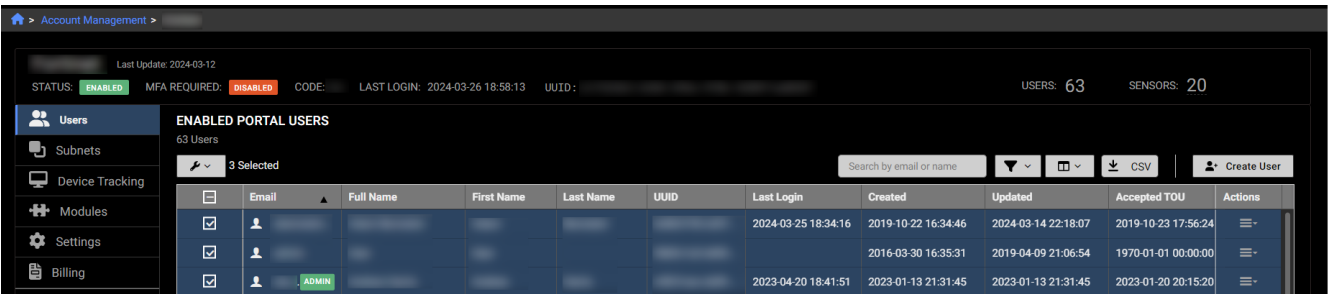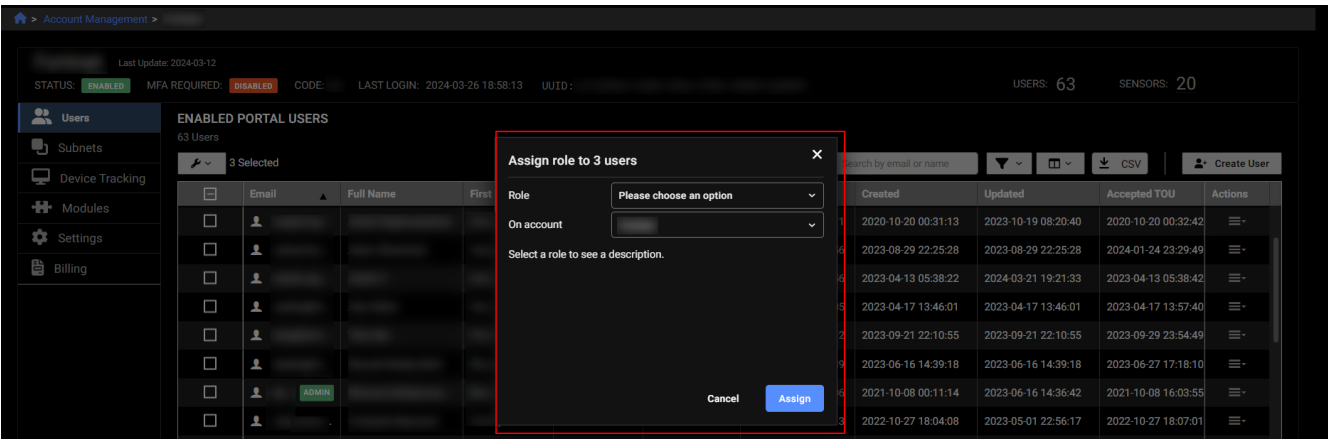

Click the tool icon and select *Assign Role* or *Revoke Role*.

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*.
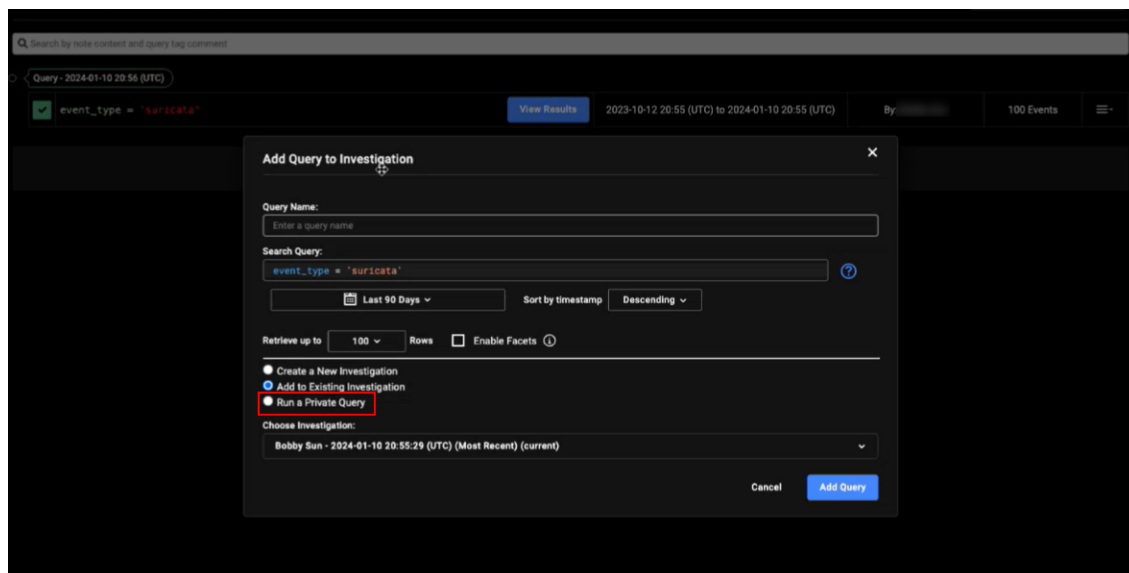
Export sensor information

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

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.
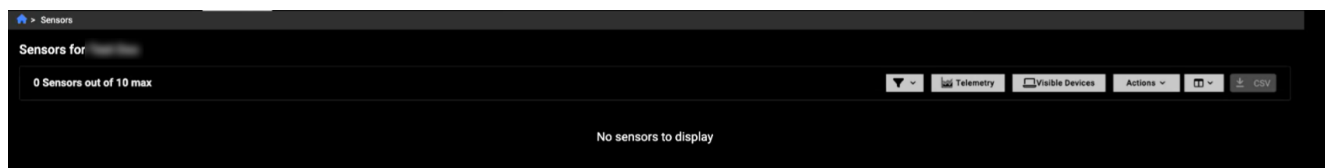
29 February 2024 version 2024.2.0

New Functionality

Sensors page

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*.
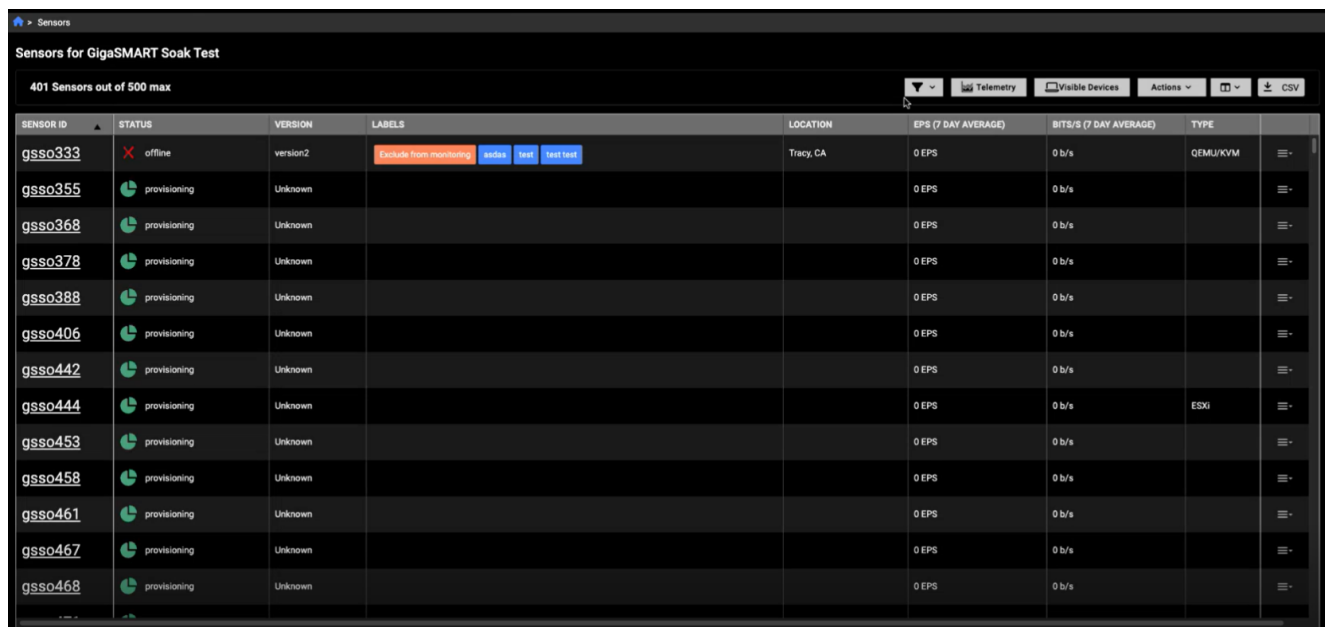
Other improvements

- 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 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.
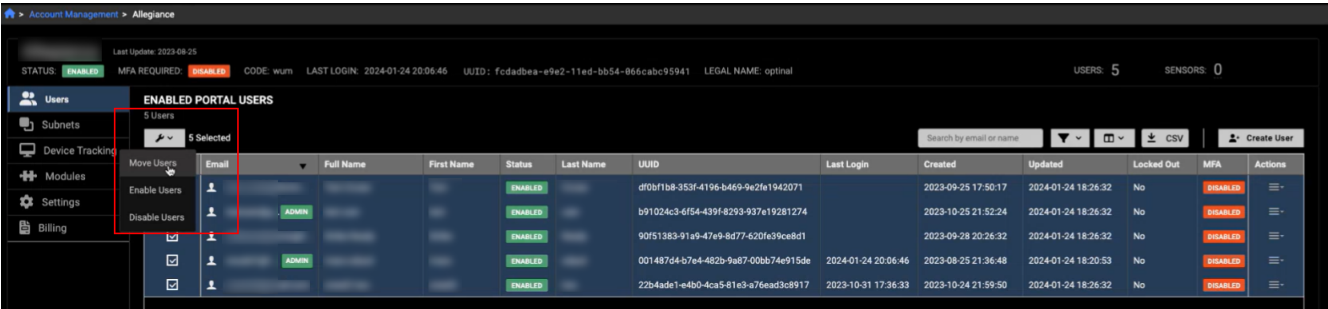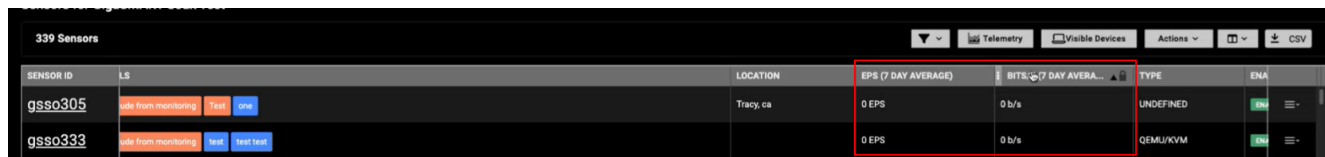
You are also able to filter users by account access.
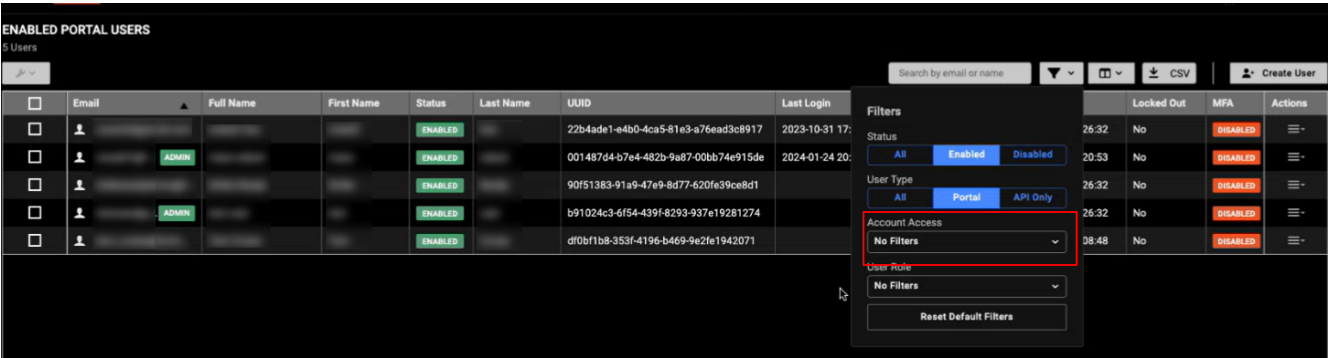
Sensor table

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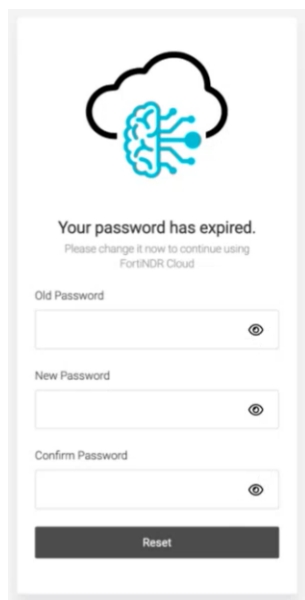
Password enforcement

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

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

2024.3.0

Rules

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

Observations

Name	Description
SSL C2 Beaconing Similarity	Identify SSL connections that resemble Command and Control (C2) beaconing 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
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

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 *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.

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.

FÜRTINET® www.fortinet.com