Release Notes

FortiDevice 26.1.a

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 22, 2026
FortiDevice 26.1.a Release Notes
97-261a-1243925-20260122

TABLE OF CONTENTS

Change log 4
What’s new in FortiDevice 26.1.a 5
Introduction 6
Web screenshots 6
Service ports 6
Supported web browsers 6
Upgrade information 7
Product integration and support 9
Resolved issues 12
Known issues 14

Change log

Date	Change Description
January 22, 2026	Initial document release for FortiDevice 26.1.a

What’s new in FortiDevice 26.1.a

Release 26.1.a provides the following new features:

- You can now use a FortiGate device as a one-arm sniffer to collect traffic from FortiSwitch mirrored ports with the FortiOS API and report the data in the FortiDevice dashboard.

  To use this feature:

  a. Manage one or more FortiSwitch units with a FortiGate device.
  b. Add a FortiGate fabric connector in FortiDevice.
  c. Add a task.
- You can now examine your inventory with an Operational Technology (OT) view. The OT view shows a list of OT devices or the OT devices grouped by Purdue Model levels. Clicking on the MAC address or host name of an OT device gives the device details, such as hardware family, type, vendor, and version. You can change the owner of the device and add tags to devices, as well as filter the devices by site or by Purdue Model level.
- “Scans” are now referred to as “tasks” throughout the GUI.
- When a new user logs in to FortiDevice, a window now displays, asking if the user would like a trial license. Previously, a trial contract was activated automatically for a new user.
- There are new pagination options at the bottom of the *Inventory > Devices*, *Inventory > Vulnerabilities*, *Inventory > Software*, *Inventory > Services*, *Events > Events*, and *Events > Log Servers* pages that allow you to change how many items are displayed per page. You can now select 10, 20, 50, 100, and 500 items. Previously, you could only select 100 items.
- When you create a standard task, a new checkbox, *Skip Unresponsive Hosts*, can decrease the amount of time for executing a task. When the vulnerability scan level is set to *Partial* or *Full*, the new checkbox is automatically selected, but you can clear the checkbox if you prefer.

Introduction

This document provides the following information for FortiDevice 26.1.a build 0018 and FortiDevice Detector 3.1.0 build 0007:

- Upgrade information on page 7
- Product integration and support on page 9
- Resolved issues on page 12
- Known issues on page 14

See the Fortinet Document Library for FortiDevice documentation.

Web screenshots

FortiDevice Detector uses Google Chrome to access a web service (for example, HTTP 80 or HTTPS 443) URL and store the response as an HTML file. If the headless mode does not work properly, use the official Chrome packages with the following commands:

```
curl -o chrome.deb https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb
      && sudo apt install ./chrome.deb
```

Service ports

FortiDevice Detector connects to the FortiDevice server host on TCP port 443.

Supported web browsers

FortiDevice supports the latest versions of the following web browsers:

- Google Chrome
- Mozilla Firefox

Other web browsers might work as well but have not been rigorously tested.

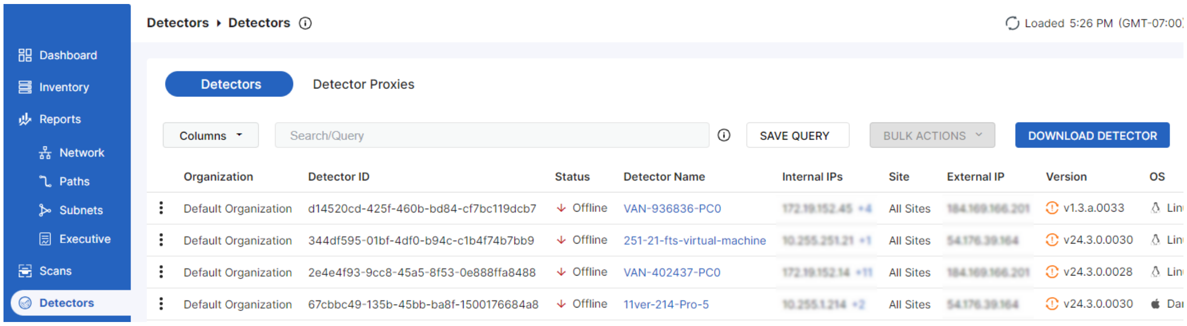
Upgrade information

FortiDevice Detector is a lightweight scan engine that enables network and asset discovery and vulnerability scanning. FortiDevice requires the use of at least one Detector within your environment. The Detector needs to be installed on a system with reliable connectivity to the network you want to discover.

To install FortiDevice Detector, see the *FortiDevice Administration Guide*.

To upgrade FortiDevice Detector:

1. Go to *Detectors*.

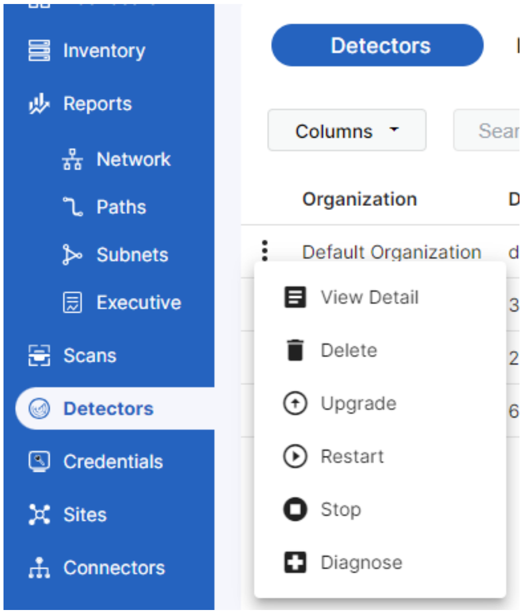


	Organization	Detector ID	Status	Detector Name	Internal IPs	Site	External IP	Version	OS
⋮	Default Organization	d14520cd-425f-460b-bd84-cf7bc119dcb7	↓ Offline	VAN-936836-PC0	[redacted]	All Sites	[redacted]	v1.3.a.0033	Lin
⋮	Default Organization	344df595-01bf-4df0-b94c-c1b4f74b7bb9	↓ Offline	251-21-fts-virtual-machine	[redacted]	All Sites	[redacted]	v24.3.0.0030	Lin
⋮	Default Organization	2e4e4f93-9cc8-45a5-8f53-0e888ffa8488	↓ Offline	VAN-402437-PC0	[redacted]	All Sites	[redacted]	v24.3.0.0028	Lin
⋮	Default Organization	67cbbc49-135b-45bb-ba8f-1500176684a8	↓ Offline	11ver-214-Pro-5	[redacted]	All Sites	[redacted]	v24.3.0.0030	Dar

2. Click the ellipsis at the left end of the row of the Detector that you want to upgrade.

The Detector must be online.

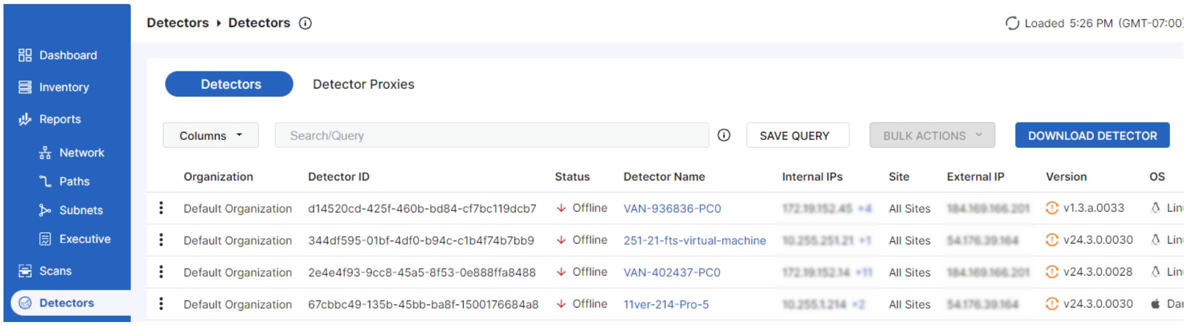
3. Select *Upgrade*.



4. In the *Upgrade Detector?* dialog box, click *UPGRADE*.

To upgrade multiple FortiDevice Detectors:

1. Go to *Detectors*.



	Organization	Detector ID	Status	Detector Name	Internal IPs	Site	External IP	Version	OS
⋮	Default Organization	d14520cd-425f-460b-bd84-cf7bc119dcb7	↓ Offline	VAN-936836-PC0	[redacted]	All Sites	[redacted]	v1.3.a.0033	Lin
⋮	Default Organization	344df595-01bf-4df0-b94c-c1b4f74b7bb9	↓ Offline	251-21-fts-virtual-machine	[redacted]	All Sites	[redacted]	v24.3.0.0030	Lin
⋮	Default Organization	2e4e4f93-9cc8-45a5-8f53-0e888ffa8488	↓ Offline	VAN-402437-PC0	[redacted]	All Sites	[redacted]	v24.3.0.0028	Lin
⋮	Default Organization	67cbbc49-135b-45bb-ba8f-1500176684a8	↓ Offline	11ver-214-Pro-5	[redacted]	All Sites	[redacted]	v24.3.0.0030	Dar

2. Select two or more rows.
3. From the *BULK ACTIONS* menu, select *Upgrade*.

> The Detectors must be online.

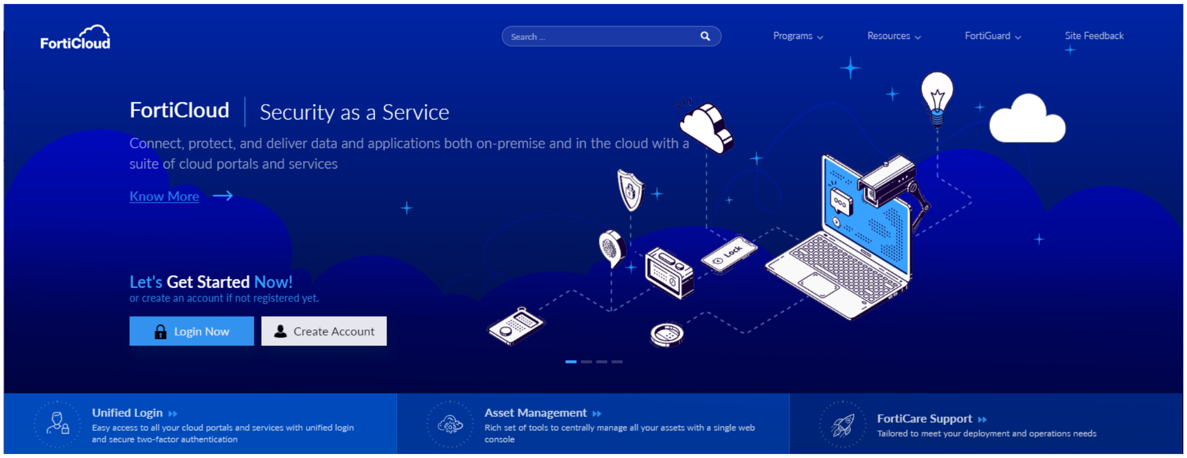
4. In the *Upgrade Detector?* dialog box, click *UPGRADE*.

Product integration and support

You need to create an account in the FortiCloud support portal, create an IAM user, and register your FortiDevice license.

To create an account:

1. Go to https://support.fortinet.com/.



FortiCloud | Security as a Service

Connect, protect, and deliver data and applications both on-premise and in the cloud with a suite of cloud portals and services

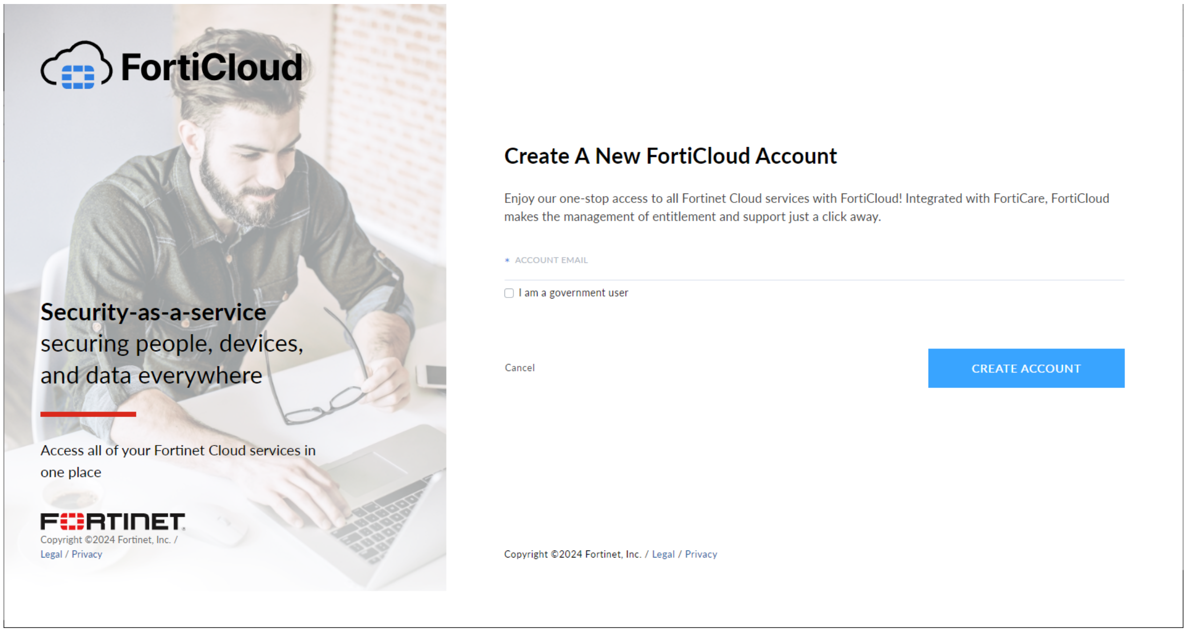
Let's Get Started Now!
or create an account if not registered yet.

Unified Login
Easy access to all your cloud portals and services with unified login and secure two-factor authentication

Asset Management
Rich set of tools to centrally manage all your assets with a single web console

FortiCare Support
Tailored to meet your deployment and operations needs

2. Click *Create Account* to create an account.



Security-as-a-service securing people, devices, and data everywhere

Access all of your Fortinet Cloud services in one place

Copyright ©2024 Fortinet, Inc. /

Create A New FortiCloud Account

Enjoy our one-stop access to all Fortinet Cloud services with FortiCloud! Integrated with FortiCare, FortiCloud makes the management of entitlement and support just a click away.

☐ I am a government user

Copyright ©2024 Fortinet, Inc. /

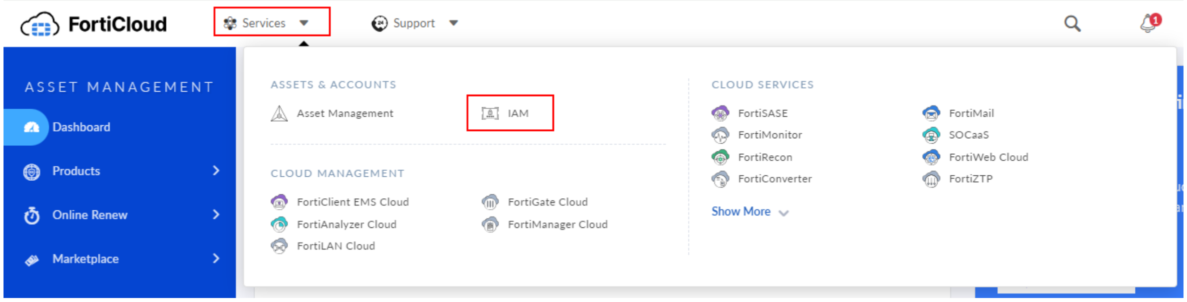
3. If you are a government user, select the *I am a government user* checkbox. Follow the steps in the dialog box if you are a U.S. Federal Government user or click *No, Just Proceed.*
4. If you are not a government user, enter your email address for your account and click *CREATE ACCOUNT*.

5. In the *Enter Captcha Code* field, enter the provided CAPTCHA code.
6. Click *Get Email Verification Code*.

   An email that includes a verification code is sent to your email address that you entered earlier.
7. In the *Email Verification Code* field, enter the verification code that you received at your email address.
8. Click *NEXT*.
9. Enter a password in the *PASSWORD* and *CONFIRM PASSWORD* fields.
10. Click *NEXT*.
11. Enter your information in the *FIRST NAME*, *LAST NAME*, *COMPANY*, *ADDRESS*, *COUNTRY*, *CITY*, and *PHONE* fields.
12. Click *SUBMIT*.
13. After you review the terms and conditions, select the checkbox, and click *Accept.*
14. Click *COMPLETE*.
15. Sign in with your new user name and password.
16. Review the terms and conditions and select the checkbox.
17. Click *ACCEPT.*

To create an IAM user:

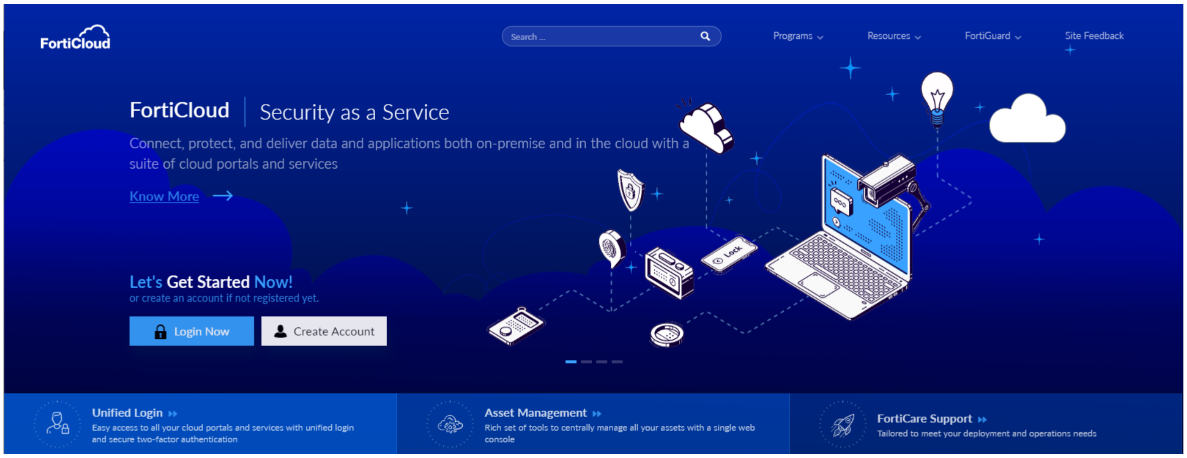
1. Log in to https://support.fortinet.com/.
2. Go to *Services* > *IAM*.



3. For more details, see https://docs.fortinet.com/document/forticloud/24.2.a/identity-access-management-iam/5478/adding-iam-users.

To register your license:

1. Log in to https://support.fortinet.com/.



FortiCloud | Security as a Service

Connect, protect, and deliver data and applications both on-premise and in the cloud with a suite of cloud portals and services

Let's Get Started Now!

or create an account if not registered yet.

Easy access to all your cloud portals and services with unified login and secure two-factor authentication

Rich set of tools to centrally manage all your assets with a single web console

Tailored to meet your deployment and operations needs

2. Go to *Products* and click *Register More*.
3. In the *Registration Code* field, enter your registration code.
4. Click *A government user* or *A non-government user*.
5. Click *Next*.
6. In the *Support Contract No.* field, enter your support contract number.
7. In the *Product Description* field, enter any notes about this license.
8. In the *Asset Permissions* dropdown list, select where to save your registration information.
9. Click *Next*.
10. Review the terms and conditions of the agreement, select the checkbox, and click *Next*.
11. Review your asset details, select the checkbox, and then click *Confirm*.

    The registration summary is displayed.
12. Click *Done*.

Resolved issues

The following issues have been fixed in FortiDevice 26.1.a. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1154509	A trial license should not be automatically activated when a new user logs in to the FortiDevice console with an account number.
1180527	When testing an external connector, the test result should show after 1 minute, instead of the test timing out.
1187103	A scan results in segmentation faults.
1187185	In the *Inventory > Devices* page, the IP address is not aligned with the MAC addresses.
1187419	Some Nmap Scripting Engine (NSE) scripts need to be modified.
1187769	In the *Inventory > Vulnerabilities* page, when selecting all statuses in a query, the server does not return vulnerabilities with all statuses.
1235962	When you create an OT task, there is an internal error.
1236128	A non-OT FortiGate task should not have OT traffic in the log.
1236467	“Scans” needs to be changed to “Tasks” in a couple of places in the GUI.
1236482	Going to the *Inventory > Devices* page causes an error.
1237591	The `inventory/device/ot/list` API endpoint does not support an IP query.
1237611	When selecting the level in the search query, “=” should be the only choice.
1237663	After selecting the site from the dropdown list and then switching to the *OT View* page, the site is not included in the query parameters.
1237671	Switching from one site to all sites does not refresh the displayed data.
1237723	When changing the task type between *OT* and *FortiGate*, the “For OT Environment” setting is not updated.
1237918	When a server has too many errors, FortiDevice will stop scanning before scanning everything specified.
1238057	The search query works with “Ot” but not with “OT”.
1238064	When the task type is *OT*, the database shows the task type as 5.
1238103	The `inventory/device/ot/list` API endpoint does not support a hardware vendor query.
1238377	When a device has a name in the *Topology* tab, the name is not displayed in the *Devices* tab.
1238530	When there is no host name in the *OT View*, the MAC address should be displayed.
1238550	The *Site ID* value is shown in the API response but not displayed in the GUI.

Bug ID	Description
1238628	After deleting 234 devices failed, the OPTIONS API request has a 403 response.
1239230	The *FortiGate* task type and the *OT* task type produce duplicate devices.
1239380	After going to the details page from the *Topology* tab, you should be able to return to the *Topology* tab.
1239389	The option to skip unresponsive hosts should always be selected for a Standard task.
1239406	There should be a vertical scroll bar for the *Device Details* pane.
1239968	Some of the OT traffic is not logged.
1239972	The *OT View* page displays a maximum of 100 devices.
1239975	The Reload button does not work.
1240097	On the *Devices* tab of the *OT View* page, the *EXPORT > Export CSV* command does not work.
1240327	There should not be a *SAVE QUERY* button on the *OT View* page.
1240343	“Scan” needs to be changed to “Task” for the *Notifications* pages.
1240396	Trying to select from the *Levels* dropdown menu on the *OT View* page does not work the first time.
1240408	“Scan” needs to be changed to “Task” in the *Add Task* dialog box.
1240719	“Scan” needs to be changed to “Task” in the *Detector Details* page.
1240720	The FortiDevice Detector build failed.
1240848	The device type of the OT device should be the same in the GUI and API.
1241052	The destination IP address and destination MAC address should be linked.
1241261	The *Levels* dropdown list on the *OT View* page is not working correctly.
1241469	“Scan” needs to be changed to “Task” in the Executive report.
1241928	The traffic log should include the Industrial category as a filter.
1242842	The vulnerability data in the FortiGate devices need to be shown in FortiDevice.
1243547	Users should be able to get logs from the */api/v2/log/fortianalyzer/traffic/forward* endpoint.
1243999	Scanning the same host multiple times causes false fixed vulnerabilities to be reported.
1244020	FortiDevice should be able to identify the camera device type.
1244502	The IoT vulnerabilities should have the same severity as in the FortiGate GUI.
1244516	When OT vulnerabilities are reported from a FortiGate device, errors are reported.
1244545	The number of vulnerabilities should be displayed on the *OT View* page.
1244601	The OT environment value differs on the *Inventory > Device* and *Inventory > Vulnerabilities* pages.
1245539	If the IP address changes for a device, the vulnerabilities should not be duplicated.

Known issues

The following known issues have been identified with FortiDevice 26.1.a. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
1025341	When the server browser is set to GMT X:30 or GMT X:45, the dashboard is not updating every hour at 00 minutes.
1134561	After deleting a detector and then copying a scan that used that detector, the *Detector* field in the *Copy Scan* field does not show other detectors.
1157368	When groups are synchronized from the LDAP server, a Microsoft Active Directory (AD) member is not included when the Microsoft AD member is a group.
1160612	In the *Paths* report, it is difficult to select a row in the *Source Asset* or *Destination Asset* table.
1164585	When the scan rate is set to moderate for one IP address, the scan times out and fails.
1164904	After deleting the detector in a scan and then copying the scan, no detectors are shown in the dropdown list.
1166105	There are no info icons on the *Users > Owners*, *Users > Owner Groups*, and *Users > Owner Sync* pages.
1166675	The *Notes* field should be under the Type field for adding, copying, and editing fabric connector and external Connector dialogs.
1179484	When you delete a Windows detector that was installed on an office PC, FortiEDR reports that it has “Blocked Credentials Access.”
1180301	In *Organization Information*, when the number of days in the *Stale Devices* field is less than the number of days in the *Devices going stale* field, the hyperlinks for the larger values should be 0.
1181820	The FortiCloud *Services* menu and *Support* menu needs to be updated.
1183491	If there are more than 3,000 expired accounts waiting to be purged, the system times out.
1183808	When a user removes a member of an organization, there is confirmation dialog before the user saves the change.
1184009	No trial contract should be generated for an IAM/Sub user in a viewer role who has no contract for this account.
1186923	After logging in to forticloud.com, selecting FortiDevice, and then logging out, the user is not redirected to the login portal.
1187827	The embedded JPEG image for a FortiDevice notification is not displaying in Gmail.
1189502	There is no switch information when using an SNMP credential.

Bug ID	Description
1240147	When the *Skip Unresponsive Hosts* checkbox is selected, the log only shows the arguments for one host .
1242919	Some devices are reported multiple times because they are discovered using different methods, and each method creates a separate entry.

www.fortinet.com