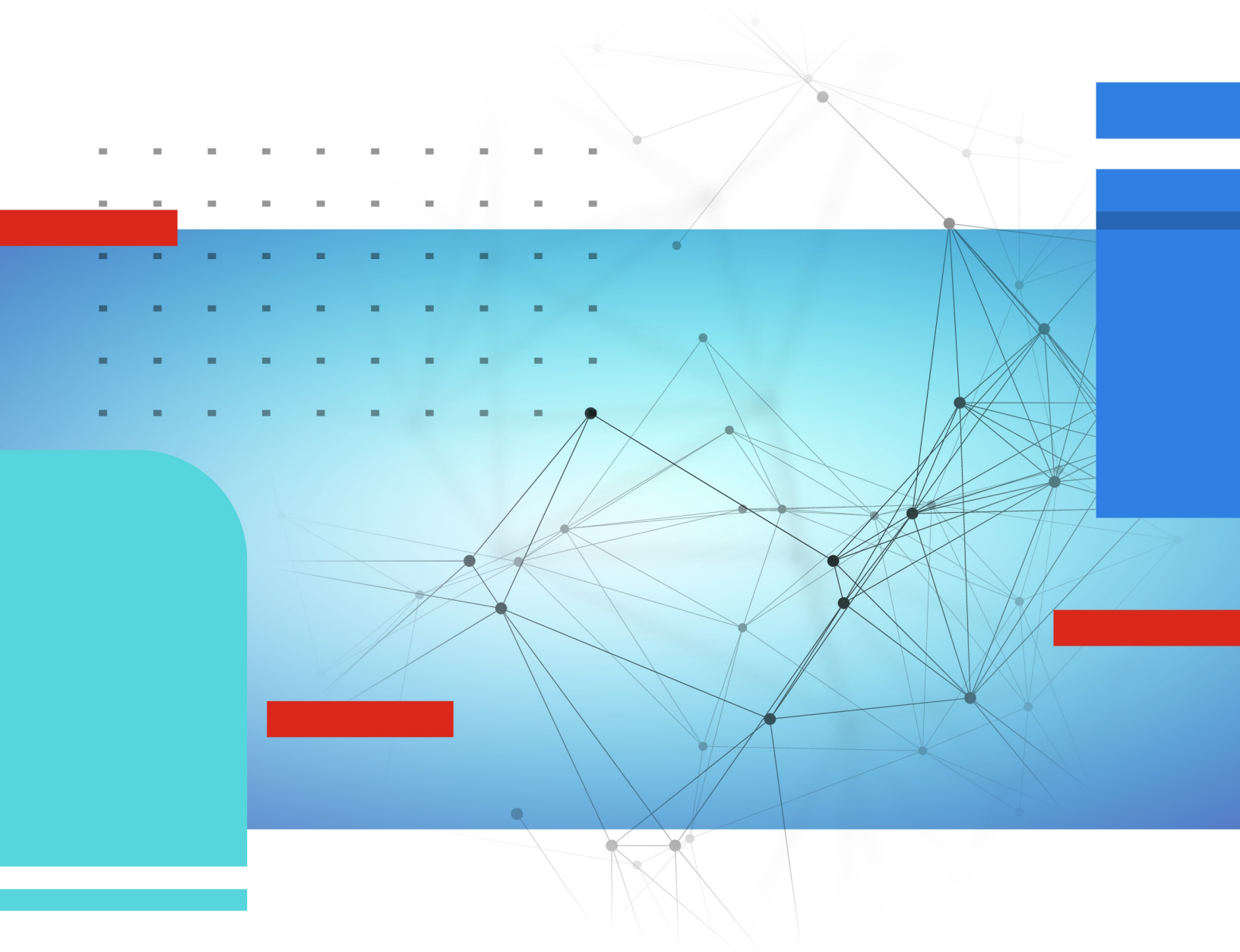
Release Notes

FortiDevice 25.2.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

June 25, 2025
FortiDevice 25.2.a Release Notes
97-252a-1149729-20250625

TABLE OF CONTENTS

Change log

Date	Change Description
June 25, 2025	Initial document release for FortiDevice 25.2.a

What's new in FortiDevice 25.2.a

Release 25.2.a provides the following new features:

- You can now identify Internet of Things (IoT) and Operational Technology (OT) devices by scanning a site with a FortiGate fabric connector. The scan provides such details as hardware family, hardware type, hardware vendor, and hardware version.
- You can now use FortiNAC to identify endpoint devices in the network and managed infrastructure devices by scanning a site with a FortiNAC fabric connector. The scan provides such details as the IPv4 or IPv6 address of the host, MAC address of the host, and operating system.
- You can use FortiDevice with FortiNAC to identify vulnerable devices and then select what action to take on the host.
- The *Inventory* > *Assets* page has been renamed. It is now the *Inventory* > *Devices* page.
- Microsoft Active Directory is now supported. After you add an external connector, FortiDevice can scan all of your Microsoft Active Directory users and groups.
- The Google G Suite (Google Workspace) is now supported. After you add an external connector, FortiDevice can scan all of your G Suite users and groups.
- You can now enable or disable out-of-bound (OOB) vulnerability scanning when you configure a standard scan.
- You can now have FortiDevice send admin users email reminders when your FortiDevice contract is expiring in the next 30 days. Admin users are also notified in the FortiDevice Cloud GUI.
- You can now have FortiDevice send admin users email reminders when devices are going to become stale in the next 30 days. Admin users are also notified in the FortiDevice Cloud GUI.
- You can now test your fabric connectors and external connectors to make certain they work before using them for scans.

Introduction

This document provides the following information for FortiDevice 25.2.a build 0155 and FortiDevice Detector 2.2.a build 0149:

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.

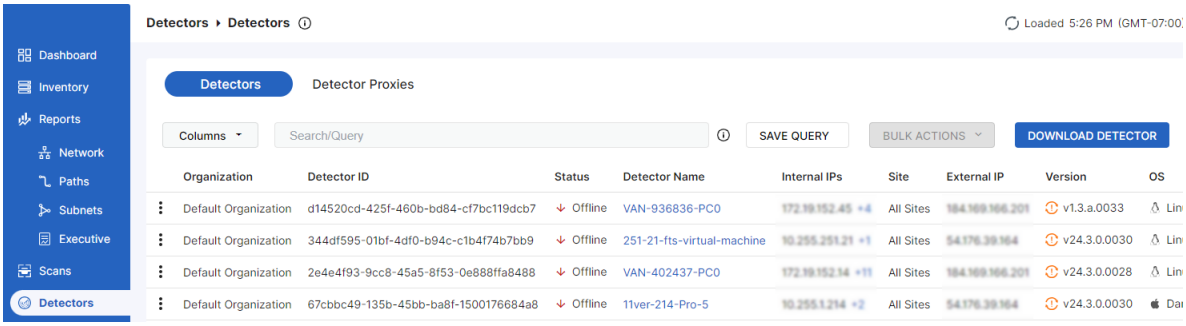
Upgrade information

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*.

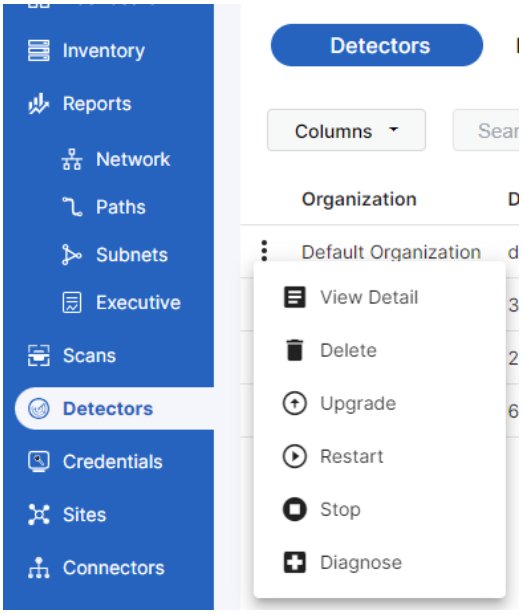


2. Click the ellipsis at the left end of the row of the Detector that you want to upgrade.

The Detector must be online.

---

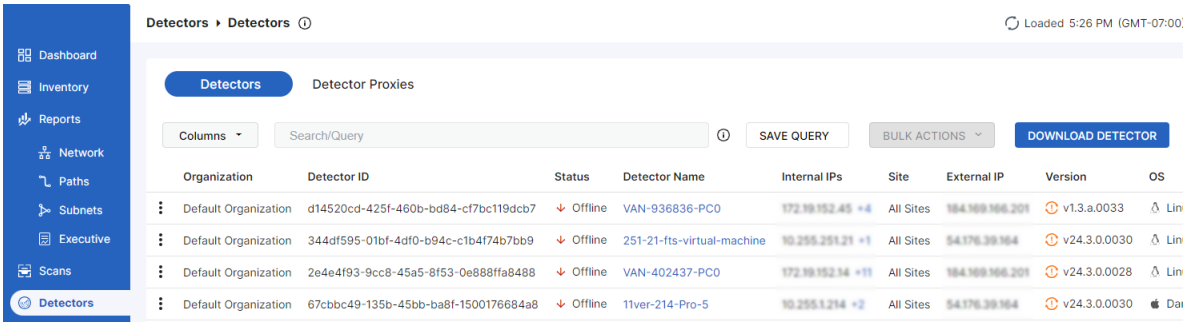
3. Select *Upgrade*.



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

To upgrade multiple FortiDevice Detectors:

1. Go to *Detectors*.



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

The Detectors must be online.

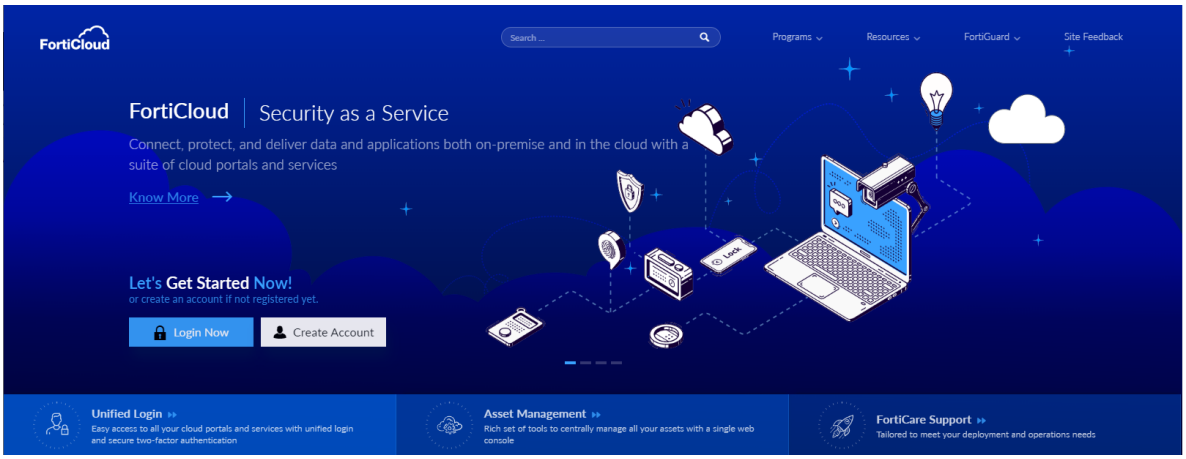
4. In the *Upgrade Detector?* dialog box, click *UPGRADE*.

Product integration and support

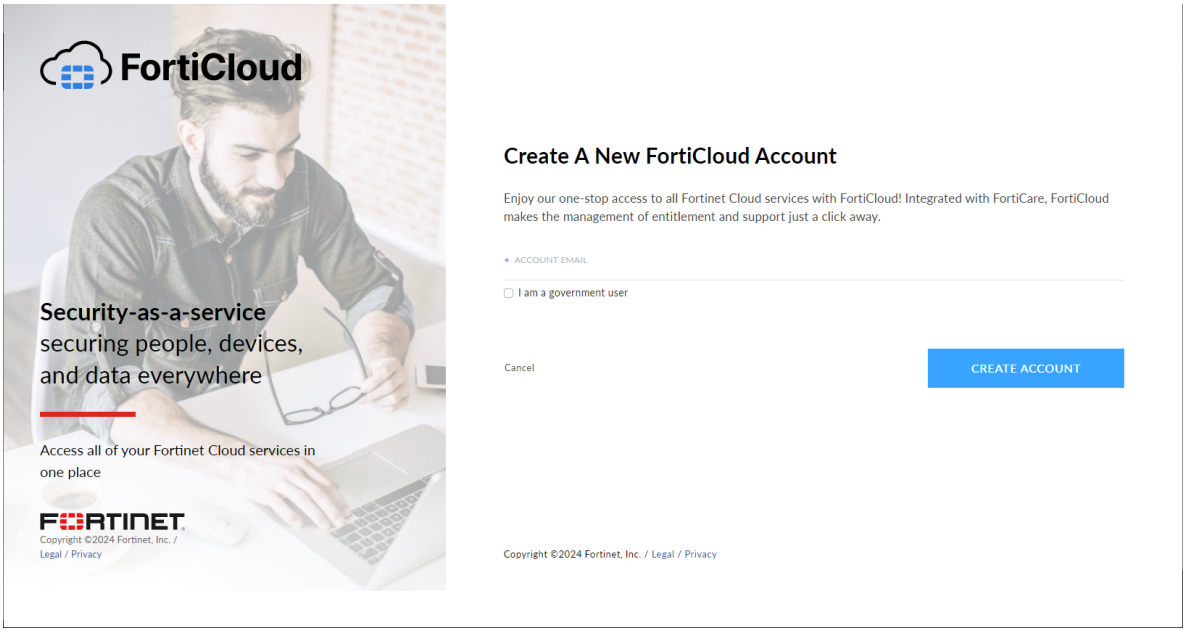
You need to create an account in the FortiCloud support portal, create an IAM user, and register your FortiDevice license.

To create an account:

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



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



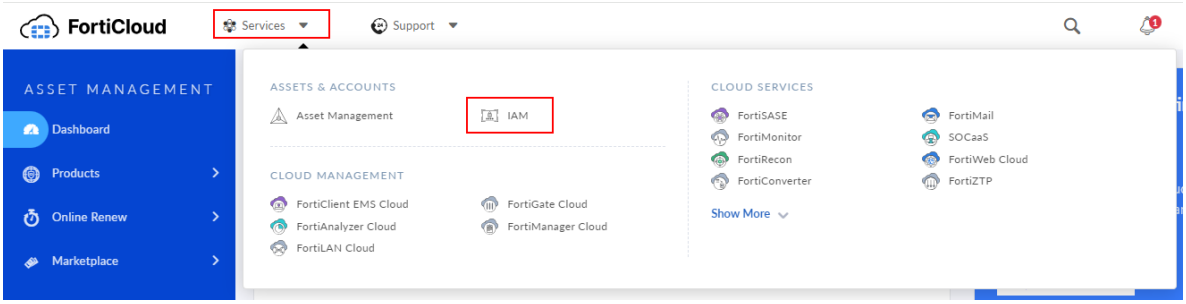
3. If you are a government user, select the *I am a government user* checkbox. Follow the steps in the dialog box if you are a U.S. Federal Government user or click *No, Just Proceed.*
4. If you are not a government user, enter your email address for your account and click *CREATE ACCOUNT*.
5. In the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

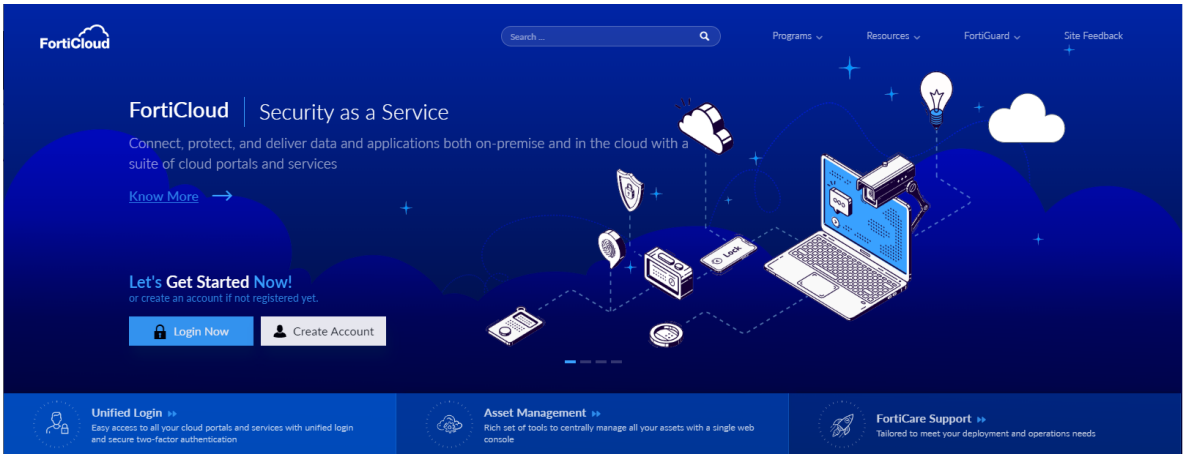
1. Log in to https://support.fortinet.com/.
2. Go to *Services* > *IAM*.



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/.



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 25.2.a. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1152649	There are no notifications to admin users before assets become stale.
1162158	There needs to be more information about vulnerabilities in the alerts.
1163268	Users need to be notified when a new release is available.
1165554	There needs to be an option to enable and disable out-of-bound (OOB) vulnerability scanning.
1167139	The connector/query REST API endpoint needs to support the Test Result query and the *Last Tested* field.
1168947	FortiDevice incorrectly reports that it has reached the provisioned limit for querying or organization updates.
1169190	When the vulnerability scan level is set to *None*, the GUI is not sending the parameter for OOB vulnerability scanning.
1169572	After deleting the data for the current hour, deleting a vulnerability, software, or a server might cause a dashboard server error.
1169842	When testing credentials, there should be a green icon to indicate connected IP addresses and a red icon to indicated failed IP addresses in the *Test Results* tab.
1169852	When FortiDevice scans vCenter, the VMs need to be grouped into the correct ESXi in the *Inventory* > *Devices* > *Device Details* page.
1170049	Sorting by site in the *IP Usage* tab of the *Subnets* report produces incorrect results.
1170142	When the *Show VMs with IP addresses as separate assets in the asset inventory and in the hypervisor asset details* checkbox is selected, all VMs should be created, even if the IP address for the VM device is not in the scan scope.
1170398	The detector status is sometimes wrong on the *Events* > *Events* page.
1170593	When the scan type is set to *Cloud*, all external connectors are listed when configuring a scan, instead of just the Cloud connectors.
1170705	There should be more information in the *Device Details* tab for FortiNAC devices.
1170742	When a FortiNAC scan uses an invalid connector, the status of the scan should be “failed.”
1171238	The hint for the *Password* field should be “Required.”
1171328	The background image for the FortiDevice notification should expand to the width of the email.
1171329	When testing a connector, there should be an indication that the test is in progress.
1172144	When a webhook channel is created or updated, empty headers should be allowed.

Bug ID	Description
1172155	The query details are not displayed after creating a query and then clicking on the query name.
1172184	After setting the number of days before stale devices are removed from the inventory in the *Add Organization* dialog, the value is not saved.
1172211	The notif/query REST API endpoint does not show the stale asset type.
1172246	Admin users should be notified about stale devices for their organization (s).
1172717	The *Change History tab is missing from the Inventory > Device >device Details page*
1173262	When a FortiGate fabric connector is used, the assets it discovers should be marked as IoT.

Known issues

The following known issues have been identified with FortiDevice 25.2.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.
1130206	Asset owners and asset group owners need to be listed separately on the *Asset Details* page and *Scan Details* page.
1134258	The *Specify owner for the scanned assets* field in the *Add Scan* dialog needs to support searching for multiple items (more than two) and selecting multiple items.
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.
1154509	A trial license should not be automatically activated when a new user logs in to the FortiDevice console with an account number.
1155603	FortiDevice stops responding when an owner is selected during adding or copying a scan when there are over 20,000 scan owners configured.
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.
1162129	The IP address range is not checked before the scan scope configuration is saved.
1162139	The *Export* button is not working in the *Devices* tab of the *Reports* > *Network* page.
1162153	The *Export* button is not working in the *Paths* tab of the *Reports* > *Paths* page.
1163865	When the credential type is SNMPv3, the value in the *Authentication Algorithm* and *Privacy Algorithm* fields cannot be changed in the *Add Credentials* dialog.
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.
1168714	If the user selects a site for a detector and then changes the site when adding a scan, the detector is no longer listed as available for the original site that the detector was selected for .
1170049	Filtering for a site does not work correctly on the *IP Usage* tab of the *Reports* > *Subnets* page
1171861	When there is no VM, the scan with ESXI credentials does not report network information.

Bug ID	Description
1171865	There is no note to warn users that the faster and fastest scan can use up network resources.

www.fortinet.com