

DrayTek

DrayTek Threat Protection
Introductie & Activatie



Inhoudsopgave

Threat Protection.....	3
Kernfunctionaliteiten	3
1. Router als toegangspoort.....	3
2. Netwerk- en apparaattoezicht	3
3. Bescherming van IoT- en onbeheerde apparaten	4
4. Veilig internetten en contentfiltering	4
Threat Protection licentie	5
Activeren licentie	6
Threat Protection inschakelen op de router.....	9
Beheren en monitoren via het gebruikersportaal	10

Threat Protection

Threat Protection biedt geavanceerde, gateway-gebaseerde beveiliging om netwerken en aangesloten apparaten te beschermen tegen voortdurend veranderende cyberdreigingen, door middel van intelligente verkeersanalyse en dreigingsdetectie aan de rand van het netwerk.

Kernfunctionaliteiten

1. Router als toegangspoort

De router vormt de toegangspoort tot uw bedrijfsnetwerk. Door de netwerkperimeter te versterken, voorkomt het systeem dat externe aanvallen uw bedrijfsactiviteiten verstoren.

Belangrijkste functies:

- Mitigatie van DoS-/DDoS-aanvallen
- Detectie van poortscans
- Bescherming tegen brute-force toegangspogingen



Waarde voor uw bedrijf:

- Maximaliseert de netwerkbeschikbaarheid en stabiliteit, zelfs tijdens actieve cyberaanvallen.

2. Netwerk- en apparaattoezicht

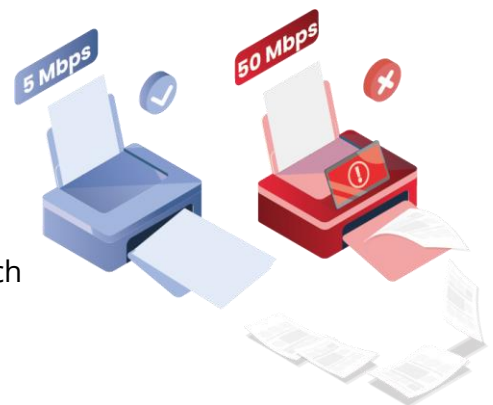
Zichtbaarheid is de eerste stap naar een veilige netwerkgeving. Het systeem ontdekt automatisch alle apparaten op uw LAN en monitort continu hun activiteit.

Belangrijkste functies:

- Continu toezicht op apparaatgebruik en automatisch identificeren van alle aangesloten hardware.

Directe reactie:

- Verdachte of gecompromitteerde apparaten worden automatisch gedetecteerd en geïsoleerd om te voorkomen dat bedreigingen zich lateraal binnen uw netwerk verspreiden.



3. Bescherming van IoT- en onbeheerde apparaten

Printers, IP-camera's en POS-systemen vormen vaak de zwakste schakels in uw netwerk, omdat zij geen antivirussoftware kunnen draaien. Het systeem biedt netwerkbescherming voor deze apparaten om risico's te minimaliseren.



Belangrijkste functies

- **Detectie van gedragsafwijkingen**
 - Identificeert abnormale patronen in IoT-verkeer om exploitatie- en injectieaanvallen te stoppen.
- **Waarde voor uw bedrijf**
 - Sluit de "IoT-kloof" door netwerkniveau-bescherming te bieden voor apparaten die zichzelf niet kunnen beschermen.

4. Veilig internetten en contentfiltering

Bescherm uw team tegen de gevaren van het internet met realtime evaluatie van websites en domeinen.

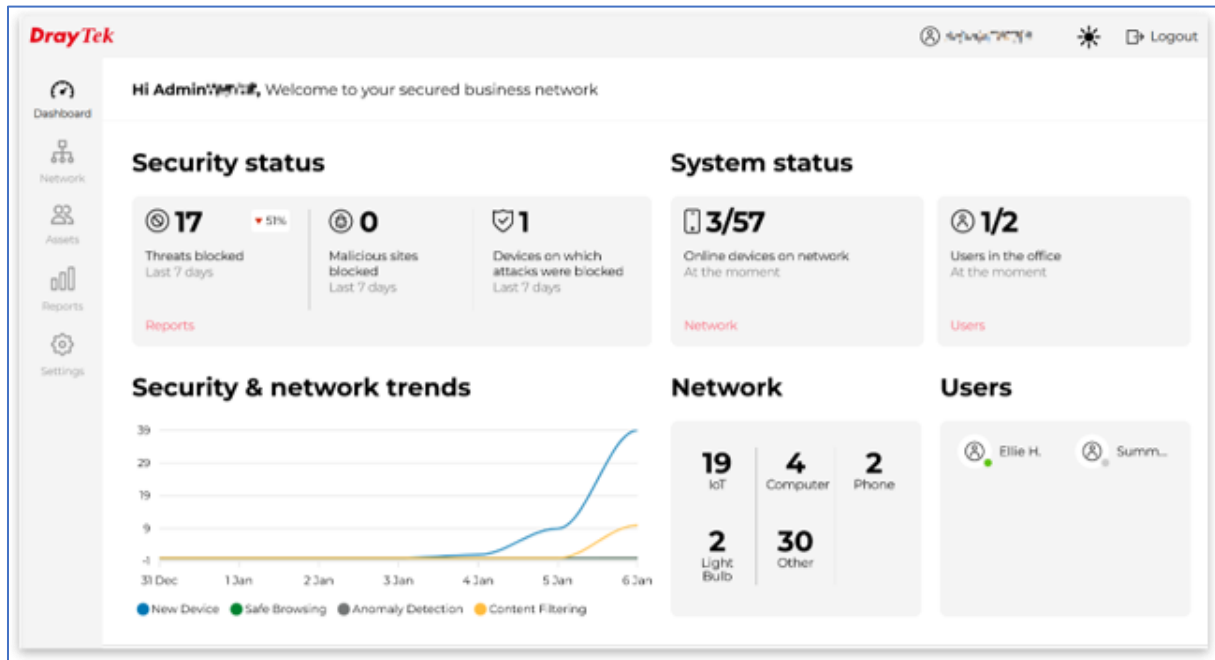
Belangrijkste functies

- **Blokkeren van bedreigingen**
 - Voorkomt toegang tot phishing-sites, malware-hosts, ransomware-commandocentra en botnet-servers.
- **Flexibele beleidsregels**
 - Handhaaf gebruiksregels door categorie gebaseerde filtering op gebruikers- of apparaatsniveau.



Threat Protection licentie

Om gebruik te kunnen maken van Threat Protection hebt u een licentie nodig welke u kunt aanvragen bij uw DrayTek partner/verkooppunt.



Threat Protection wordt aangeboden in twee licentieniveaus:

Sentry: Ontworpen voor thuis- en kleine kantooromgevingen.

Ondersteunde modellen: Vigor2136 & Vigor2767 serie

Firmware: 5.3.7 en hoger

Bescherming: tot 100 apparaten

Guardian: Ontworpen voor MKB- en grotere vestigingsnetwerken.

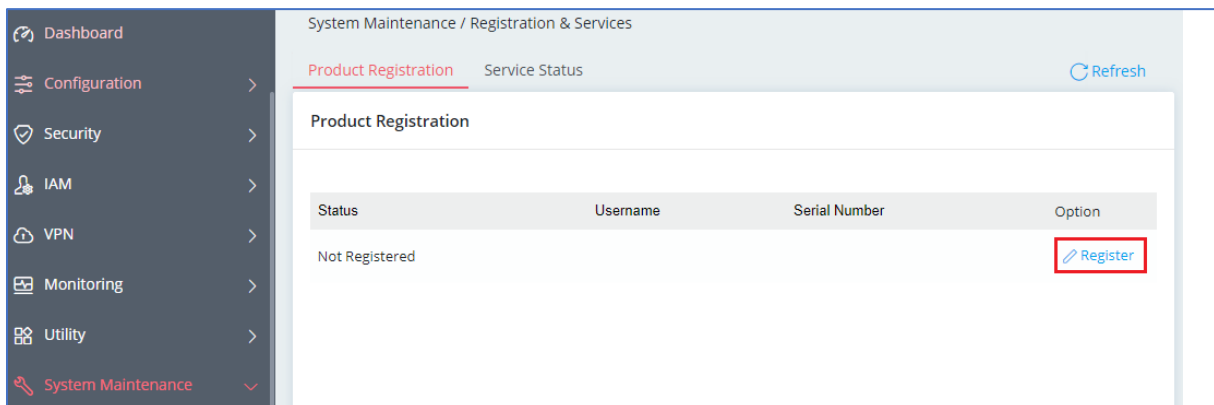
Ondersteunde modellen: Vigor2867 & Vigor2928 serie

Firmware: *future support**

Bescherming: tot 200 apparaten

Activeren licentie

Voor het activeren van de licentie is het noodzakelijk dat de router wordt geregistreerd bij de MyVigor-portal. Hiervoor kunt u in de WebUI van de DrayTek naar **System Maintenance > Registration & Services** gaan. Klik vervolgens op **Register** om de router aan uw MyVigor-account toe te voegen.



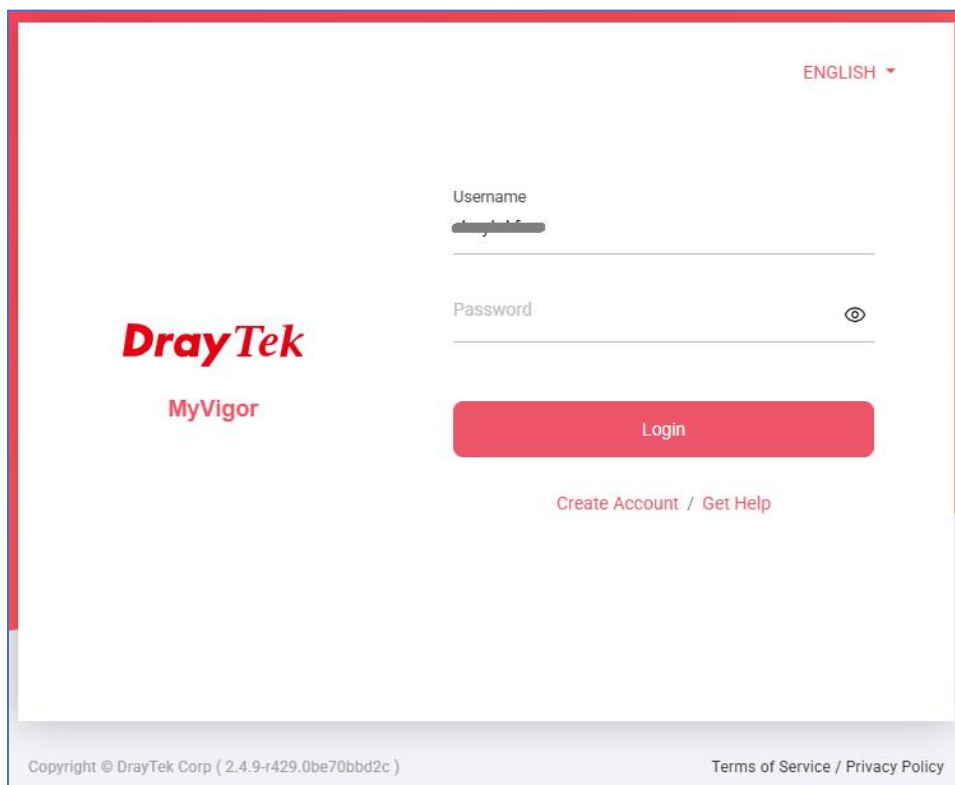
Indien u nog geen MyVigor-account heeft, kunt u hier tevens een nieuw account aanmaken.

Product register (Add Device)

Device Name	<input type="text" value="FAE_V2136"/>
Model	Vigor2136
MAC	1449BC39AF08
Serial Number	2023101315025101

[Cancel](#)

Ga naar System Maintenance / Registration & Services. In het tabblad Service Status klikt u op +Manage Licenses & Services. U wordt vervolgens doorgestuurd naar de MyVigor-inlogpagina, waar u dient in te loggen met uw MyVigor-account.



ENGLISH ▾

Username
[Redacted]

Password [Eye icon]

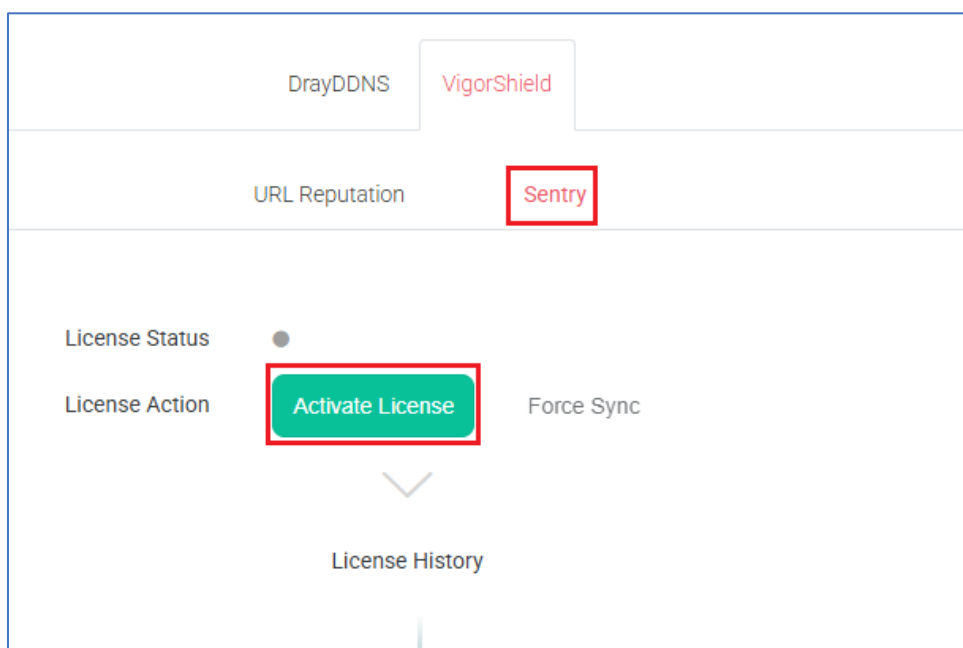
DrayTek
MyVigor

Login

[Create Account](#) / [Get Help](#)

Copyright © DrayTek Corp (2.4.9-r429.0be70bbd2c) [Terms of Service / Privacy Policy](#)

Ga in het tabblad VigorShield naar de optie Sentry of Guardian en klik op Activate License. Vervolgens krijgt u de voorwaarden van Sentry of Guardian te zien welke u dient te accepteren.



DrayDDNS VigorShield

URL Reputation **Sentry**

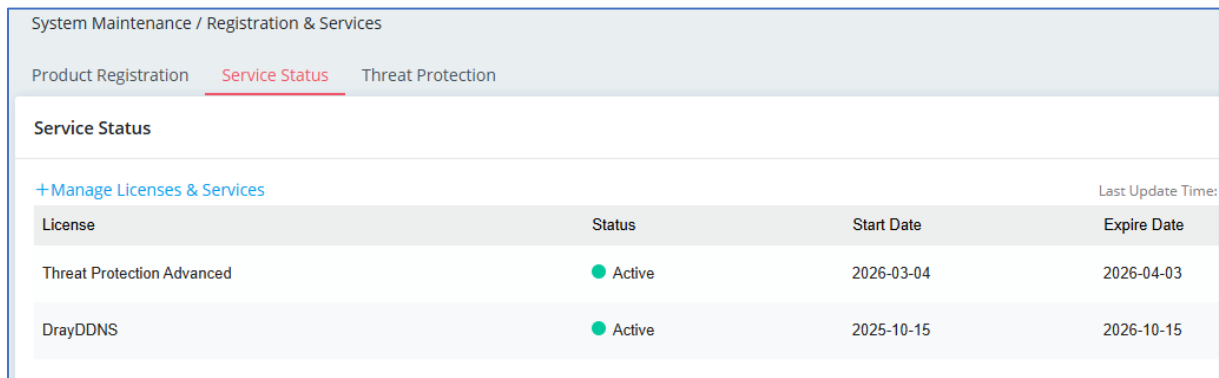
License Status ●

License Action **Activate License** Force Sync

License History

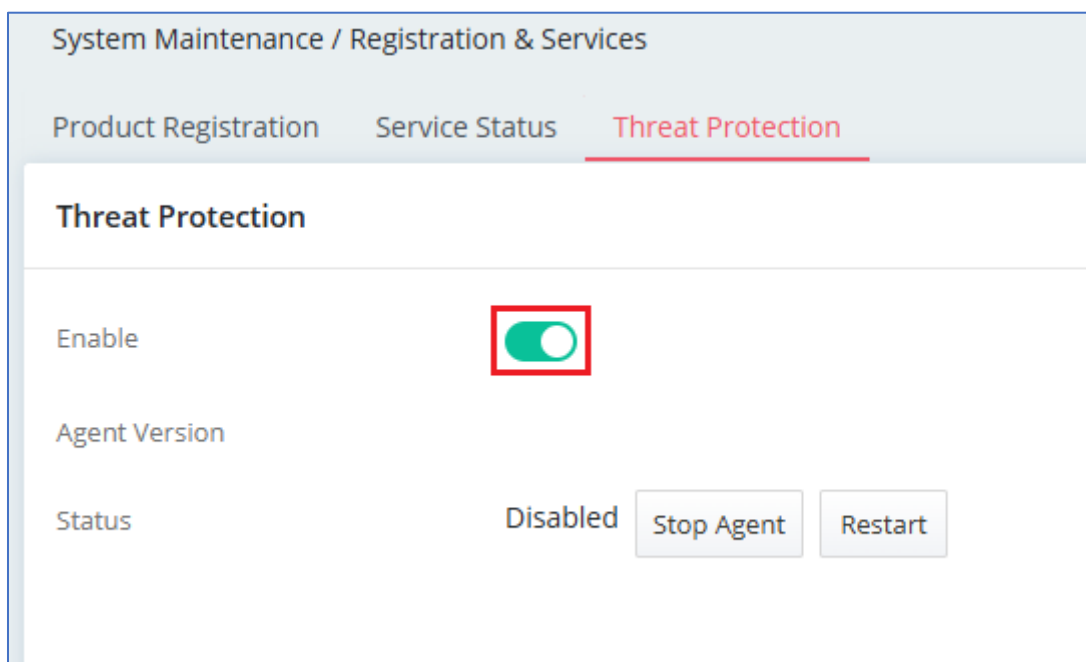
Threat Protection inschakelen op de router.

Na het activeren van de licentie dient deze ook zichtbaar te zijn onder System Maintenance > Registration & Services > Service Status.



System Maintenance / Registration & Services			
Product Registration <u>Service Status</u> Threat Protection			
Service Status			
+Manage Licenses & Services			Last Update Time:
License	Status	Start Date	Expire Date
Threat Protection Advanced	● Active	2026-03-04	2026-04-03
DrayDDNS	● Active	2025-10-15	2026-10-15

Inschakelen van de Threat Protection agent is mogelijk in het Threat Protection menu.



System Maintenance / Registration & Services

Product Registration Service Status Threat Protection

Threat Protection

Enable

Agent Version

Status Disabled Stop Agent Restart

Beheren en monitoren via het gebruikersportaal

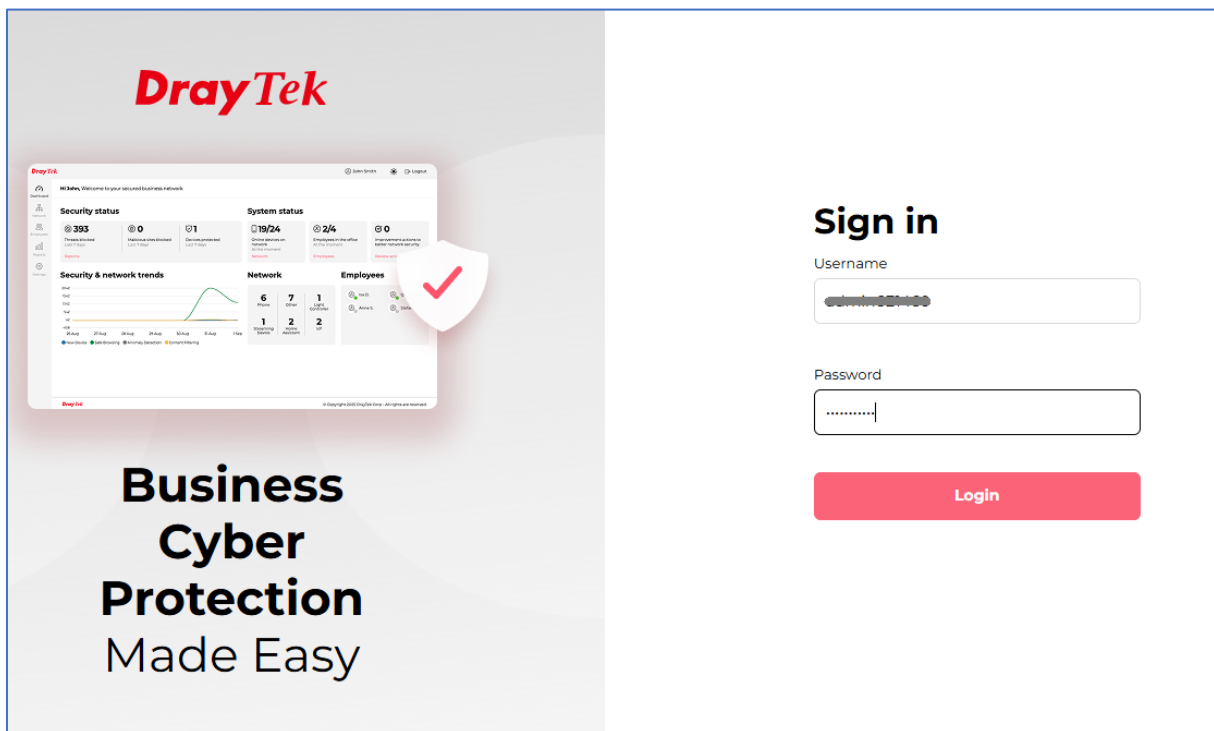
Threat Protection biedt een cloudgebaseerd gebruikersportaal waarmee u de apparaten op uw netwerk eenvoudig kunt beheren en monitoren.

Na het activeren van de licentie dient u contact op te nemen met de distributeur bij wie u de Threat Protection-licentie heeft aangeschaft. Zij verstrekken de accountgegevens die nodig zijn voor toegang tot het portaal.

Houd er rekening mee dat het tot één werkdag kan duren voordat het systeem het gebruikersaccount heeft aangemaakt nadat de licentie op de router is geactiveerd.

Wanneer u de accountgegevens heeft ontvangen, gaat u naar **vs.draytek.com** en logt U in met de verstrekte gegevens. Bij de eerste keer inloggen wordt u gevraagd uw wachtwoord te wijzigen om de beveiliging van uw account te waarborgen.

Zodra u bent ingelogd, kunt u uw apparaten beheren en monitoren via het portaal.



The image displays the DrayTek Business Cyber Protection user portal. On the left, a screenshot of the dashboard is shown with the DrayTek logo at the top. The dashboard includes sections for Security status (393), System status (19/24), Security & network trends (a line graph), Network (6), and Employees (7). A red checkmark icon is overlaid on the screenshot. Below the screenshot, the text "Business Cyber Protection Made Easy" is written in a large, bold font. On the right, a "Sign in" form is visible, featuring fields for "Username" and "Password", and a red "Login" button.

Voorbehoud

We behouden ons het recht voor om deze en andere documentatie te wijzigen zonder de verplichting gebruikers hiervan op de hoogte te stellen. Afbeeldingen en screenshots kunnen afwijken.

Copyright verklaring

© 2026 DrayTek

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand en/of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier zonder voorafgaande schriftelijke toestemming van de uitgever.

Ondanks alle aan de samenstelling van deze handleiding bestede zorg kan noch de fabrikant, noch de auteur, noch de distributeur aansprakelijkheid aanvaarden voor schade die het gevolg is van enige fout uit deze uitgave.

Trademarks

Alle merken en geregistreerde merken zijn eigendom van hun respectievelijke eigenaren.