



Website Traffic Control

User Manual for Beginners

Module: `oeasyai_website_traffic_control`
For Odoo Community

Written for people who have never used this module, and who may be new to Odoo.

Contents

1. What this module does
2. How to read this manual
3. Before you start (one-time setup)
4. Opening Traffic Control
5. The Dashboard
6. Monitoring: seeing who visits
7. Security: finding and blocking hostile visitors
8. Login protection
9. Reporting
- .0. Configuration
 - .1. Privacy and data retention
 - .2. What the module does on its own
 - .3. When something goes wrong
 - .4. Reference: roles, statuses and words

1. What this module does

Website Traffic Control gives you one place to answer five questions about your Odoo website and backend:

- **Who visits?** Every request that reaches Odoo is written down: the address (IP) it came from, the page asked for, the browser, the result.
- **From where?** Each address is placed on the map: country, region and city.
- **What do they look at?** Website pages for visitors; apps, menus and records for your own staff.
- **Who looks hostile?** The module watches for typical attack behaviour and gives each address a *threat score*.
- **How do I stop them?** You block an address, a range of addresses or a whole country. Password-guessing attacks on the login page are blocked automatically.

What it does not do

- It is **not** a firewall against very large floods of traffic. Odoo only sees a request after it has passed your web server (nginx). For that layer, the module can export a block list that nginx understands (chapter 7).
- It cannot see files that nginx serves directly without asking Odoo.
- It never stores a password, not even a wrong one.

2. How to read this manual

Chapters 3 and 10 are for the person who installs and configures the module (the administrator). Chapters 4 to 9 are for everyday use. If you only look at numbers, chapters 4, 5 and 9 are enough.

Words used in this manual

Word	Meaning
Click	Press the left mouse button once.
Menu path, e.g. Security > Suggestions	Click the first word in the top bar, then the second word in the list that opens.
List	A table of records, one per line.
Form	One record opened on its own page. Click a line of a list to open its form.
Field	A box you type in or choose from.
IP address (or "IP")	The number that identifies the computer or network a visitor comes from, for example 203.0.113.7 .
Request	One question a browser asks the server: "give me this page", "save this record".
Bot	A program, not a person, that visits your site: search engines, monitoring tools, and also attack tools.
Block	Refuse to answer a visitor. The visitor sees a short "Access denied" page.

The pictures were taken on a test database with sample traffic. Your own screen shows your own numbers, but the buttons are in the same places.

3. Before you start (one-time setup)

This chapter is for the administrator. Do these four things once.

3.1 Install the module

- 1 Open the **Apps** application.
- 2 In the search box type `Traffic Control`.
- 3 Click **Activate** on the card "Website Traffic Control".
- 4 Wait until the page reloads. A new application named **Traffic Control** appears in the applications menu.

The module needs the Website and Discuss applications; Odoo installs them for you if they are missing.

3.2 Give people a role

Nobody except the administrator sees the application until you give them a role. There are three roles, each one includes the one before it:

Role	Can see	Can do
Viewer	Dashboard and summary reports. No individual IP address.	Look only.
Analyst	Everything a Viewer sees, plus requests, IP profiles, login attempts, threat events and suggestions.	Mark a suggestion "Watch" or "Dismiss", write notes.
Manager	Everything.	Block, unblock, allow-list, edit rules, delete data, export, change settings.

- 1 Open **Settings > Users & Companies > Users**.
- 2 Click the person's name.
- 3 Find the line **Website Traffic Control** in the access rights and choose Viewer, Analyst or Manager.
- 4 Save. The person must reload their browser page to see the new application.

3.3 Check that Odoo sees the real visitor address

In most installations Odoo sits behind a web server called a reverse proxy (usually nginx). Unless Odoo is told so, every visitor appears to come from the proxy itself, typically `127.0.0.1`.

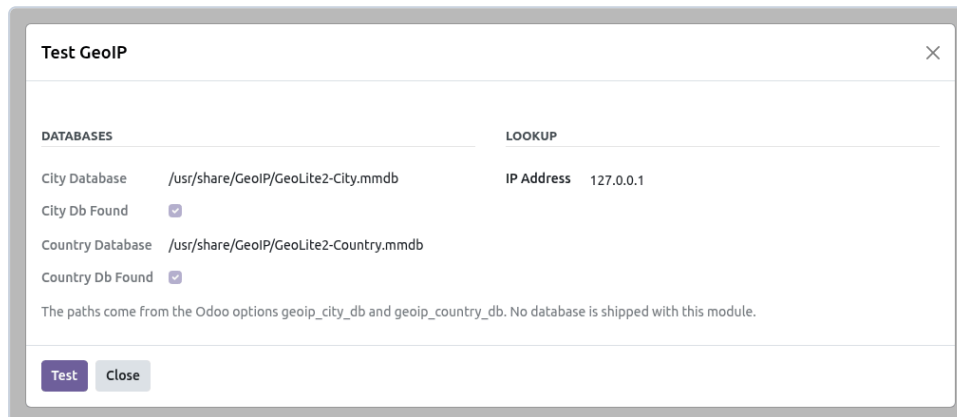
- In the Odoo configuration file, set `proxy_mode = True` and restart Odoo. Your server administrator does this.
- The dashboard shows the result at the bottom: **Proxy mode: detected** is what you want.

Safety net. While visitors appear with a private address such as `127.0.0.1` or `192.168.x.x`, the module refuses to block those addresses, because that would lock everybody out at once. See the setting "Also Block Private Addresses" in chapter 10.

3.4 Turn on locations (GeoIP)

Countries and cities come from a free database published by MaxMind (GeoLite2). The module does not include it.

- 1 Your server administrator downloads `GeoLite2-City.mmdb` and `GeoLite2-Country.mmdb` from MaxMind (a free account is required) and puts them on the server.
- 2 In the Odoo configuration file they set `geoip_city_db` and `geoip_country_db` to the paths of those two files, then restart Odoo.
- 3 You check the result: **Configuration** > **Settings**, block **Status**, click **Test GeoIP**, type an address such as `8.8.8.8` and click **Test**.



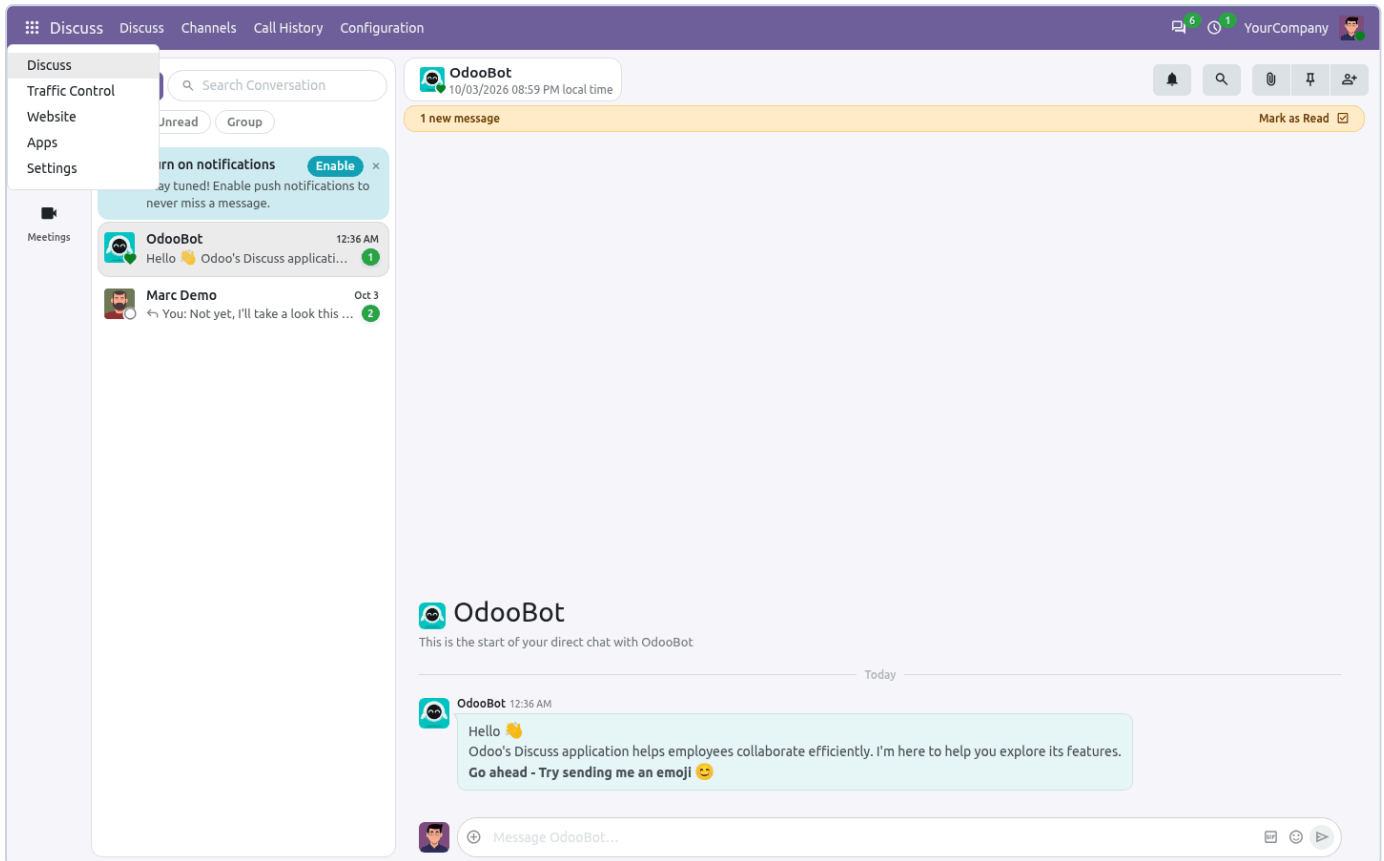
Test GeoIP: shows whether the database files are found and what they say about one address

The **Diagnosis** box of that window explains in plain words what is missing when it does not work. Once it works, click **Locate Existing IPs** to give a country to the addresses that were recorded before.

Without the database everything still works; only countries and cities stay empty, and the dashboard tells you "GeoIP database not configured".

4. Opening Traffic Control

- 1 Log in to Odoo.
- 2 Click the grid icon in the top-left corner. The list of applications opens.
- 3 Click **Traffic Control**.



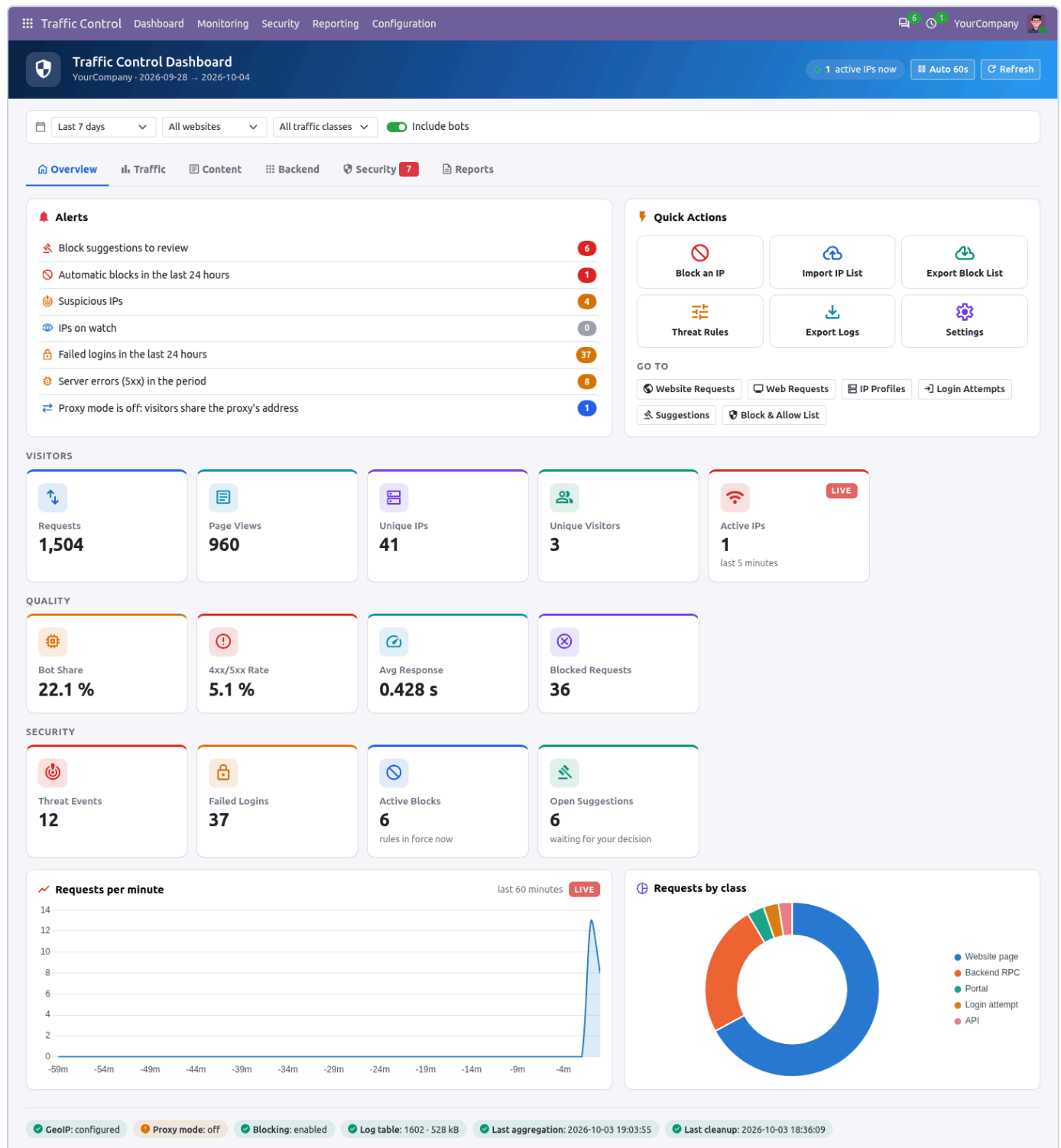
The applications menu with Traffic Control

The top bar now shows the five menus of the application:

Menu	What is inside
Dashboard	The overview screen (chapter 5).
Monitoring	Website Requests, Web Requests, IP Profiles, Backend Activity, Login Attempts (chapter 6). Analysts and Managers.
Security	Suggestions, Threat Events, Block & Allow List, and the block / import / export tools (chapter 7). Analysts and Managers.
Reporting	Ten analyses and three printable reports (chapter 9).
Configuration	Threat Rules, User Agents, Export Raw Logs, Purge Data, Settings (chapter 10). Managers only.

5. The Dashboard

Open it with **Dashboard**. It refreshes by itself every 60 seconds.



The dashboard, Overview tab

5.1 The blue band at the top

- **Company and period** currently shown.
- **Active IPs now:** how many different addresses sent a request in the last five minutes.
- **Auto 60s:** click to pause the automatic refresh; click again to resume.

- **Refresh:** reload the figures now.

5.2 The filter bar

These choices apply to every figure below them.

- **Period:** Today, Last 7 days, Last 30 days, or Custom period (two date boxes appear).
- **Website:** only shown when you have more than one website.
- **Traffic class:** website pages, backend, login, API and so on.
- **Include bots:** switch off to count people only.

5.3 Overview tab

Alerts

The list of things that need you. A grey 0 means nothing to do. Click a line to open the records behind it.

Alert	What to do
Block suggestions to review	Decide each one (chapter 7.2).
Automatic blocks in the last 24 hours	Look at who was blocked; nothing to do unless it was a mistake.
Suspicious IPs / IPs on watch	Open the profiles and judge.
Failed logins in the last 24 hours	A few are normal (typing mistakes). Many from one address is an attack.
Server errors (5xx) in the period	Tell your Odoo administrator: pages are failing.
GeoIP not configured / Proxy mode is off	Finish the setup of chapter 3.
Emergency switch on	Nothing is being blocked. See chapter 13.

Quick Actions

Large buttons for the most common jobs (Managers): Block an IP, Import IP List, Export Block List, Threat Rules, Export Logs, Settings. Under "Go to" are shortcuts to the lists.

The number tiles

Each tile shows one figure for the period. The small arrow in the corner compares it with the period just before (for example, yesterday when you look at today). Green is good news, red is bad news. Click a tile to see the details.

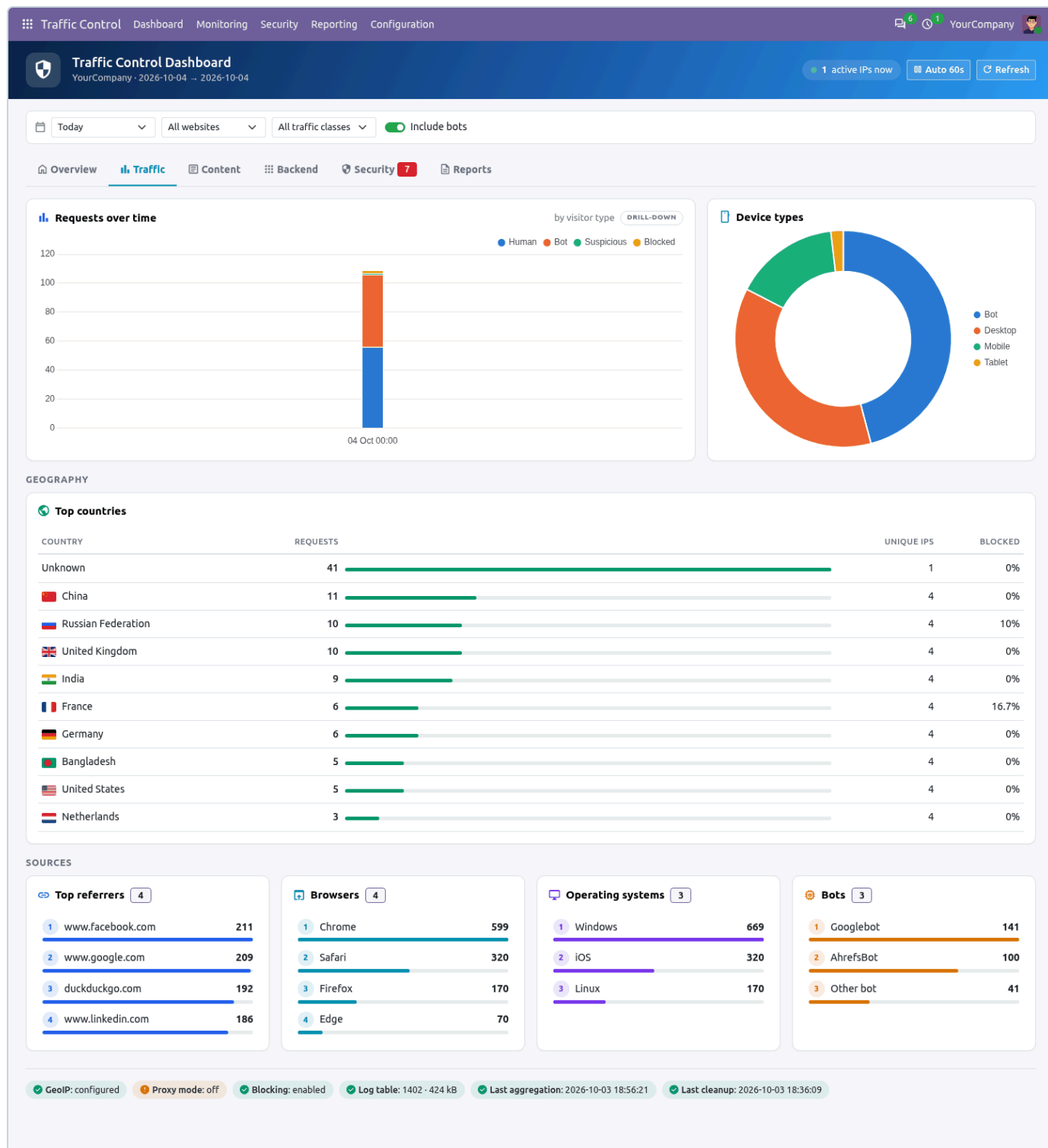
Tile	Meaning
Requests	How many requests reached Odoo.
Page Views	How many website pages were shown successfully.
Unique IPs	How many different addresses.
Unique Visitors	How many different website visitors, as counted by the Website application.
Active IPs (LIVE)	Addresses seen in the last five minutes.
Bot Share	Percentage of requests made by bots.
4xx/5xx Rate	Percentage of requests that ended in an error ("not found", "forbidden", "server error").
Avg Response	Average time Odoo needed to answer, in seconds. 0.250 s is a quarter of a second.
Blocked Requests	Requests refused by a block rule.
Threat Events	How many times a threat rule was triggered.
Failed Logins	Wrong login attempts.
Active Blocks	Block rules in force right now.
Open Suggestions	Suggestions waiting for your decision.

The two charts

- **Requests per minute:** the last 60 minutes, live.
- **Requests by class:** what share is website pages, backend, login and so on.

5.4 Traffic tab

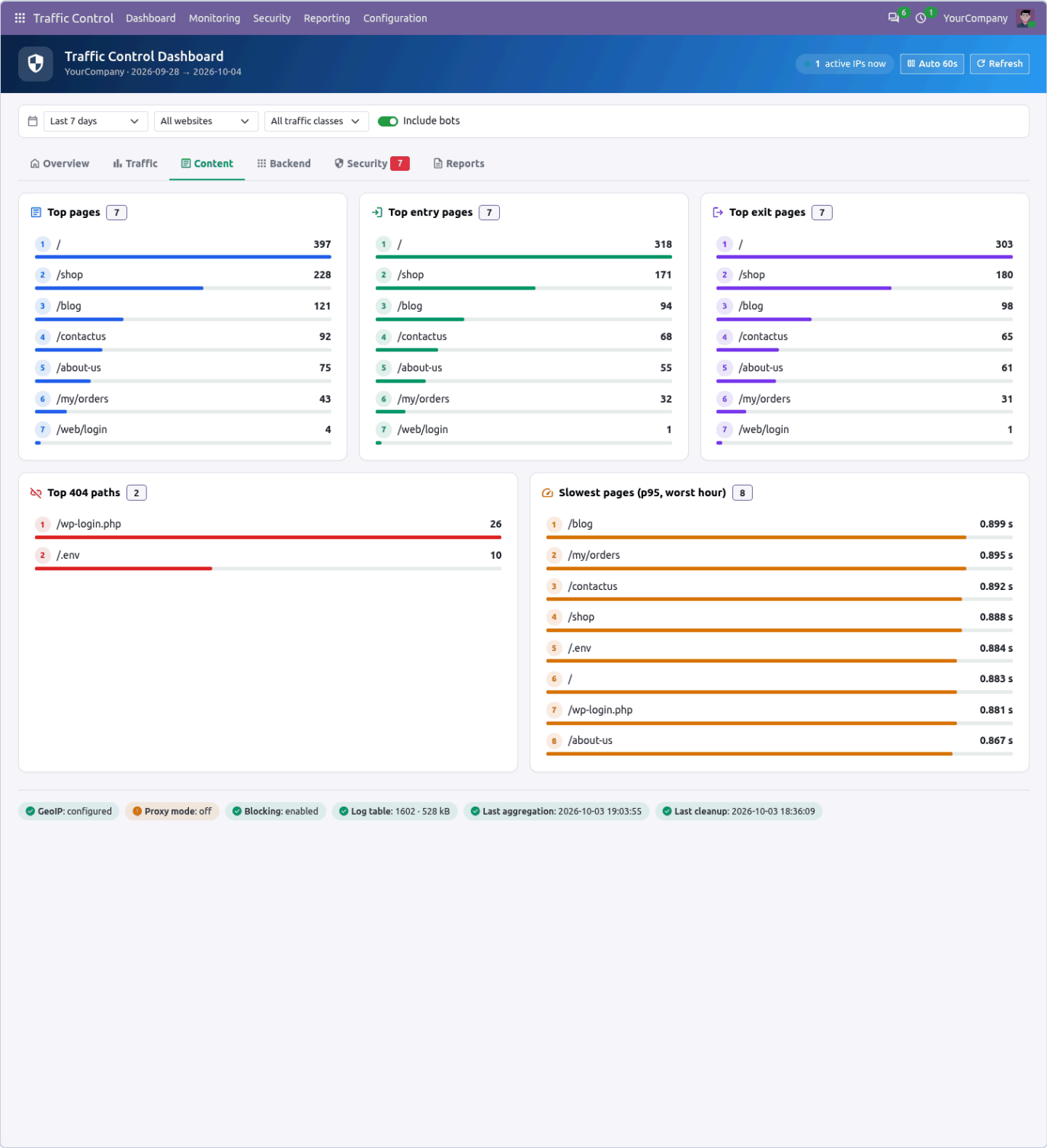
Requests over time split into Human, Bot, Suspicious and Blocked; device types; the top countries with flags; and where visitors come from (referrers), their browsers, operating systems and the bots.



Traffic tab

5.5 Content tab

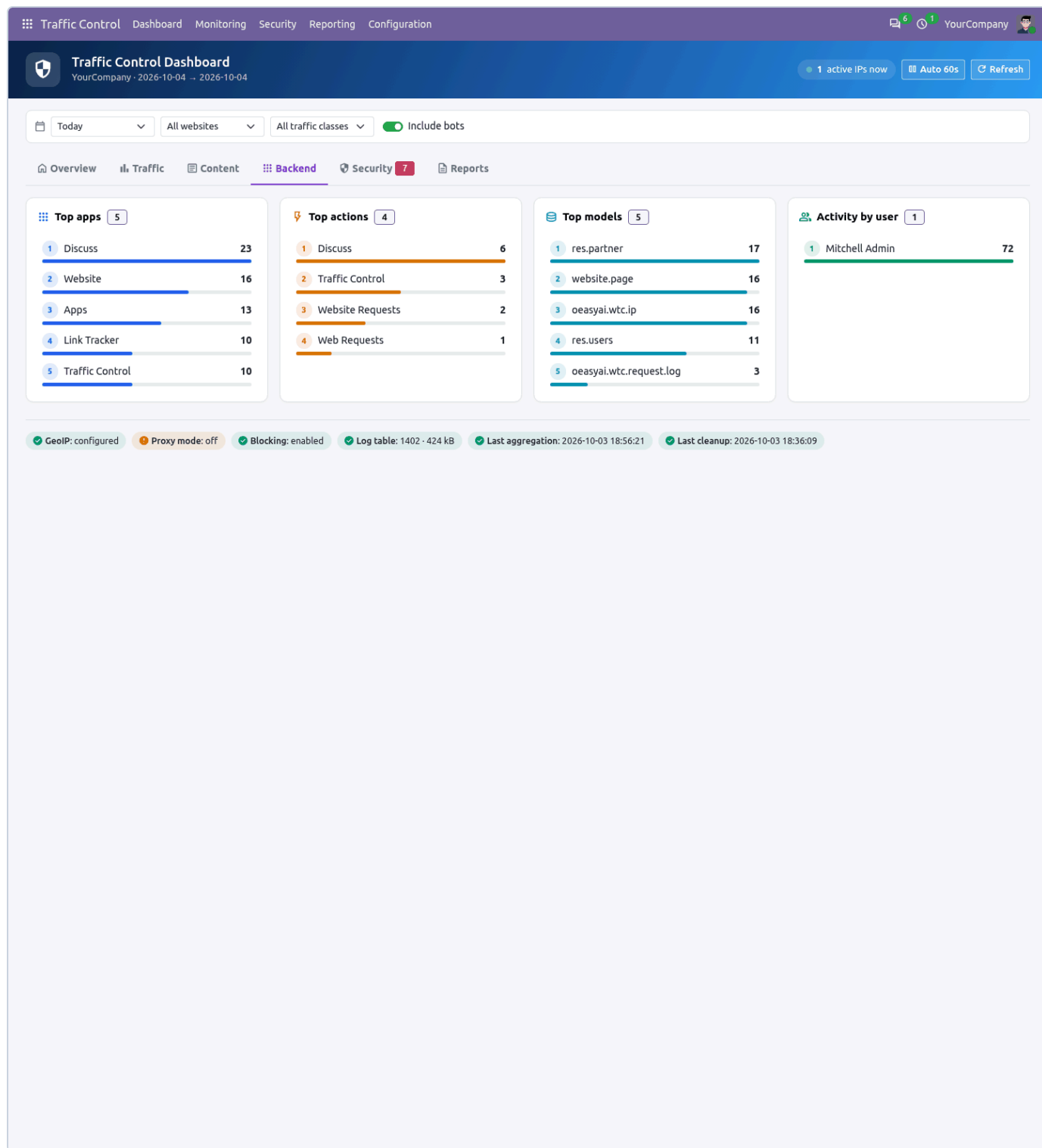
Top pages, the pages visitors arrive on (entry pages) and leave from (exit pages), the addresses that were asked for but do not exist (404), and the slowest pages. Click a line to open the analysis for that page.



Content tab

5.6 Backend tab

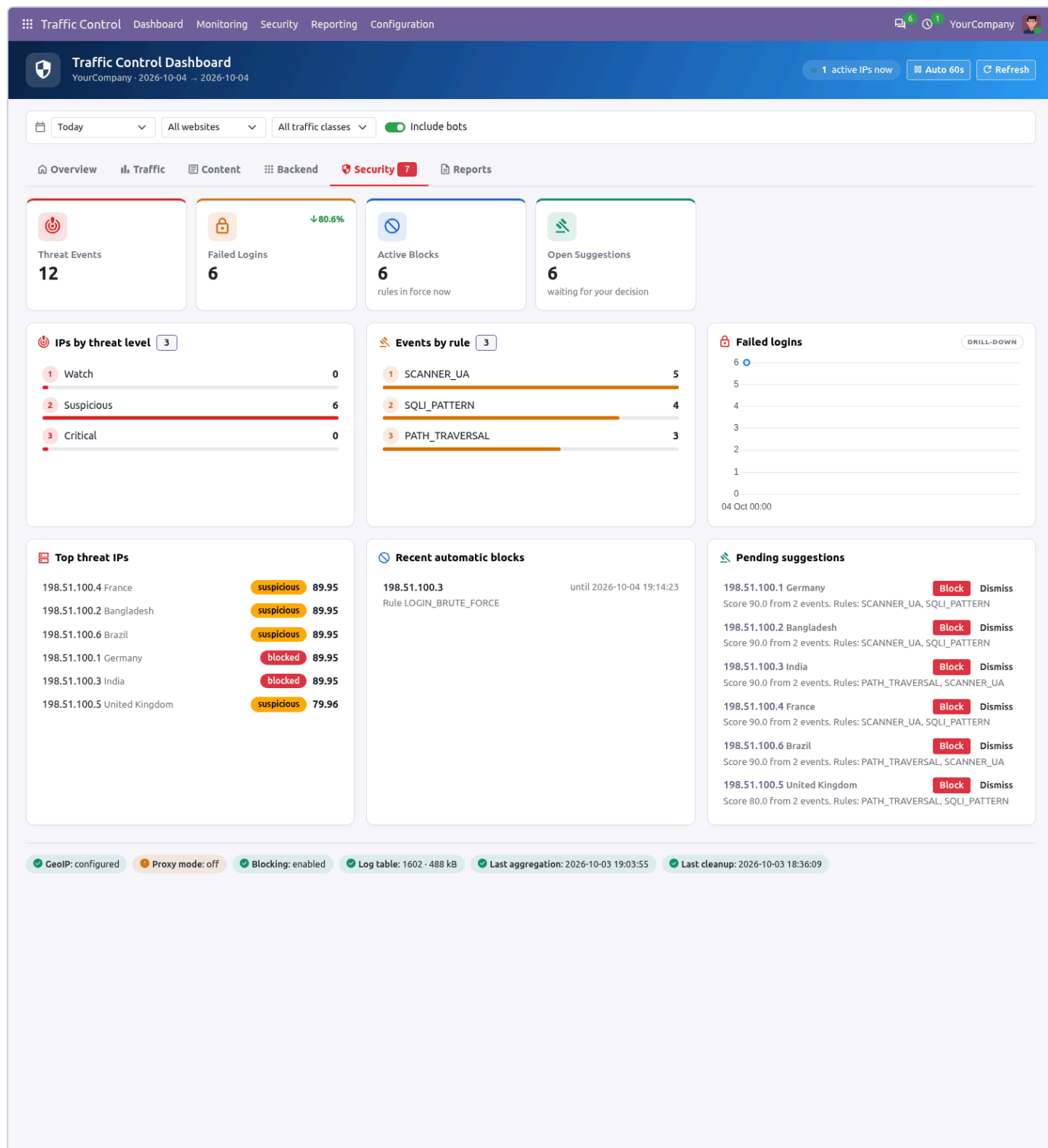
What your own staff use inside Odoo: the applications, actions and models opened most, and activity per user.



Backend tab

5.7 Security tab

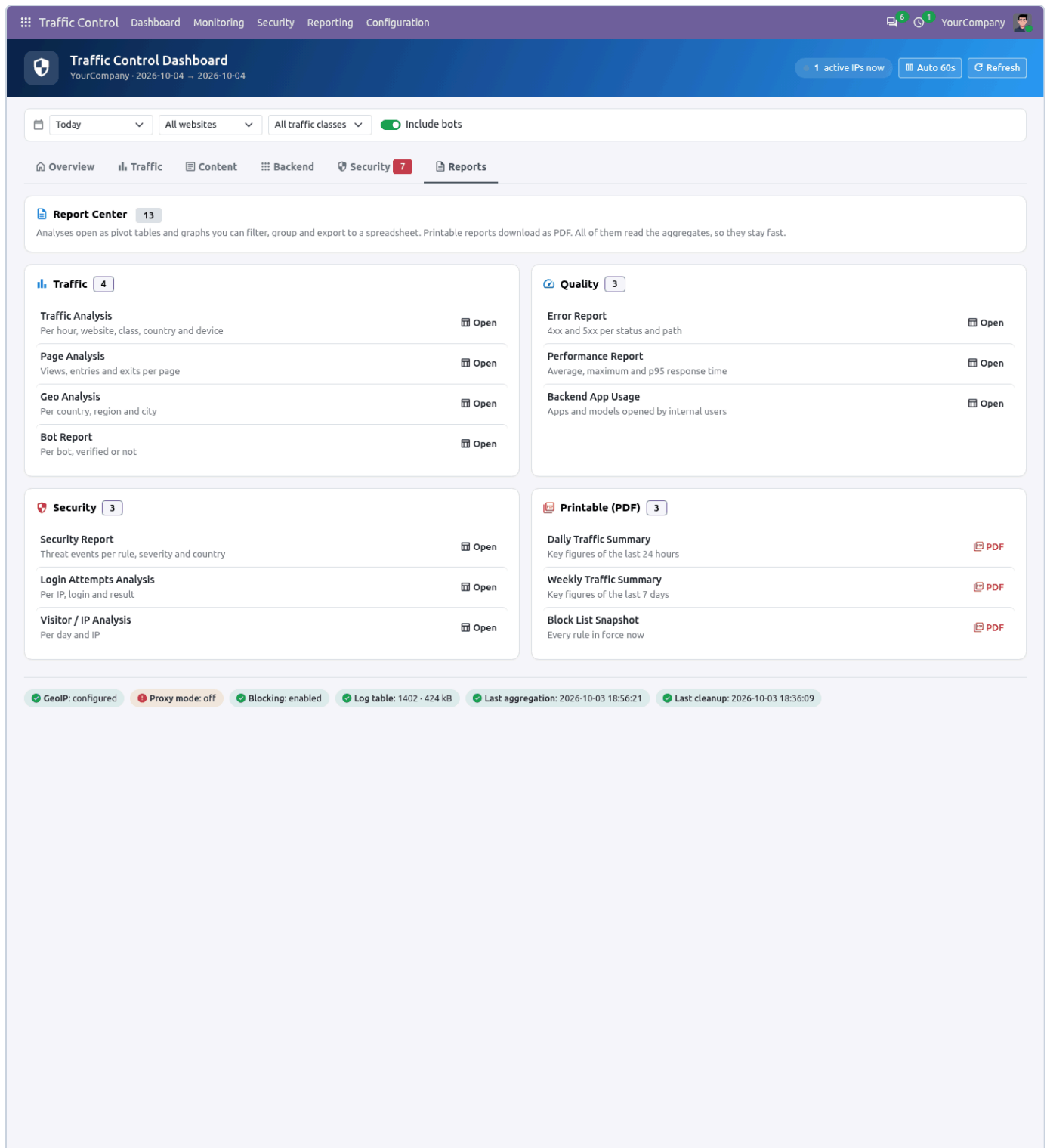
The security tiles, how many addresses are at each threat level, which rules fired most, failed logins over time and, for Analysts and Managers, three lists: the most threatening addresses, the latest automatic blocks, and the suggestions waiting. On each suggestion a Manager can click **Block** (blocks for 24 hours) or **Dismiss** directly.



Security tab

5.8 Reports tab

Every analysis and printable report in one place. Click a line to open it.



Reports tab (Report Center)

5.9 The status line at the bottom

Small labels that tell you whether the module itself is healthy: GeoIP, Proxy mode, Blocking, the size of the log, and when the figures were last calculated and cleaned. An orange label needs attention.

The dashboard figures are calculated every 15 minutes from the raw log. A request made one minute ago appears in the "Requests per minute" chart at once, but in the tiles only after the next calculation.

6. Monitoring: seeing who visits

This menu is for Analysts and Managers.

6.1 Website Requests

Monitoring > Website Requests lists what visitors asked of your website: pages, website forms and the customer portal. The list opens on today's requests; remove the "Today" label in the search box to see older ones.

Traffic Control Dashboard Monitoring Security Reporting Configuration											
Website Requests											
Search...											
1-80 / 1056											
Date	IP	Country	Request	Method	Technical Path	Status	Duration (s)	Class	User	Blocked	Suspicious
Oct 4, 12:58 AM	127.0.0.1		Login page	GET	/web/login	200	1.146	Website page			
Oct 4, 12:55 AM	127.0.0.1		Login page	GET	/web/login	200	1.017	Website page			
Oct 4, 12:37 AM	127.0.0.1		Login page	GET	/web/login	200	0.902	Website page			
Oct 4, 12:35 AM	127.0.0.1		Login page	GET	/web/login	200	0.884	Website page			
Oct 4, 12:34 AM	198.51.100.17	China	/shop	GET	/shop	200	0.160	Website page			
Oct 4, 12:32 AM	198.51.100.7	China	/shop	GET	/shop	200	0.750	Website page			
Oct 4, 12:31 AM	198.51.100.23	India	Page: Home	GET	/	200	0.069	Website page			
Oct 4, 12:30 AM	198.51.100.6	Brazil	/shop	GET	/shop	200	0.405	Website page			
Oct 4, 12:30 AM	198.51.100.12	Bangladesh	Page: Home	GET	/	200	0.197	Website page			
Oct 4, 12:29 AM	198.51.100.4	France	/shop	GET	/shop	200	0.113	Website page			
Oct 4, 12:29 AM	198.51.100.31	Germany	Page: Home	GET	/	200	0.129	Website page			
Oct 4, 12:28 AM	198.51.100.3	India	/blog	GET	/blog	200	0.382	Website page			
Oct 4, 12:28 AM	198.51.100.28	Russian Federation	/shop	GET	/shop	200	0.860	Website page			
Oct 4, 12:28 AM	198.51.100.7	China	Page: Home	GET	/	200	0.378	Website page			
Oct 4, 12:28 AM	198.51.100.19	Netherlands	/shop	GET	/shop	200	0.230	Website page			
Oct 4, 12:27 AM	198.51.100.4	France	Page: Contact Us	GET	/contactus	200	0.398	Website page			
Oct 4, 12:25 AM	198.51.100.10	United States	Page: Home	GET	/	200	0.372	Website page			
Oct 4, 12:25 AM	198.51.100.22	Bangladesh	/blog	GET	/blog	200	0.427	Website page			
Oct 4, 12:25 AM	198.51.100.25	United Kingdom	/blog	GET	/blog	200	0.845	Website page			

Website Requests

Column	Meaning
Date	When the request arrived.
IP, Country	Where it came from.
Request	What was asked, in plain words: "Page: Contact Us", "Login page". When the module does not recognise the address, the address itself is shown.
Technical Path	The exact address asked for, as the server saw it.
Status	The answer code: 200 = fine, 404 = not found, 403 = refused, 429 = too many requests, 500 = server error.
Duration (s)	How long Odoo took to answer, in seconds.
Class	The kind of request.
Blocked / Suspicious	Ticked when a block rule refused it, or a threat rule matched it.

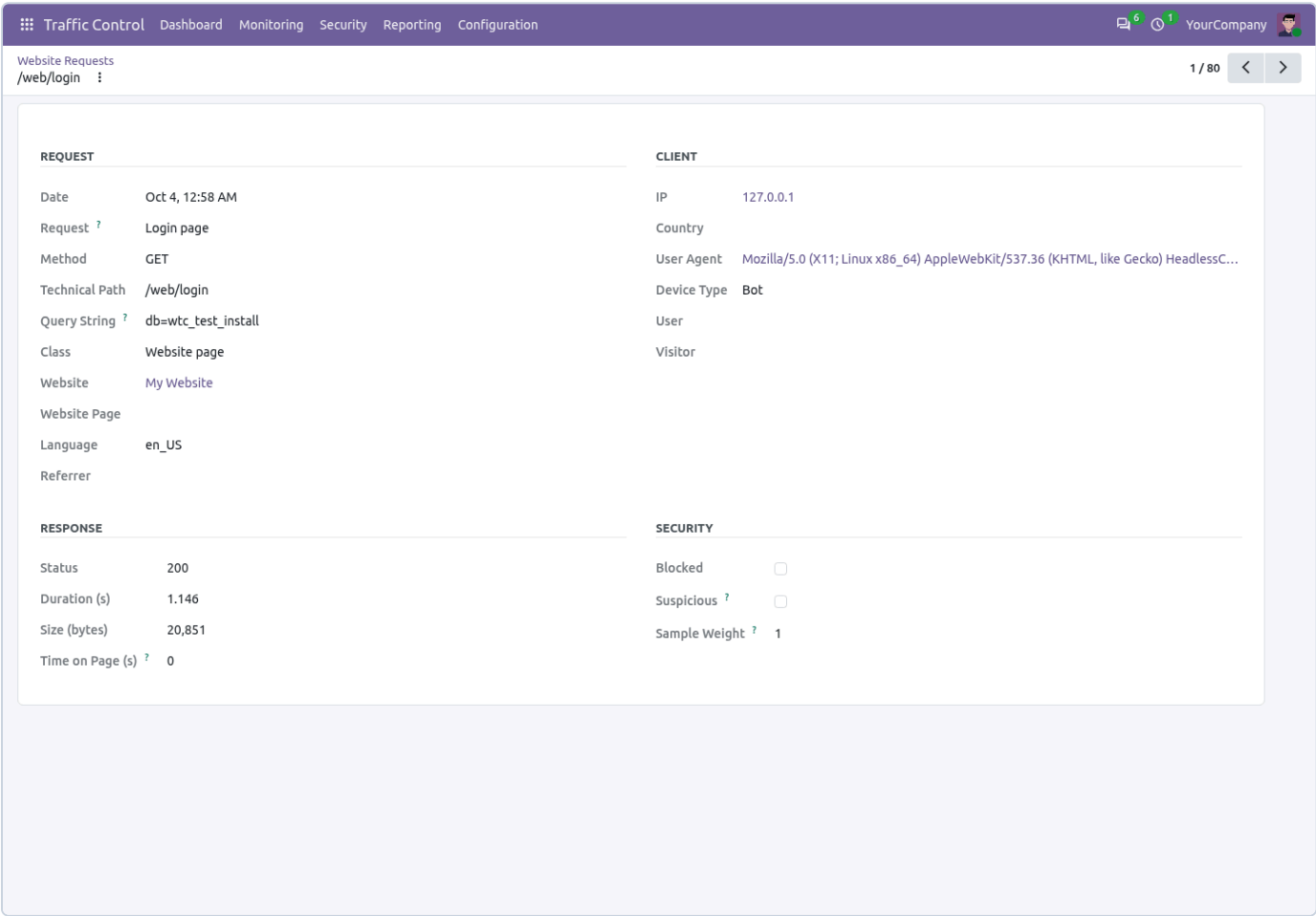
Line colours: **red** = blocked, **orange** = suspicious, **grey** = ended in an error.

Finding things

- 1 Click in the search box at the top.
- 2 Type part of a path or an IP address and press Enter, or click the small arrow at the right of the box to choose a ready-made filter (Blocked, Suspicious, Errors, 404...) or a grouping (by IP, by Path, by Status...).

Opening one request

Click a line. The form shows everything recorded about that request, including the browser and the page it was linked from.



One request opened

6.2 Web Requests

Monitoring > Web Requests is the same list for everything that is not the public website: what the Odoo backend does while your staff work, login attempts, and other programs talking to Odoo (API).

Traffic Control Dashboard Monitoring Security Reporting Configuration										6 1 YourCompany	
Web Requests										1-80 / 420	
☐	Date	IP	Country	Request	Method	Technical Path	Status	Duration (s)	Class	User	B. S...
☐	Oct 4, 1:00 AM	127.0.0.1		Traffic Control Request ...	POST	/web/dataset/call_kw/oeasyai.wtc.request.lo...	200	0.023	Backend R...	Mitchell A...	☐
☐	Oct 4, 1:00 AM	127.0.0.1		Traffic Control Request ...	POST	/web/dataset/call_kw/oeasyai.wtc.request.lo...	200	0.007	Backend R...	Mitchell A...	☐
☐	Oct 4, 1:00 AM	127.0.0.1		Open a menu or action	POST	/web/action/load	200	0.014	Backend R...	Mitchell A...	☐
☐	Oct 4, 1:00 AM	127.0.0.1		Backend	GET	/odoo/action-oeasyai_website_traffic_control...	200	0.090	Backend R...	Mitchell A...	☐
☐	Oct 4, 1:00 AM	127.0.0.1		Traffic Control Request ...	POST	/web/dataset/call_kw/oeasyai.wtc.request.lo...	200	0.005	Backend R...	Mitchell A...	☐
☐	Oct 4, 1:00 AM	127.0.0.1		Traffic Control Request ...	POST	/web/dataset/call_kw/oeasyai.wtc.request.lo...	200	0.012	Backend R...	Mitchell A...	☐
☐	Oct 4, 1:00 AM	127.0.0.1		Traffic Control Request ...	POST	/web/dataset/call_kw/oeasyai.wtc.request.lo...	200	0.010	Backend R...	Mitchell A...	☐
☐	Oct 4, 1:00 AM	127.0.0.1		Traffic Control Request ...	POST	/web/dataset/call_kw/oeasyai.wtc.request.lo...	200	0.036	Backend R...	Mitchell A...	☐
☐	Oct 4, 1:00 AM	127.0.0.1		Open a menu or action	POST	/web/action/load	200	0.022	Backend R...	Mitchell A...	☐
☐	Oct 4, 1:00 AM	127.0.0.1		Backend	GET	/odoo/action-oeasyai_website_traffic_control...	200	0.020	Backend R...	Mitchell A...	☐
☐	Oct 4, 12:59 AM	127.0.0.1		Scripts and styles	GET	/web/bundle/web.chartjs_lib	200	0.001	Backend R...	Mitchell A...	☐
☐	Oct 4, 12:59 AM	127.0.0.1		Traffic Control Dashboa...	POST	/web/dataset/call_kw/oeasyai.wtc.dashboard...	200	0.075	Backend R...	Mitchell A...	☐
☐	Oct 4, 12:59 AM	127.0.0.1		Open a menu or action	POST	/web/action/load	200	0.009	Backend R...	Mitchell A...	☐
☐	Oct 4, 12:59 AM	127.0.0.1		Backend	GET	/odoo/action-oeasyai_website_traffic_control...	200	0.014	Backend R...	Mitchell A...	☐
☐	Oct 4, 12:59 AM	127.0.0.1		Scripts and styles	GET	/web/bundle/web.assets_emoji	200	0.000	Backend R...	Mitchell A...	☐
☐	Oct 4, 12:59 AM	127.0.0.1		Open a menu or action	POST	/web/action/load	200	0.008	Backend R...	Mitchell A...	☐
☐	Oct 4, 12:59 AM	127.0.0.1		Backend	GET	/odoo	200	0.017	Backend R...	Mitchell A...	☐
☐	Oct 4, 12:59 AM	127.0.0.1		Scripts and styles	GET	/web/bundle/web.assets_emoji	200	0.002	Backend R...	Mitchell A...	☐
☐	Oct 4, 12:59 AM	127.0.0.1		Open a menu or action	POST	/web/action/load	200	0.005	Backend R...	Mitchell A...	☐

Web Requests. "Contact: list records" means somebody opened the Contacts list

6.3 IP Profiles

Monitoring > IP Profiles has one line per address ever seen, with its totals and its status.

Traffic Control Dashboard Monitoring Security Reporting Configuration										6 1 YourCompany	
IP Profiles										1-41 / 41	
☐	IP Address	Country	City	Last Seen	Requests	404 Errors	Failed L...	Threat Score	Bot	Status	
☐	127.0.0.1			Oct 4, 12:56 AM	41	0	0	0.00	☒	Normal	
☐	198.51.100.40	United States	City 40	Oct 4, 12:35 AM	30	0	0	0.00	☐	Normal	
☐	198.51.100.39	Netherlands	City 39	Oct 4, 12:35 AM	35	2	0	0.00	☐	Normal	
☐	198.51.100.38	Russian Federation	City 38	Oct 4, 12:35 AM	38	1	0	0.00	☐	Normal	
☐	198.51.100.37	China	City 37	Oct 4, 12:35 AM	31	0	0	0.00	☐	Normal	
☐	198.51.100.36	Brazil	City 36	Oct 4, 12:35 AM	32	2	0	0.00	☐	Normal	
☐	198.51.100.35	United Kingdom	City 35	Oct 4, 12:35 AM	29	2	0	0.00	☐	Normal	
☐	198.51.100.34	France	City 34	Oct 4, 12:35 AM	36	0	0	0.00	☐	Normal	
☐	198.51.100.33	India	City 33	Oct 4, 12:35 AM	39	0	0	0.00	☐	Normal	
☐	198.51.100.32	Bangladesh	City 32	Oct 4, 12:35 AM	34	1	0	0.00	☐	Normal	
☐	198.51.100.31	Germany	City 31	Oct 4, 12:35 AM	40	0	0	0.00	☐	Normal	
☐	198.51.100.30	United States	City 30	Oct 4, 12:35 AM	41	1	0	0.00	☐	Normal	
☐	198.51.100.29	Netherlands	City 29	Oct 4, 12:35 AM	32	3	0	0.00	☐	Normal	
☐	198.51.100.28	Russian Federation	City 28	Oct 4, 12:35 AM	46	1	0	0.00	☐	Normal	
☐	198.51.100.27	China	City 27	Oct 4, 12:35 AM	24	1	0	0.00	☐	Normal	
☐	198.51.100.26	Brazil	City 26	Oct 4, 12:35 AM	31	1	0	0.00	☐	Normal	
☐	198.51.100.25	United Kingdom	City 25	Oct 4, 12:35 AM	32	2	0	0.00	☐	Normal	
☐	198.51.100.24	France	City 24	Oct 4, 12:35 AM	46	1	0	0.00	☐	Normal	
☐	198.51.100.23	India	City 23	Oct 4, 12:35 AM	42	1	0	0.00	☐	Normal	

IP Profiles

Status	Meaning
Normal	Nothing noticed.
Watch	Some doubtful behaviour (score 30 or more), or you asked to keep an eye on it.
Suspicious	Clearly doubtful (score 60 or more). A suggestion is waiting for you.
Blocked	A block rule is in force for this address.
Allowed	On your allow list: never blocked, never scored.

Click a line to open the profile.

The screenshot displays the 'IP Profiles' section for the IP address 198.51.100.39. The interface includes a top navigation bar with links to Traffic Control, Dashboard, Monitoring, Security, Reporting, and Configuration. Below the navigation bar, there are buttons for 'Block', 'Watch / Unwatch', 'Refresh Location', and 'Forget this IP'. The main content area is divided into several sections: 'LOCATION' (Country: Netherlands, Region, City: City 39, Timezone, Latitude, Longitude, Geolocated On), 'NETWORK' (IP Version: 4, ISP, ASN, Reverse DNS, Bot), 'ACTIVITY' (First Seen: Oct 1, 12:35 AM, Last Seen: Oct 4, 12:35 AM, Pages: 21, 404 Errors: 2, 4xx Errors: 3, 5xx Errors: 1, Failed Logins: 0), and 'THREAT' (Threat Score: 0.00, Score Computed At, Watched). A right sidebar shows a chat window with OdooBot, indicating 'Traffic Control IP Profile created'. At the bottom, there are tabs for 'Threat Events', 'Login Attempts', and 'Rules', followed by a table with columns: Date, Rule, Severity, Score, and Evidence Summary.

An IP profile: location, network, activity, threat score, and tabs for events, logins and rules

Buttons at the top (Managers):

- **Block:** opens the block window for this address (chapter 7.5).
- **Unblock:** lifts the block; you can also put the address on the allow list.
- **Watch / Unwatch:** keep the address on "Watch" whatever its score.
- **Refresh Location:** look the address up again in the GeoIP database.
- **Forget this IP:** delete everything recorded about it (chapter 11).
- The **Requests** button on the right opens all its requests.
- The printer menu offers the **Security Incident Report** (chapter 9.3).

At the bottom you can write a note; every automatic block is also written there.

6.4 Backend Activity

Monitoring > Backend Activity: one line each time one of your staff opens an application, a list or a record inside Odoo: who, which application, which kind of record, when.

Traffic Control

Dashboard

Monitoring

Security

Reporting

Configuration

6

1

YourCompany

Backend Activity

Search...

1-78 / 78

☐	Date	User	App	Action	Model	View Type	Record ID	IP	
☐	Oct 4, 1:01 AM	Mitchell Admin	Traffic Control	IP Profiles	oeasyai.wtc.ip	form	165	127.0.0.1	
☐	Oct 4, 1:01 AM	Mitchell Admin	Traffic Control	IP Profiles	oeasyai.wtc.ip	list	0	127.0.0.1	
☐	Oct 4, 1:00 AM	Mitchell Admin	Traffic Control	Web Requests	oeasyai.wtc.request.log	list	0	127.0.0.1	
☐	Oct 4, 1:00 AM	Mitchell Admin	Traffic Control	Website Requests	oeasyai.wtc.request.log	form	1,586	127.0.0.1	
☐	Oct 4, 1:00 AM	Mitchell Admin	Traffic Control	Website Requests	oeasyai.wtc.request.log	list	0	127.0.0.1	
☐	Oct 4, 12:59 AM	Mitchell Admin	Discuss	Traffic Control		client	0	127.0.0.1	
☐	Oct 4, 12:59 AM	Mitchell Admin	Discuss	Discuss		client	0	127.0.0.1	
☐	Oct 4, 12:59 AM	Mitchell Admin	Discuss	Discuss		client	0	127.0.0.1	
☐	Oct 4, 12:58 AM	Mitchell Admin	Traffic Control	Web Requests	oeasyai.wtc.request.log	list	0	127.0.0.1	
☐	Oct 4, 12:57 AM	Mitchell Admin	Traffic Control	Website Requests	oeasyai.wtc.request.log	form	1,561	127.0.0.1	
☐	Oct 4, 12:56 AM	Mitchell Admin	Traffic Control	Website Requests	oeasyai.wtc.request.log	list	0	127.0.0.1	
☐	Oct 4, 12:56 AM	Mitchell Admin	Discuss	Traffic Control		client	0	127.0.0.1	
☐	Oct 4, 12:56 AM	Mitchell Admin	Discuss	Discuss		client	0	127.0.0.1	
☐	Oct 4, 12:56 AM	Mitchell Admin	Discuss	Discuss		client	0	127.0.0.1	
☐	Oct 4, 12:38 AM	Mitchell Admin	Discuss	Traffic Control		client	0	127.0.0.1	
☐	Oct 4, 12:38 AM	Mitchell Admin	Discuss	Discuss		client	0	127.0.0.1	
☐	Oct 4, 12:36 AM	Mitchell Admin	Discuss	Traffic Control		client	0	127.0.0.1	
☐	Oct 4, 12:36 AM	Mitchell Admin	Discuss	Discuss		client	0	127.0.0.1	
☐	Oct 4, 12:35 AM	Mitchell Admin	Discuss		website.page	form	0		

Backend Activity

6.5 Login Attempts

Monitoring > Login Attempts: every attempt to log in, successful (green) or not (red), with the reason of a failure.

Traffic Control

Dashboard

Monitoring

Security

Reporting

Configuration

6

1

YourCompany

Login Attempts

Q

Search...

1-41 / 41

<

>

☐	Date	IP	Country	Login	User	Channel	Success	Failure Reason	
☐	Oct 4, 12:59 AM	127.0.0.1		admin	Mitchell Admin	Web form	☒		
☐	Oct 4, 12:56 AM	127.0.0.1		admin	Mitchell Admin	Web form	☒		
☐	Oct 4, 12:38 AM	127.0.0.1		admin	Mitchell Admin	Web form	☒		
☐	Oct 4, 12:36 AM	127.0.0.1		admin	Mitchell Admin	Web form	☒		
☐	Oct 4, 12:33 AM	198.51.100.2	Bangladesh	admin		Web form	☐	Wrong password	
☐	Oct 4, 12:31 AM	198.51.100.1	Germany	root		Web form	☐	Wrong password	
☐	Oct 4, 12:28 AM	198.51.100.1	Germany	root		Web form	☐	Wrong password	
☐	Oct 4, 12:19 AM	198.51.100.8	Russian Federation	admin		Web form	☐	Wrong password	
☐	Oct 4, 12:19 AM	198.51.100.6	Brazil	root		Web form	☐	Wrong password	
☐	Oct 4, 12:14 AM	198.51.100.5	United Kingdom	root		Web form	☐	Wrong password	
☐	Oct 3, 11:52 PM	198.51.100.8	Russian Federation	info@example.com		Web form	☐	Wrong password	
☐	Oct 3, 11:20 PM	198.51.100.7	China	info@example.com		Web form	☐	Wrong password	
☐	Oct 3, 11:10 PM	198.51.100.4	France	info@example.com		Web form	☐	Wrong password	
☐	Oct 3, 11:05 PM	198.51.100.4	France	root		Web form	☐	Wrong password	
☐	Oct 3, 10:50 PM	198.51.100.5	United Kingdom	root		Web form	☐	Wrong password	
☐	Oct 3, 10:45 PM	198.51.100.6	Brazil	admin		Web form	☐	Wrong password	
☐	Oct 3, 10:34 PM	198.51.100.8	Russian Federation	info@example.com		Web form	☐	Wrong password	
☐	Oct 3, 10:34 PM	198.51.100.2	Bangladesh	root		Web form	☐	Wrong password	
☐	Oct 3, 10:18 PM	198.51.100.4	France	info@example.com		Web form	☐	Wrong password	

Login Attempts

Failure reason	Meaning
Unknown login	Nobody has that login name.
Wrong password	The login exists, the password was wrong.
Blocked / cooldown	Refused because of too many recent failures.
Two-factor failed	The password was right, the second code was wrong.
Inactive user	The user account is archived.
Invalid API key	A program used a wrong key.

7. Security: finding and blocking hostile visitors

7.1 How the module judges a visitor

The module has a list of **threat rules** (chapter 10.1). Each rule describes one doubtful behaviour and has a number of points. Examples:

- Asking for `/wp-login.php` : that is a WordPress page; Odoo has none. Somebody is probing. 25 points.
- A browser name used by an attack tool: 50 points.
- More than 120 requests in one minute: 20 points, and the address is slowed down for 5 minutes.

Every time a rule matches, a **threat event** is recorded and its points are added to the address's **threat score**. Points fade: after 24 hours they count for half, after 48 hours for a quarter. So an address that stops misbehaving becomes "Normal" again by itself.

Score	What happens
30 or more	Status becomes Watch.
60 or more	Status becomes Suspicious and a block suggestion is created for you.
100 or more	Blocked automatically, but only if you switched "Automatic Block on Score" on (it is off by default).

A rule match never stops the request by itself. The visitor is only refused once a block rule exists for them.

7.2 Suggestions: your decisions

Security › **Suggestions** lists the addresses the module proposes to block.

Traffic Control Dashboard Monitoring Security Reporting Configuration							YourCompany	
Block Suggestions							1-6 / 6	
☐ To Review ☐ Search...								
☐ Raised On	IP	Country	Score	Reason	Decided By	Status		
☐ Oct 4, 12:35 AM	198.51.10...	Brazil	90.00	Score 90.0 from 2 events. Rules: PATH_TRAVERSAL, SCANNER_UA		To Review	Block	Dismiss
☐ Oct 4, 12:35 AM	198.51.10...	France	90.00	Score 90.0 from 2 events. Rules: SCANNER_UA, SQLI_PATTERN		To Review	Block	Dismiss
☐ Oct 4, 12:35 AM	198.51.10...	India	90.00	Score 90.0 from 2 events. Rules: PATH_TRAVERSAL, SCANNER_UA		To Review	Block	Dismiss
☐ Oct 4, 12:35 AM	198.51.10...	Bangladesh	90.00	Score 90.0 from 2 events. Rules: SCANNER_UA, SQLI_PATTERN		To Review	Block	Dismiss
☐ Oct 4, 12:35 AM	198.51.10...	Germany	90.00	Score 90.0 from 2 events. Rules: SCANNER_UA, SQLI_PATTERN		To Review	Block	Dismiss
☐ Oct 4, 12:35 AM	198.51.10...	United King...	80.00	Score 80.0 from 2 events. Rules: PATH_TRAVERSAL, SQLI_PATTERN		To Review	Block	Dismiss

Suggestions waiting for a decision

- 1 Click a line to open it. Read the reason and the tab **Evidence**, which lists what the address did.
- 2 Choose one of the four buttons at the top.

Traffic Control

DashboardMonitoringSecurityReportingConfiguration

6

1

YourCompany

Block Suggestions198.51.100.61 / 6<>

Block

Watch

Allow-list

Dismiss

To ReviewBlocked

Send message

Log note

Activity

0

IP198.51.100.6Decided By

CountryBrazilDecided At

Score90.00Resulting Rule

REASON

Score 90.0 from 2 events. Rules: PATH_TRAVERSAL, SCANNER_UA

Evidence

Date	Rule	Severity	Score	Evidence Summary
Oct 4, 12:35 AM	Path traversal	High	40	field: path, matched: sample
Oct 4, 12:35 AM	Vulnerability scanner	High	50	field: path, matched: sample

Today

OdooBot12:35 AM

Traffic Control Block Suggestion created

A suggestion with its evidence

Button	Who	Effect
Block	Manager	Opens a small window: choose how long and for which part of the site, then Apply. A block rule is created.
Watch	Analyst, Manager	No block; the address stays on Watch.
Allow-list	Manager	You trust this address: it will never be blocked or scored.
Dismiss	Analyst, Manager	Close the suggestion without doing anything.

Decide Suggestions

Suggestions

Decision

Block

Watch

Allow-list

Dismiss

Duration

24 hours

Scope

Whole site

Note

Apply

Discard

The decision window

Several at once. In the list, tick the boxes at the left of several lines, then click **Decide** at the top.

7.3 Threat Events

Security > Threat Events is the diary of every rule match: when, which address, which rule, how many points, and the evidence (what exactly matched).

Traffic Control Dashboard Monitoring Security Reporting Configuration							61 YourCompany	
Threat Events							1-12 / 12	
☐	Date	IP	Country	Rule	Severity	Score	Evidence Summary	
☐	Oct 4, 12:35 AM	198.51.100.6	Brazil	Path traversal	High	40	field: path, matched: sample	
☐	Oct 4, 12:35 AM	198.51.100.6	Brazil	Vulnerability scanner	High	50	field: path, matched: sample	
☐	Oct 4, 12:35 AM	198.51.100.5	United Kingdom	Path traversal	High	40	field: path, matched: sample	
☐	Oct 4, 12:35 AM	198.51.100.5	United Kingdom	SQL injection pattern	High	40	field: path, matched: sample	
☐	Oct 4, 12:35 AM	198.51.100.4	France	Vulnerability scanner	High	50	field: path, matched: sample	
☐	Oct 4, 12:35 AM	198.51.100.4	France	SQL injection pattern	High	40	field: path, matched: sample	
☐	Oct 4, 12:35 AM	198.51.100.3	India	Path traversal	High	40	field: path, matched: sample	
☐	Oct 4, 12:35 AM	198.51.100.3	India	Vulnerability scanner	High	50	field: path, matched: sample	
☐	Oct 4, 12:35 AM	198.51.100.2	Bangladesh	SQL injection pattern	High	40	field: path, matched: sample	
☐	Oct 4, 12:35 AM	198.51.100.2	Bangladesh	Vulnerability scanner	High	50	field: path, matched: sample	
☐	Oct 4, 12:35 AM	198.51.100.1	Germany	Vulnerability scanner	High	50	field: path, matched: sample	
☐	Oct 4, 12:35 AM	198.51.100.1	Germany	SQL injection pattern	High	40	field: path, matched: sample	
							530	

Threat Events

7.4 Block & Allow List

Security > Block & Allow List holds every rule: the ones you made, the ones made from suggestions, and the automatic ones.

Traffic Control Dashboard Monitoring Security Reporting Configuration										6 1 YourCompany		
New	Block & Allow List		Search...							1-7 / 7		
☐	Name	List	Match Type	Value	Country	Action	Scope	Source	Expires	Hit Count	Last Hit	Active
☐	Automatic block of 198.5...	Block	IP address	198.51.100.3		Throttle (...)	Login only	Automatic...	Oct 5, 1:14 AM	0		☒
☐	Hide the database manager	Block	Path (regex)	^/web/dat...		Block (403)	Whole site	Manual		0		☒
☐	Bad crawler	Block	User agen...	BadCrawle...		Block (403)	Whole site	Manual		57	Oct 4, 1:14 AM	☒
☐	No backend from Antarct...	Block	Country		Antarctica	Block (403)	Backend o...	Manual		0		☒
☐	Hosting range used by sc...	Block	IP range (...)	192.0.2.0/24		Throttle (...)	Website o...	Manual	Nov 3, 1:14 AM	1,830	Oct 4, 1:14 AM	☒
☐	Scanner from 198.51.100.1	Block	IP address	198.51.100.1		Block (403)	Whole site	Suggestion	Oct 11, 1:14 AM	214	Oct 4, 1:14 AM	☒
☐	Allow head office	Allow	IP range (...)	203.0.113....		Block (403)	Whole site	Manual		0		☒
										2,101		

Block & Allow List

Two lists live here:

- **Block:** who is refused.
- **Allow:** who is always let in. **The allow list always wins.** Put your own office address here so you can never block yourself.

Traffic Control
Dashboard
Monitoring
Security
Reporting
Configuration

6
1
YourCompany

New
Block & Allow List
Scanner from 198.51.100.1
6 / 7

Lift

Name
Scanner from 198.51.100.1

MATCH

List
Block
Allow

Match Type
IP address

Value
198.51.100.1

IP Profile
198.51.100.1

EFFECT

Action
Block (403)

Scope
Whole site

Date Start
Oct 4, 1:14 AM

Expires
Oct 11, 1:14 AM

ORIGIN

Source
Suggestion

HITS

Hit Count
214

Last Hit
Oct 4, 1:14 AM

REASON

Repeated SQL injection attempts

Send message
Log note

Today

OdooBot
1:14 AM

Traffic Control Block / Allow Rule created

A rule opened

Field	Meaning
List	Block or Allow.
Match Type	IP address (one address); IP range (many addresses, written like 203.0.113.0/24); Country; User agent (the browser or program name); Path (an address on your site).
Value / Country	The address, range, country or text to match.
Action	Block (403) : refuse. Throttle (429) : refuse with the message "too many requests, retry later". Log only : let through, just count.
Scope	Whole site; Login only (the visitor can still read the website but cannot try to log in); Website only; Backend only.
Expires	When the rule ends. Empty = for ever.
Source	Manual, Suggestion, Automatic (login), Automatic (threat) or Import.
Hits	How many requests the rule has caught.

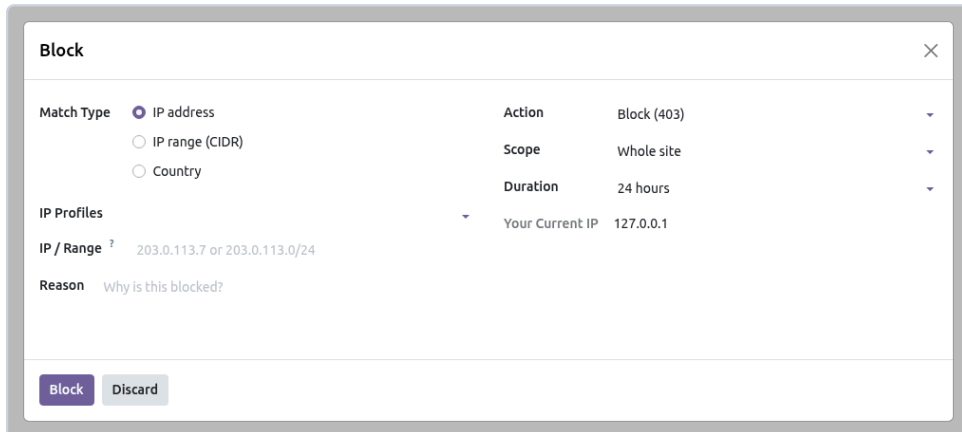
To end a rule, open it and click **Lift**, or switch off the toggle at the end of its line. The rule is archived, not deleted, so the history is kept. Rules that reach their expiry are archived automatically.

Website Traffic Control - User Manual

Page 27 of 50

7.5 Blocking an address, a range or a country

- 1 Open **Security > Block an IP, Range or Country** (or click **Block an IP** on the dashboard, or **Block** on an IP profile).
- 2 Choose what to block: IP address, IP range, or Country.
- 3 Type the address or range, or choose the country.
- 4 Choose the Action, the Scope and the Duration (15 minutes up to Permanent).
- 5 Write the reason, so your colleagues understand later.
- 6 Click **Block**.



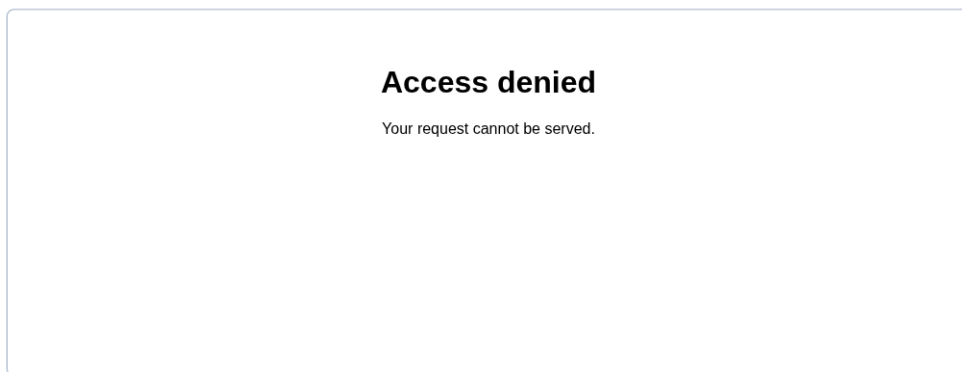
The screenshot shows a 'Block' configuration window. It has a title bar with a close button. The main area is divided into two columns. The left column has 'Match Type' with three radio buttons: 'IP address' (selected), 'IP range (CIDR)', and 'Country'. Below this is 'IP Profiles' with a dropdown arrow, and 'IP / Range' with a text input field containing '203.0.113.7 or 203.0.113.0/24'. The right column has 'Action' with a dropdown showing 'Block (403)', 'Scope' with a dropdown showing 'Whole site', and 'Duration' with a dropdown showing '24 hours'. Below these is 'Your Current IP' with a text input field showing '127.0.0.1'. At the bottom, there is a 'Reason' label and a text input field containing 'why is this blocked?'. At the very bottom, there are two buttons: 'Block' and 'Discard'.

The Block window. "Your Current IP" shows your own address

Do not lock yourself out. If the rule would match your own address, a red message appears and you must tick "I understand this blocks my own address" before the button works. If you are not sure, do not tick it.

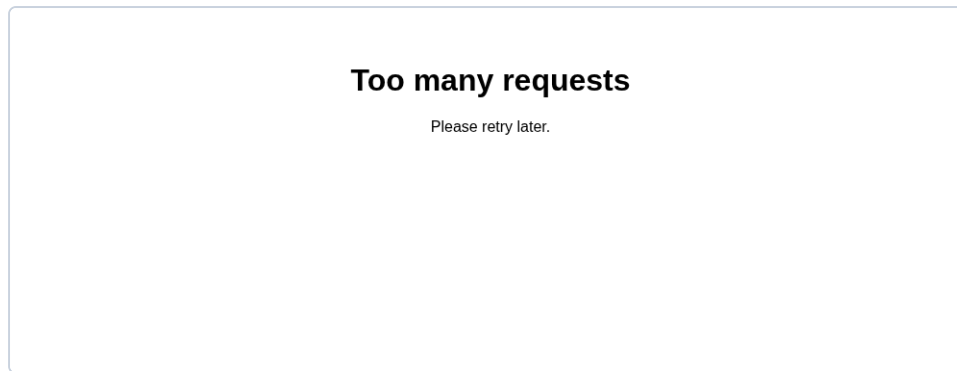
7.6 What a blocked visitor sees

A short page with no logo and no information about your system. You can change the sentence in the settings ("Block page text").



The screenshot shows a simple web page with a light blue border. In the center, the text 'Access denied' is displayed in a bold, black font. Below it, in a smaller, regular black font, is the text 'Your request cannot be served.'

Blocked (403)

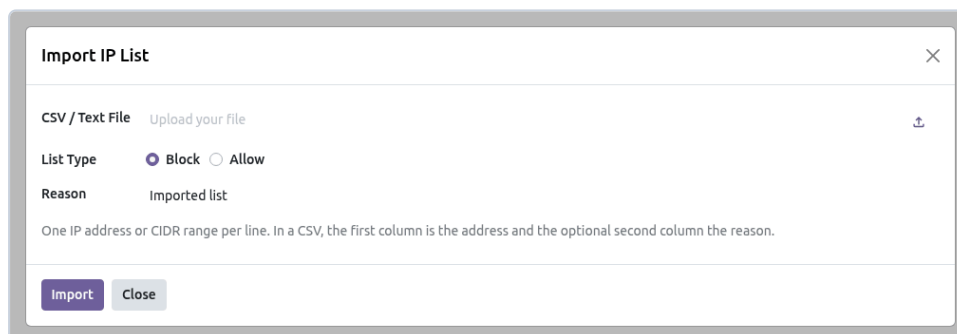


Throttled (429)

7.7 Importing a list of addresses

Use this when you received a list of bad addresses from somebody else.

- 1 Prepare a text or CSV file with one address or range per line. A second column, after a comma, may hold the reason.
- 2 Open **Security > Import IP List**.
- 3 Click the file box and choose your file.
- 4 Choose Block or Allow, then click **Import**.
- 5 Read the result: how many rules were created, how many already existed, and which lines were not valid addresses.



Import IP List

7.8 Exporting the block list

- 1 Open **Security > Export Block List**.
- 2 Choose the format: **nginx deny snippet** (for your server administrator to load into nginx), **Plain IP list**, or **CSV** (for a spreadsheet).
- 3 Click **Generate**, then click the file name that appears to download it.

Export Block List

Format

☒ nginx deny snippet

☐ Plain IP list

☐ CSV

nginx and plain list: live whole-site IP and range blocks only. CSV: every live IP and range block rule with its scope. Country, user-agent and path rules are not exported.

Generate

Close

Export Block List

The nginx and plain formats contain only whole-site blocks of addresses and ranges. Country, browser-name and path rules exist only inside Odoo.

8. Login protection

This part works by itself from the moment the module is installed. You do not have to do anything.

8.1 What it does

- Every login attempt is recorded (chapter 6.5): on the login page, and also by programs that connect to Odoo.
- When one address fails **10 times in 10 minutes**, it is blocked from logging in. This is called a brute-force attack: a program trying many passwords.
- When one address tries **5 different login names in 10 minutes**, it is blocked too. This is called password spraying.
- The Managers receive a notification in Odoo, and the block is written on the IP profile.

8.2 How long the block lasts

It grows each time the same address comes back within 30 days:

Block number	Duration
First	15 minutes
Second	1 hour
Third	24 hours
After that	24 hours again, and a suggestion asks you whether to block it permanently.

By default only logging in is blocked; the address can still read your public website. You can change this to the whole site in the settings.

8.3 A real user was blocked by mistake

- 1 Open **Security > Block & Allow List**.
- 2 Click the filter **Automatic** to find the rule with the person's address.
- 3 Open it and click **Lift**.
- 4 If it is your own office, also add the office address to the Allow list (chapter 7.4).

8.4 Many addresses attacking one account

When one login name fails 20 times from 5 or more different addresses in 30 minutes, the Managers are alerted. The account itself is never disabled by the module. An optional short "cooldown" can refuse that login name for some minutes (chapter 10.5).

9. Reporting

9.1 The ten analyses

Open them from the **Reporting** menu or from the dashboard's Reports tab.

Analysis	Answers the question
Traffic	How many requests, when, of which kind, from which country and device?
Pages	Which pages are viewed, entered on and left from?
Geography	Which countries, regions and cities?
Visitors / IPs	What did each address do each day? (Analysts)
Backend App Usage	Which applications do my staff use?
Errors	Which addresses return errors?
Performance	Which pages are slow?
Security	Which rules fire, how severe, from where?
Login Attempts	Who tries to log in, with what result? (Analysts)
Bots	Which bots visit, and are they genuine?

Traffic Control Dashboard Monitoring Security Reporting Configuration

6 1 YourCompany

Traffic Analysis

Q Last 30 Days x Search...

Measures

Total

Human Bot Suspicious Blocked

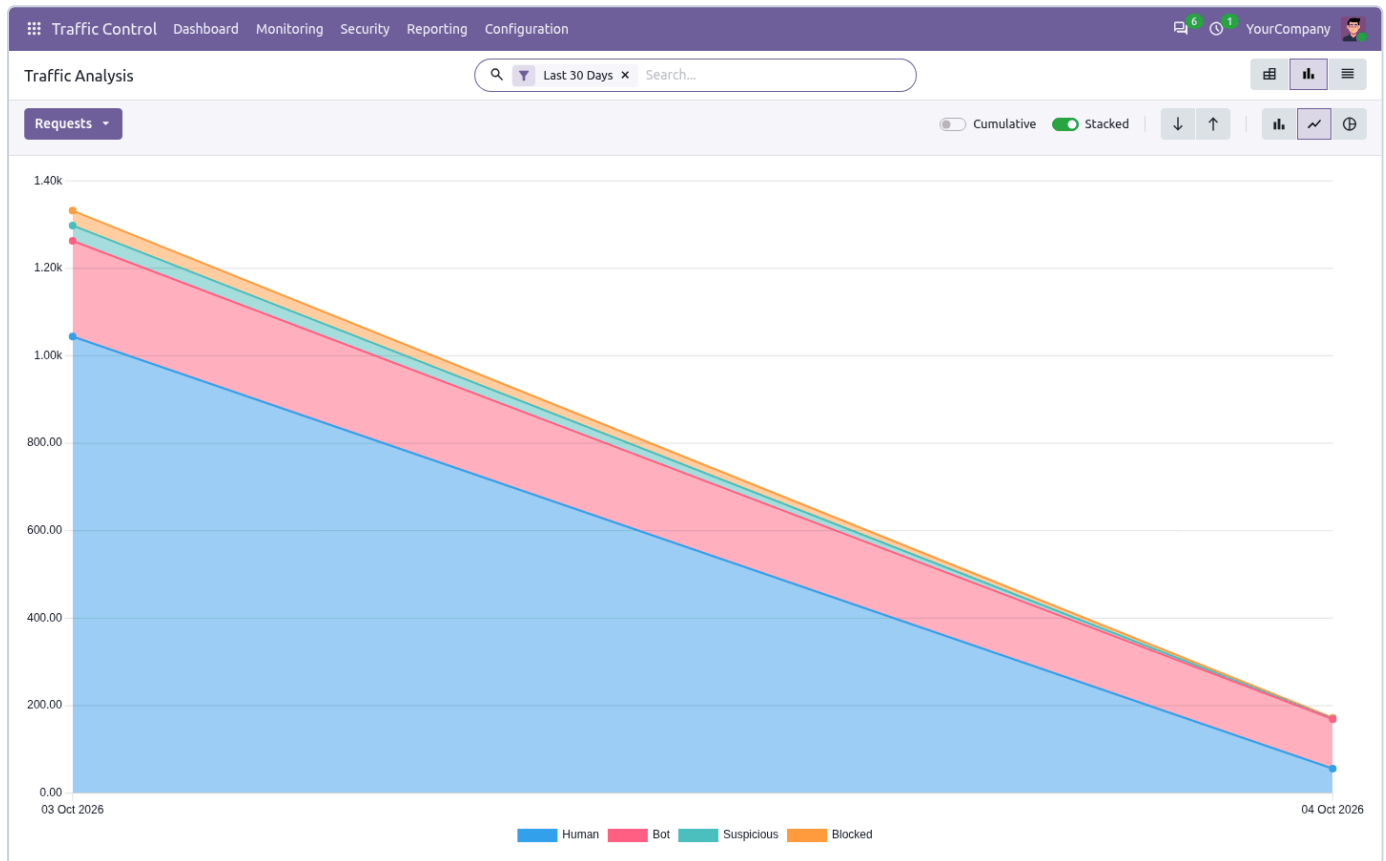
Requests Requests Requests Requests Requests

Total	1,100	332	36	36	1,504
03 Oct 2026	1,044	219	35	34	1,332
04 Oct 2026	56	113	1	2	172

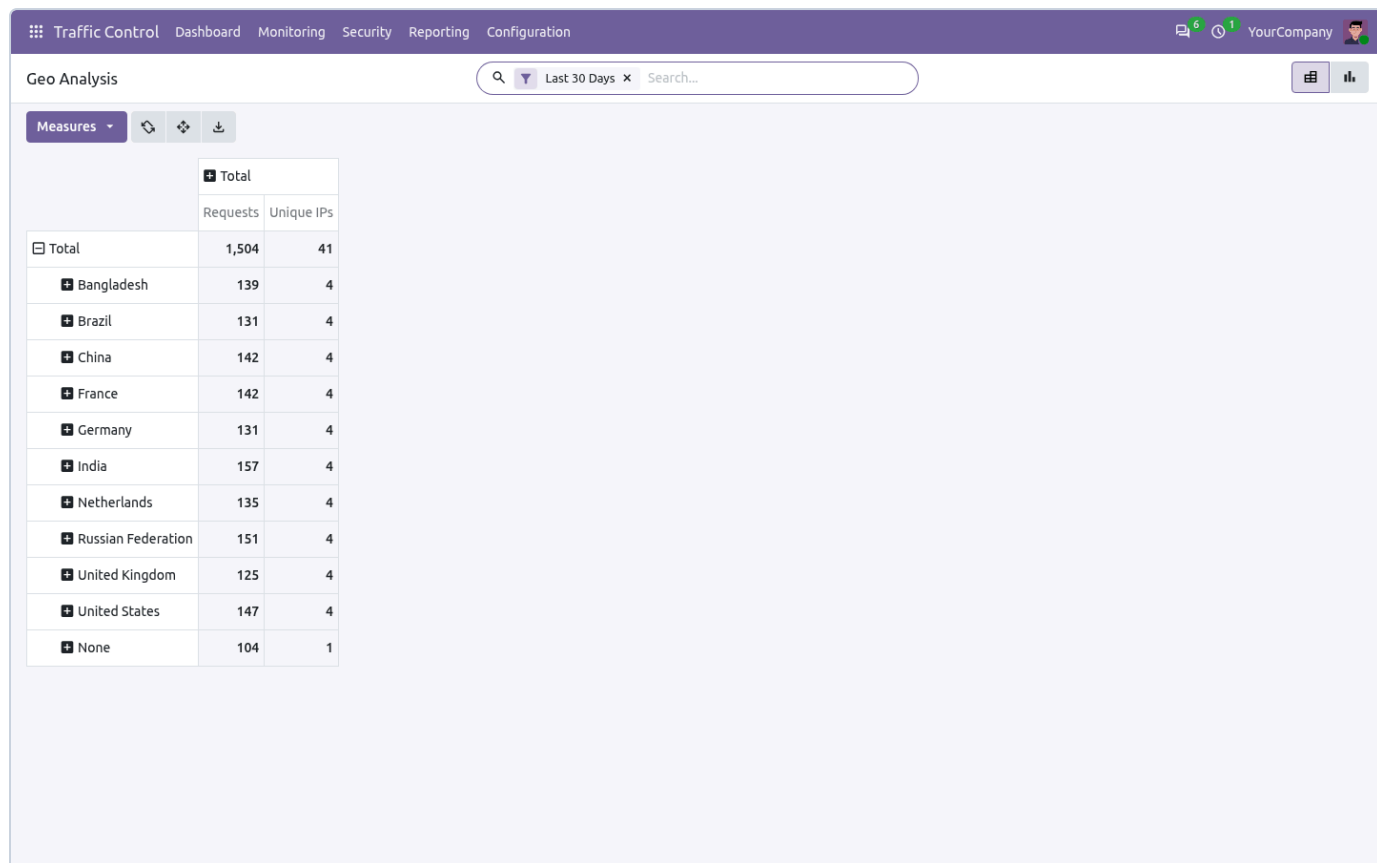
Traffic analysis as a table (pivot)

9.2 How to use an analysis

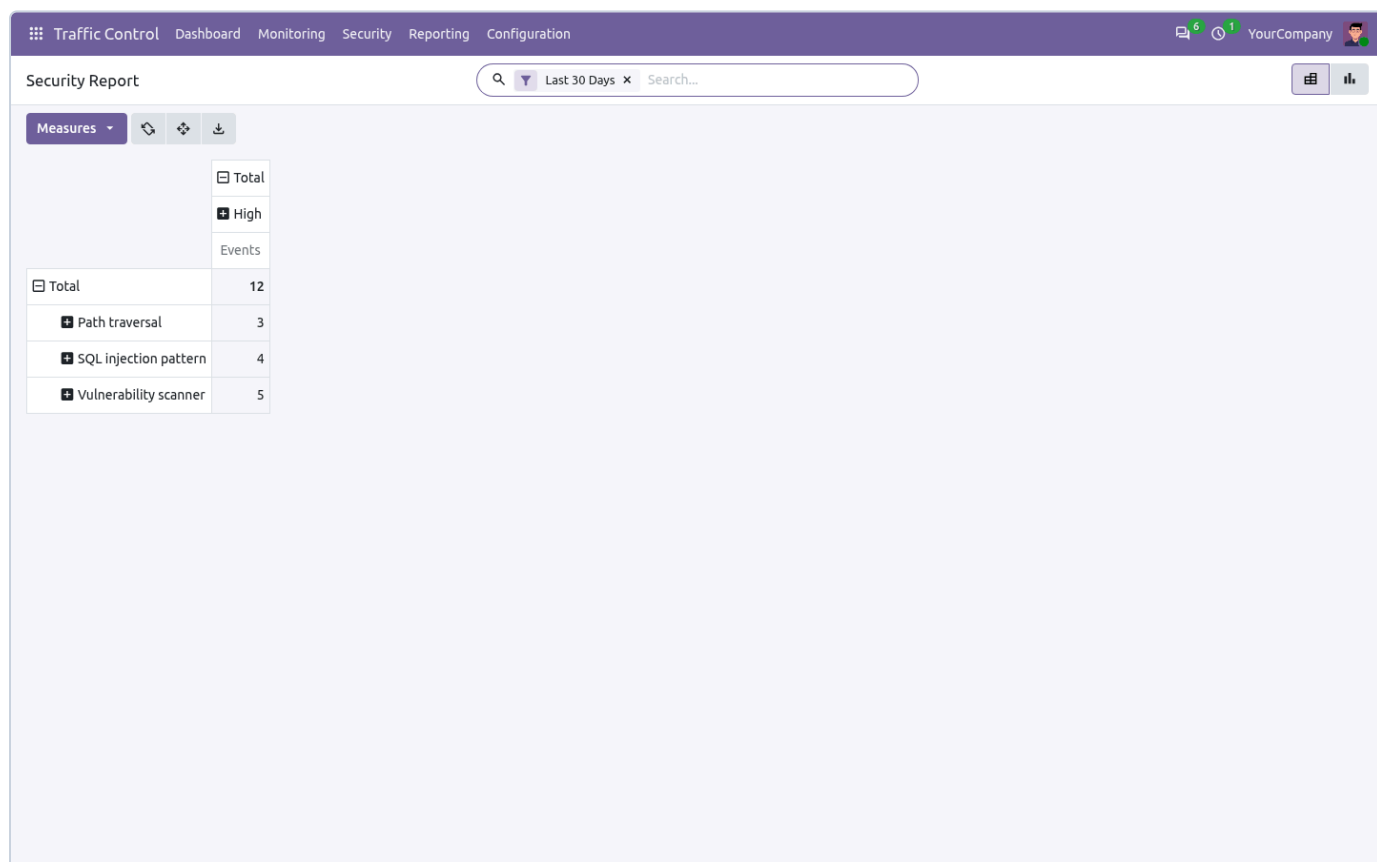
- **Table or chart.** The small icons at the top right switch between the table (pivot), the chart (graph) and, where it exists, the list.
- **Period.** Each analysis opens on the last 30 days. In the search box, remove that label and choose Today or Last 7 Days from the filter arrow.
- **Break down.** In the table, click a grey header with a plus sign and choose what to split by (country, device...). Click it again to fold.
- **Measures.** The **Measures** button chooses which numbers are shown.
- **To a spreadsheet.** In the table view, the download icon saves what you see as an Excel file.



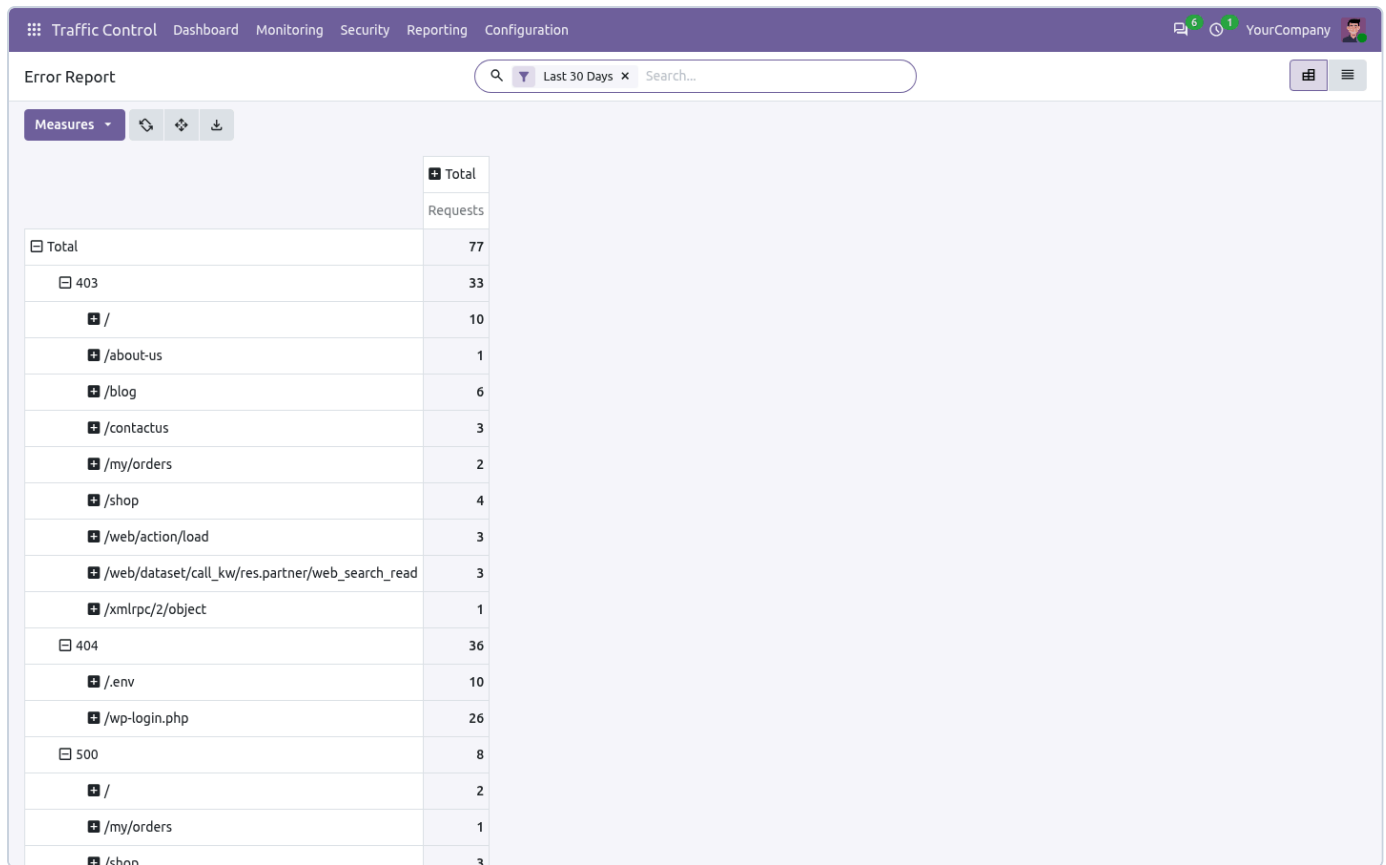
The same analysis as a chart



Geography analysis



Security analysis



Error analysis

9.3 Printable reports (PDF)

Report	Where	Content
Daily Traffic Summary	Reporting > Daily Summary (PDF)	Key figures of the last 24 hours, top countries, pages, 404s and rules.
Weekly Traffic Summary	Reporting > Weekly Summary (PDF)	The same for the last 7 days. Can be e-mailed every week (chapter 10.5).
Block List Snapshot	Reporting > Block List Snapshot (PDF)	Every rule in force now.
Security Incident Report	On an IP profile: printer menu	Everything about one address: profile, events, login attempts, actions taken.

Weekly Traffic Summary

09/26/2026 08:58:59 PM - 10/03/2026 08:58:59 PM

Key figures

Indicator	This period	Previous period
Requests	1441	0
Unique IPs	41	0
Unique visitors	3	0
Page views	959	0
Bot share (%)	18.7	0.0
4xx/5xx rate (%)	5.3	0.0
Average response (ms)	444	0
Failed logins	37	0
Blocked requests	36	0

Top countries

Country	Requests	IPs
India	157	4
Russian Federation	151	4
United States	147	4
France	142	4
China	142	4
Bangladesh	139	4
Netherlands	135	4
Germany	131	4
Brazil	131	4
United Kingdom	125	4

Top pages

Path	Views
/	397
/shop	228
/blog	121
/contactus	92
/about-us	75
/my/orders	43
/web/login	3

Top 404 paths

Path	Hits
/wp-login.php	26

Threat events by rule

Rule	Events
SCANNER_UA	5

Weekly Traffic Summary

Security Incident Report

198.51.100.1

Profile

Status	Suspicious	Threat score	89.95
Country	Germany	Region / City	City 1
ISP / ASN	Reverse DNS		
First seen	09/30/2026 08:35:05 PM	Last seen	10/03/2026 08:35:05 PM
Requests	30	404 errors	0
Failed logins	0	Bot	

Threat events (latest 100)

Date	Rule	Severity	Score	Evidence
10/03/2026 08:35:06 PM	SCANNER-UA	High	50	field: path, matched: sample
10/03/2026 08:35:06 PM	SQLI_PATTERN	High	40	field: path, matched: sample

Login attempts (latest 100)

Date	Login	Channel	Result
10/03/2026 08:31:05 PM	root	Web form	Wrong password
10/03/2026 08:28:05 PM	root	Web form	Wrong password
10/03/2026 03:07:05 PM	root	Web form	Wrong password
10/03/2026 11:11:05 AM	root	Web form	Wrong password
10/03/2026 11:10:05 AM	admin	Web form	Wrong password

Actions taken

Rule	List	Action	Scope	Source	From	Until
No rule						

Security Incident Report for one address

10. Configuration

This menu is for Managers.

10.1 Threat Rules

Configuration > Threat Rules. Sixteen rules are delivered ready to use. You can switch a rule off with the toggle at the end of its line, or open it to change its points.

Traffic Control

Dashboard

Monitoring

Security

Reporting

Configuration

6

1

YourCompany

New

Threat Rules

Search...

1-16 / 16

<

>

☐	Code	Name	Category	Rule Type	Evaluation	Score	Severity	Auto Action	Event C...	Active
☐	PATH_PROBE	Probe for foreign software	Probing	Path pattern	Each request	25	Medium	Suggest a block	0	☒
☐	PATH_TRAVERSAL	Path traversal	Injection	Path or query pattern	Each request	40	High	Suggest a block	3	☒
☐	SQLI_PATTERN	SQL injection pattern	Injection	Path or query pattern	Each request	40	High	Suggest a block	4	☒
☐	XSS_PATTERN	Cross-site scripting pattern	Injection	Path or query pattern	Each request	30	Medium	Suggest a block	0	☒
☐	SCANNER_UA	Vulnerability scanner	Scanner	User agent pattern	Each request	50	High	Suggest a block	5	☒
☐	EMPTY_UA	Missing user agent	Bot	User agent pattern	Each request	10	Low	None	0	☒
☐	DB_MANAGER_PROBE	Database manager probe	Probing	Path pattern	Each request	50	High	Suggest a block	0	☒
☐	HONEYPOT	Honeypot hit	Bot	Honeypot	Each request	60	High	Suggest a block	0	☒
☐	HIGH_RATE	High request rate	Rate	Request rate	Scheduled (window)	20	Medium	Throttle (429)	0	☒
☐	NOT_FOUND_BURST	404 burst	Probing	404 burst	Scheduled (window)	30	Medium	Suggest a block	0	☒
☐	PATH_ENUMERATION	Path enumeration	Probing	Distinct paths	Scheduled (window)	20	Medium	Suggest a block	0	☒
☐	FAKE_BOT	Fake search-engine bot	Bot	Fake bot	Scheduled (window)	40	High	Suggest a block	0	☒
☐	LOGIN_FAILURE	Failed login	Login	Login	Each request	5	Low	None	0	☒
☐	LOGIN_BRUTE_FORCE	Login brute force	Login	Login	Scheduled (window)	100	Critical	Block automatically	0	☒
☐	PASSWORD_SPRAY	Password spraying	Login	Login	Scheduled (window)	100	Critical	Block automatically	0	☒
☐	DISTRIBUTED_ATTACK	Distributed attack on one login	Login	Login	Scheduled (window)	0	High	None	0	☒

Threat Rules

Rule	Notices	Points
PATH_PROBE	Requests for software Odoo does not have (WordPress, phpMyAdmin, .env , .git , .php files).	25
PATH_TRAVERSAL	Attempts to climb out of the website folder (../).	40
SQLI_PATTERN	Database attack text in the address.	40
XSS_PATTERN	Script injection text in the address.	30
SCANNER_UA	The name of a known attack tool.	50
EMPTY_UA	A visitor that does not say what browser it is.	10
DB_MANAGER_PROBE	An anonymous visitor opening the database manager.	50
HONEYPOT	A visit to the trap address that no real visitor can find (10.5).	60
HIGH_RATE	More than 120 requests per minute from one anonymous address. Slows it down for 5 minutes.	20
NOT_FOUND_BURST	20 or more "not found" answers in 5 minutes, making up at least half of the address's requests.	30
PATH_ENUMERATION	200 or more different addresses asked in 10 minutes.	20
FAKE_BOT	A visitor claiming to be Google or Bing that is not.	40
LOGIN_FAILURE	Each failed login.	5
LOGIN_BRUTE_FORCE	10 failed logins in 10 minutes. Blocks automatically.	100
PASSWORD_SPRAY	5 different login names tried in 10 minutes. Blocks automatically.	100
DISTRIBUTED_ATTACK	One login name attacked from many addresses. Alerts the Managers.	-

Traffic Control Dashboard Monitoring Security Reporting Configuration

Threat Rules Probe for foreign software

Events 0

1 / 16

Name
Probe for foreign software

DETECTION		CONSEQUENCE	
Code	PATH_PROBE	Score	25
Category	Probing	Severity	Medium
Rule Type	Path pattern	Auto Action	Suggest a block
Evaluation	Each request		
Pattern ?	{:~}/(?:wp-admin wp-login\.php wp-content wp-includes phpmyadmin cgi		
Anonymous Visitors Only ?	☐		

DESCRIPTION

Requests for paths that do not exist in Odoo: WordPress, phpMyAdmin, .env, .git, *.php, *.asp(x), cgi-bin, server-status. Odoo's own /xmlrpc/2/* and /json/2/* are not matched.

A threat rule opened

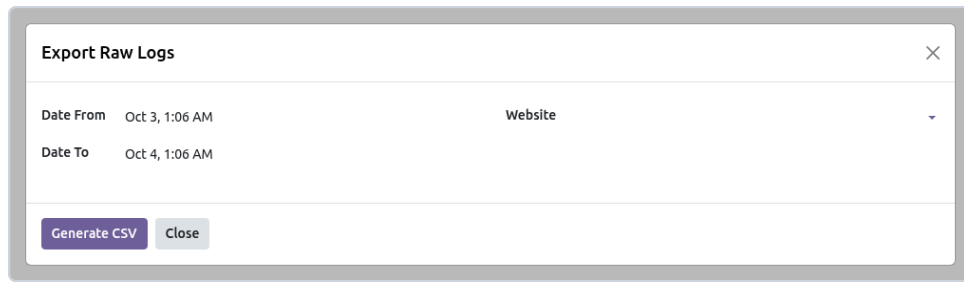
The field **Pattern** is a technical expression. Do not change it unless you know regular expressions; a wrong pattern can flag honest visitors. Changing **Score**, **Threshold** or switching a rule off is safe.

10.2 User Agents

Configuration > User Agents lists every browser and program name seen, and how the module understood it (browser, system, device, bot). It is for information only.

10.3 Export Raw Logs

- 1 Open **Configuration > Export Raw Logs**.
- 2 Choose the start and the end of the period, and optionally one website.
- 3 Click **Generate CSV**, then click the file name to download it. The file opens in any spreadsheet program.

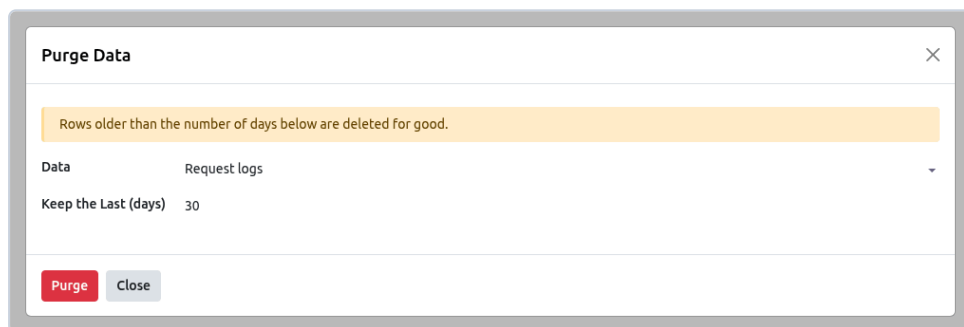


Export Raw Logs

10.4 Purge Data

Old data is deleted automatically (chapter 11). Use this window only when you want to delete by hand, for example to free space.

- 1 Open **Configuration > Purge Data**.
- 2 Choose which data, and how many of the latest days to keep.
- 3 Click **Purge** and confirm.



Purge Data

Purged data cannot be brought back.

10.5 Settings

Configuration > Settings. Change what you need, then click **Save** at the top left.

Traffic Control
Dashboard
Monitoring
Security
Reporting
Configuration

6
1
YourCompany

Save
Discard
Settings

Search...

General Settings
Website
Traffic Control

Status

☒
GeoIP database

Paths come from the Odoo options `geoip_city_db` and `geoip_country_db`.

→ Test GeoIP

ASN Database Path `/usr/share/GeoIP/GeoLite2-A...`

☐
Proxy mode

Without `proxy_mode`, every visitor is seen with the address of the proxy.

☐
Emergency switch

Set the system parameter `oeasyai_wtc.enforcement_disabled` to True (odoo shell or SQL) to switch off all blocking after a lock-out.

Log table

Estimated number of rows and size on disk of the raw request log.

1,602 rows, 488 kB

Logging

☒
Log Requests

Log each request that reaches Odoo.

Classes to Log `website_page,controller,backen`

Excluded Path Prefixes `/web/webclient/,/bus/,/mail/`

☐
Exclude Internal Users

Do not log the ordinary requests of internal users.

☐
Buffer Log Writes

Group ordinary log rows by 50 or every 5 seconds. A few rows may be lost when a worker restarts.

☒
Sampling

For very busy sites: log one ordinary request out of N. Errors, logins, suspicious and blocked requests are always logged.

1

Privacy

☒
Store full IP

☐ Mask (IPv4 /24, IPv6 /48)
☐ Keyed hash

☐
Hash Login Names

Store a keyed hash instead of the login typed. Passwords are never stored.

☐
IP anonymisation

How addresses are stored. Blocking still uses the full address in memory. Block rules keep the address in clear.

Settings, part 1

Website Traffic Control - User Manual

Page 42 of 50

Retention

Older rows are deleted every day, in batches. 0 keeps the data forever.

Request Logs (days)

30

Threat Events (days)

180

Login Attempts (days)

90

Aggregates (days)

730

☐ Time on Page

Record the time spent on each website page with a browser beacon.

Detection

☒ Threat Detection

Evaluate the threat rules and score each IP.

→ Threat Rules

☐ Automatic Block on Score

Block without approval when the score passes the threshold and the rule allows it. Login brute force is blocked automatically whatever this setting.

Honeypot

A URL no visitor should ever open. A hit scores as hostile.

/oeasyai_wtc/trap

☐ Advertise the Honeypot

☐ Score thresholds

A score above Watch flags the IP, above Suggest raises a block suggestion.

Watch Threshold

30.00

Suggest Threshold

60.00

Score Half-life (hours)

24.00

☐ Verify Search Bots by DNS

Check by reverse and forward DNS, in a scheduled job, that an IP claiming to be Googlebot or Bingbot really is.

Login Protection

☒ Login Protection

Record every login attempt and block brute force across all workers. Odoo's own per-worker cooldown stays active.

Brute force

Block an IP after this many failures, or this many distinct logins, within the window.

Failures

10

Distinct Logins

5

Window (minutes)

10

Escalation

Durations of the first, second, third... automatic block of an IP within 30 days. After the last one a permanent block is suggested.

15,60,1440

Block Scope

Login only

Whole site

Distributed attack

Many IPs failing on one login raise an alert. A cooldown can also refuse that login for a short time; the account is never disabled.

0

Enforcement

Enable Blocking

Answer 403 or 429 to the requests matching a block rule.

Block page text

Shown to blocked visitors. The page carries no branding and no database information.

Your request cannot be served.

Also Block Private Addresses

Private and loopback addresses are never blocked unless this is on. Leave it off unless you block inside a private network on purpose.

Notifications

Who is notified

Automatic blocks and distributed attacks are sent to this group. Empty means Traffic Control managers.

Each event

Weekly summary only

Weekly Summary Email

Email the weekly traffic summary (PDF) to the group every week.

Dashboard

Auto-refresh

Seconds between two refreshes of the dashboard (10 minimum).

60

Settings, part 3

Website Traffic Control - User Manual

Page 44 of 50

Block	Settings
Status	Read-only checks: GeoIP database found, proxy mode, size of the log, emergency switch. The Test GeoIP button, and the path of an optional extra database for internet provider names.
Logging	Log Requests on/off. Which classes to log and which address beginnings to skip. Exclude Internal Users (do not log your staff's ordinary work). Sampling for very busy sites: write only one ordinary request out of N. Buffer Log Writes : slightly faster, a few lines may be lost if the server restarts.
Privacy	IP Anonymisation , Hash Login Names , Retention days, Time on Page (chapter 11).
Detection	Threat Detection on/off. The Watch and Suggest thresholds and the half-life of the score. Automatic Block on Score with its threshold. Verify Search Bots by DNS . The Honeypot URL and whether to advertise it.
Login Protection	On/off. Number of failures, of distinct logins, and the window in minutes. The escalation durations. Whether a login block covers logging in only or the whole site. The cooldown for a login name under attack from many addresses.
Enforcement	Enable Blocking : the master switch. Also Block Private Addresses : leave off unless you know why. Block page text .
Notifications	Which group of users is told about automatic blocks; each event or weekly only; the weekly summary e-mail.
Dashboard	Seconds between two automatic refreshes.

The honeypot, in plain words

A honeypot is a trap: an address on your site that no person would ever open, because nothing visible links to it. When "Advertise the Honeypot" is on, the module tells well-behaved search engines to stay away from it and hides a link to it in your pages. Only a program that ignores the rules follows that link, and it is scored 60 points at once.

11. Privacy and data retention

An IP address is personal data in many countries. The module gives you four tools.

11.1 Store less: IP anonymisation

Choice	What is stored
Store full IP	The complete address.
Mask	The address with its last part removed (<code>203.0.113.77</code> becomes <code>203.0.113.0</code>). Neighbours share one profile.
Keyed hash	An unreadable code instead of the address.

Blocking still works in every case, because it is decided at the moment the visitor arrives. A block rule always keeps the real address, since it is your explicit decision. With "Keyed hash", a profile cannot be turned back into an address, so you cannot block it by hand from its profile.

11.2 Never stored

- Passwords. Only the login name tried is kept, and you can store that as a code too ("Hash Login Names").
- Secret values in an address: anything named password, token, key or secret is replaced by `***`.

11.3 Keep less long: retention

Data	Kept by default
Request logs and backend activity	30 days
Login attempts	90 days
Threat events	180 days
Summary figures (for the dashboard and reports)	730 days (2 years)

Change the numbers in the settings. 0 means "keep for ever".

11.4 Forget one address

When a person asks you to delete what you hold about them:

- 1 Open their profile in **Monitoring > IP Profiles**.
- 2 Click **Forget this IP**.
- 3 Decide whether block and allow rules for it are deleted as well.
- 4 Tick the confirmation box and click **Forget**.

Forget IP

Deletes the profile with its request logs, threat events, login attempts, daily statistics and suggestions. This cannot be undone.

IP Profiles

Also Delete Block / Allow Rules ?

I confirm the permanent deletion

Forget

Discard

Forget IP

The profile, its requests, threat events, login attempts, daily figures and suggestions are deleted for good.

12. What the module does on its own

Job	How often	What it does
Build aggregates	Every 15 minutes	Calculates the figures of the dashboard and reports from the raw log.
Window rules	Every 5 minutes	Checks the rules that look at a period of time (404 bursts, enumeration, attacks from many addresses).
Score decay	Every hour	Lets old points fade and updates each address's status.
Expire rules	Every 5 minutes	Archives block rules that reached their end.
Purge counters	Every 10 minutes	Clears the live counters.
Retention cleanup	Every day	Deletes data older than the retention settings.
Bot verification	Every hour	Checks claimed search-engine bots (when switched on).
Geo refresh	Every day	Looks old addresses up again.
Weekly summary	Every week	E-mails the weekly PDF (when switched on).

An administrator can see and run these jobs in **Settings > Technical > Scheduled Actions** (developer mode), searching for "Traffic Control".

13. When something goes wrong

What you see	Why, and what to do
I blocked myself and cannot open Odoo.	Use another connection (for example your phone's mobile data) and lift the rule. If nobody can get in, your server administrator switches all blocking off: in the Odoo shell or in the database, set the system parameter <code>oeasyai_wtc.enforcement_disabled</code> to <code>True</code> . Then lift the wrong rule and set the parameter back to <code>False</code> .
Every visitor has the address 127.0.0.1.	Proxy mode is not set. See chapter 3.3.
Countries are empty, or the dashboard says "GeoIP database not configured".	Open Configuration > Settings and click Test GeoIP . The Diagnosis box says exactly what is wrong on your server: the file is not found, Odoo is not allowed to read it, the configuration file still uses the old option <code>geoip_database</code> (rename it to <code>geoip_city_db</code>), or proxy mode is off. After your server administrator has fixed it and restarted Odoo, click Locate Existing IPs in the same window to fill the country of the addresses recorded earlier. Private addresses such as <code>127.0.0.1</code> never have a country.
The dashboard tiles show 0 but the lists show requests.	The figures are calculated every 15 minutes. Wait, or check the status line "Last aggregation".
I created a block rule but the visitor still gets in.	Check, in this order: the rule is active and not expired; its Scope covers what the visitor does; the address is not on the Allow list; "Enable Blocking" is on; the address is not a private one.
A real customer was blocked.	Lift the rule (7.4), and consider putting their address on the Allow list.
Google is marked "Suspicious".	Switch on "Verify Search Bots by DNS". Genuine search engines are then recognised and never go above Watch.
The menu Monitoring or Security is missing.	Your role is Viewer. Ask a Manager for the Analyst role (3.2).
The log table is very large.	Lower the retention days, switch on Sampling, exclude internal users, or purge by hand (10.4).
The website feels slower.	Switch on "Buffer Log Writes" and, for very busy sites, Sampling.

14. Reference

14.1 Who can do what

Task	Viewer	Analyst	Manager
See the dashboard and summary analyses	Yes	Yes	Yes
See individual IP addresses, requests, login attempts	No	Yes	Yes
Mark a suggestion Watch or Dismiss	No	Yes	Yes
Block, unblock, allow-list	No	No	Yes
Import and export block lists, export logs	No	No	Yes
Edit threat rules and settings, purge, forget an IP	No	No	Yes

14.2 Kinds of request (traffic class)

Class	Meaning
Website page	A page of your public website.
Controller / route	A website function that is not a page, such as sending a form.
Portal	The customer area ("My Account").
Backend RPC	The Odoo backend working for a logged-in user.
Login attempt	Somebody sending a login name and password.
API	Another program talking to Odoo.
Asset	Images, styles and scripts. Not logged by default.
Other	Anything else.

14.3 Answer codes (status)

Code	Meaning
200	Fine.
301, 303	The visitor was sent to another address.
403	Refused. Also what a blocked visitor receives.
404	Not found.
429	Too many requests: throttled.
500	The server failed. Tell your administrator.