



DNS PATROL

Documentation



VERSION
1.0.6

UPDATED
12 October 2026

ONLINE
labs.pages.nic.cz/dnspatrol-docs ↗

Contents



01	Overview	3
02	Infrastructure	4

WEB PORTAL

03	Main functions	7
04	Overview	9
05	DNS management	11
06	Access control	19
07	Analytics	27
08	Settings	36
09	What's new	37
10	About	39

CLIENT APPLICATIONS

11	Overview	40
12	iOS	41
13	Android	46
14	Windows	53
15	Browser extension	56

Overview



Welcome to the DNS PATROL documentation! DNS PATROL is a system that lets organisations secure and monitor DNS traffic on their network. Administrators can use the web portal to configure per-subnet policies, manage users, and monitor and analyse traffic. Thanks to the client applications, end users always connect to the correct DNS resolver.

1.1 Contents

[Infrastructure](#): Overview of the DNS PATROL system infrastructure [Web portal](#): Detailed manual for operating the administration portal [Client applications](#): Manual for the client applications

Infrastructure



DNS PATROL is a system typically consisting of several resolvers, some of which may sit directly inside the organization's network. These resolvers obtain their configuration from the backend, which is controlled through the administration web portal. Resolvers send query data to the database, with which the web portal also communicates for analytics.

2.1 Systems

This section describes the individual components of the DNS PATROL system.

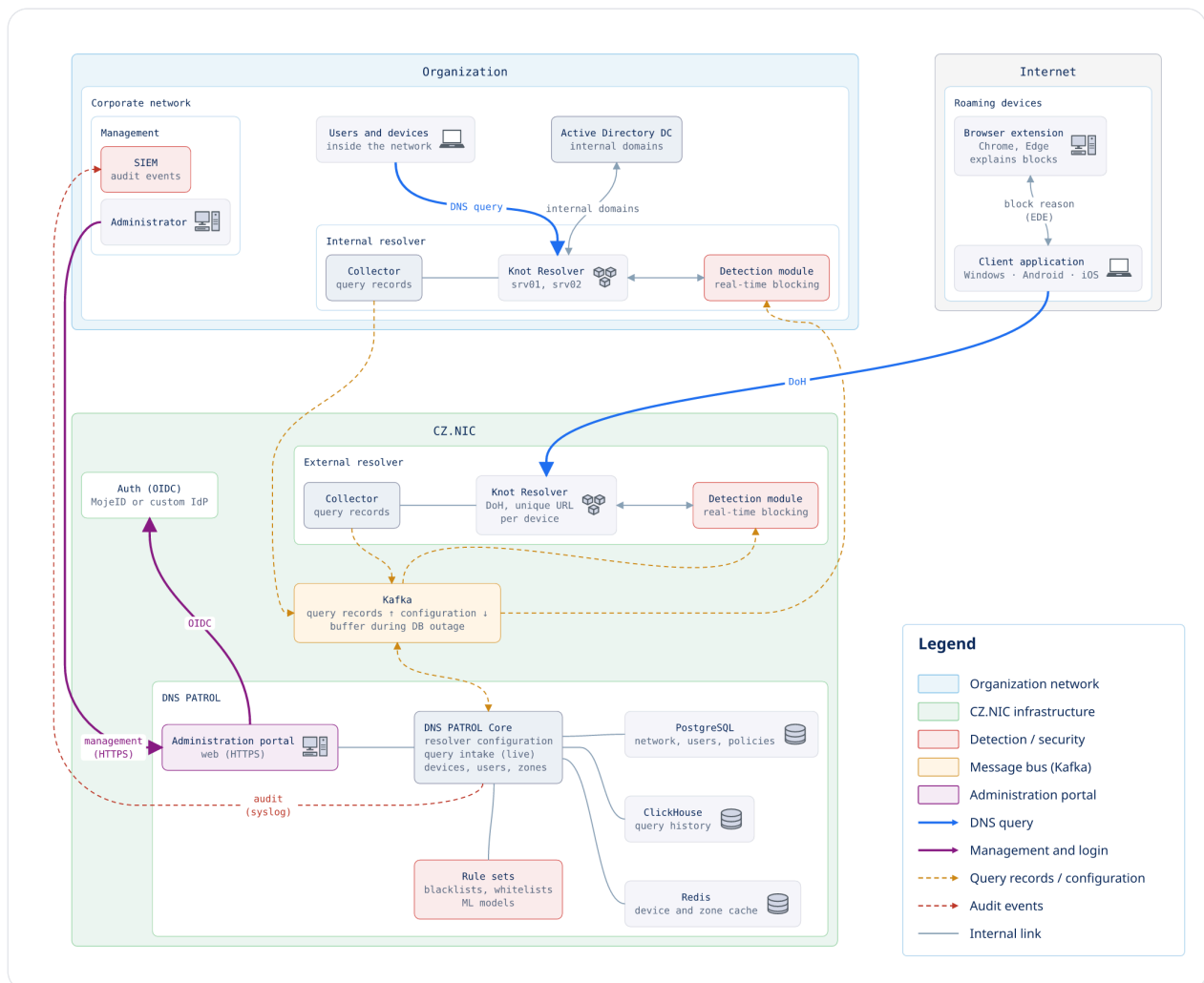


Figure 1 DNS PATROL architecture: components inside the organization's network and in the CZ.NIC infrastructure.

Resolvers

DNS queries are resolved by instances of [KNOT Resolver](#). A resolver can be located inside the organization's internal network, where it also communicates with the Active Directory Domain Controller to

resolve internal domain names. For subnets within the wider corporate network, additional resolvers may be deployed. For [end devices](#) outside the organization's network, an external resolver is available, queried via unique DoH URLs.

Alongside the resolver runs a collector, which captures information about every resolved query and publishes it to [Kafka](#).

Kafka

[Kafka](#) acts as the communication broker between the resolvers and the backend services. It also serves as a short-term buffer for DNS queries in case the main database fails.

Communication is bidirectional: resolvers publish query records into Kafka and consume configuration files (zones, blacklists and other rules) from Kafka, supplied by the [core](#) according to the current settings in the portal.

DNS PATROL Core

The core of the system, controlled through the [administration portal](#). Through [Kafka](#) it updates the resolvers' configuration according to the current settings and, in [live mode](#), receives DNS queries. It stores system configuration in the [databases](#) and queries them for long-term analytical data. User authentication is provided by external [OpenID](#) providers, such as [MojelD](#).

For fast lookups of registered devices and zones, the core uses a Redis cache, which it updates on every change to the registered devices or configuration.

The backend can forward audit events for administrator actions in the portal to external information systems over the syslog protocol, typically for integration with a corporate SIEM.

Administration portal

The administration portal is a web application; its usage is described in detail in the [Web portal](#) section.

Databases

[PostgreSQL](#): Network structure, users, devices, policy configuration, etc.

[ClickHouse](#): Handles large volumes of analytical data, stores query history for statistics and search in the portal

[Redis](#): In-memory cache of registered devices and zones for low-latency lookups.

End devices

End devices using the external resolver register into the system via a [client application](#) and a one-time registration code issued from the administration portal.

The client application on the device sends the registration code together with the hostname, MAC address and operating system information to [DNS PATROL Core](#). The core validates the code, creates a new device record bound to the user who owns the code, and returns to the client an identity token and a unique DoH URL. The device then routes all its DNS queries to that URL.

Browser extension

On Windows devices, the client application is accompanied by an extension for Chrome and Edge. When the resolver blocks a domain, it attaches the reason to its answer as an Extended DNS Error ([RFC 8914](#)). The browser ignores it, but the extension requests it through the client application and, instead of the browser's default error page, shows a page with an explanation and a reference code that identifies the event in the resolver's logs. The extension itself makes no network connections. See [Browser extension](#) for details.

2.2 Zones, subnets and rule sets

The logical structuring of the network and policies in DNS PATROL is built on three entities. A zone is the top-level unit and groups together a set of resolvers. Within a zone, subnets form a tree hierarchy based on address range. Rule sets are then attached to subnets and determine which DNS queries are allowed, blocked or merely audited at that point in the hierarchy.

Zones

A zone groups a set of [resolvers](#) managed under one configuration. A zone can be internal (for the corporate network) or external (for [end devices](#) outside the network). An external zone has a DoH URL set, to which the client applications on devices connect. Each zone contains exactly one root subnet, from which the entire subnet hierarchy descends.

Subnets

A subnet is defined by IPv4 or IPv6 address ranges and may contain any number of further subnets as children. The subnet tree makes it possible to structure the corporate network according to its actual topology. One or more [rule sets](#) can be attached to each subnet. A subnet inherits the rule sets settings of its parent, however it can be rewritten.

Rule sets

A rule set is a named list of domain names. A set can be either in the form of a block list (blacklist) or an exception list (whitelist). It can optionally have an attached ML model for evaluating queries beyond the static list.

A rule set is [attached to a subnet](#) with a specific action: `allow`, `block` or `audit` (record the query without blocking). The resulting zone configuration is published to the resolvers via [Kafka](#).

Web portal



The web portal is used to configure the behaviour of the DNS PATROL system. You can find it at <https://jezek.nic.cz/> ↗. To log in to the administration portal, use one of the offered authentication methods, e.g. mojID.

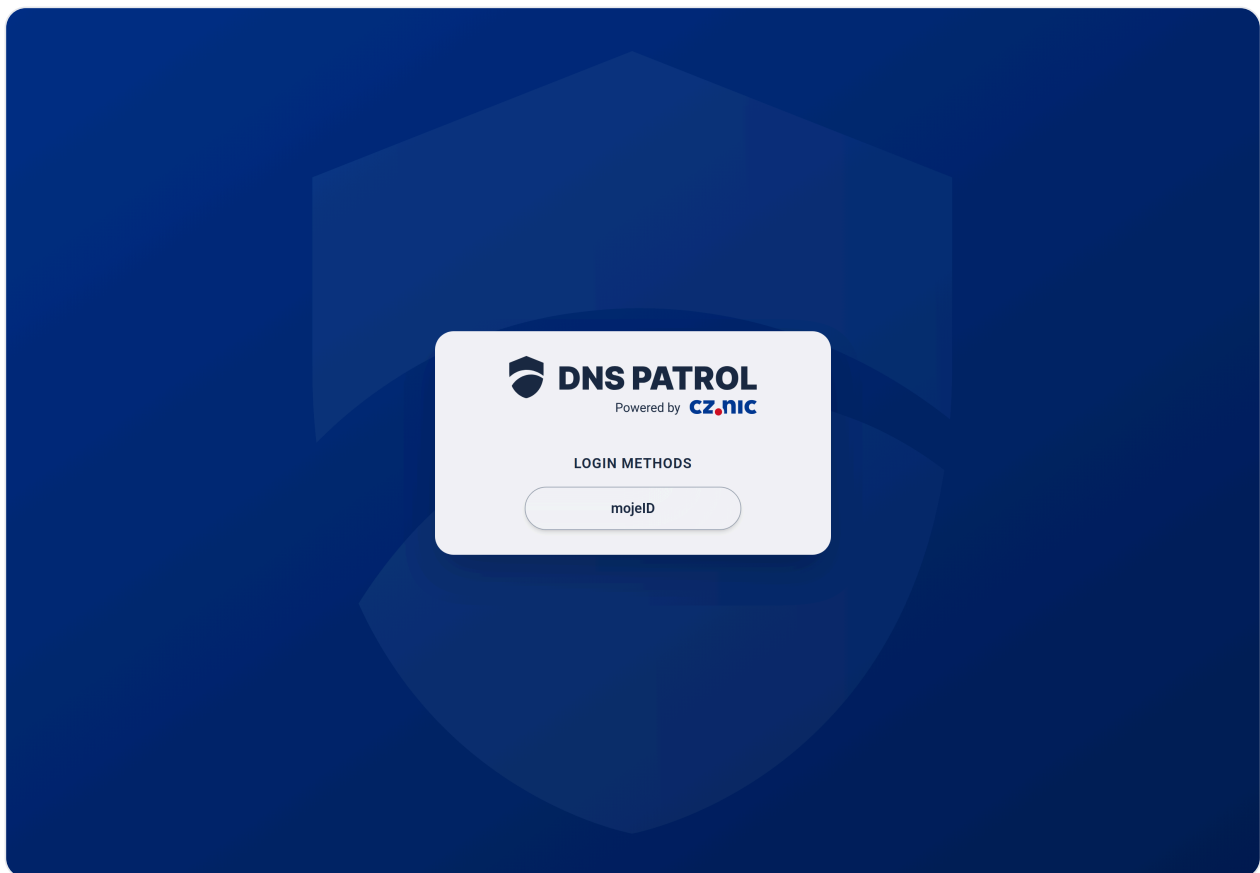


Figure 2 The sign-in page with the available authentication methods.

3.1 Navigation panel

After signing in, a side panel is used to navigate the application. At its top you can see the signed-in user's name and the roles assigned to them, which determine which sections of the application they can browse and modify. Besides navigation links to the various sections of the application (described in more detail further on), it also contains a sign-out button.

The navigation panel can be collapsed with the 'Collapse' button at its bottom, or expanded again by clicking the double-arrow icon.

About

The [About](#) page contains licence information and other details about the application and the DNS PATROL system.

What's new

A quick overview of application changes for each released version.

Sign out

Signs the current user out.

3.2 Working with tables

The following behaviour is shared by the tables in all sections of the administration portal.

Column visibility. The columns icon next to the table title opens the [Column settings](#) window. There you can show or hide a column with its checkbox, search the columns by name, restore the default set with the [Reset](#) button and confirm the changes with [Save](#). The settings are stored per user and per table.

Column width. A column can be resized by dragging the edge in the table header. Double-clicking the same edge returns that column to its default width.

Clearing filters, sorting and widths. When a table has an active filter, sorting or a custom column width, a bar appears above it with the [Clear all filters](#), [Clear sorting](#) and [Reset column widths](#) buttons. Each one is shown only when there is something to clear.

Keeping filters. By default, filters and sorting are discarded when you leave the page. The [Save table filters](#) option in the [Settings](#) section turns on their automatic restoration when you return to the page.

Searching in dropdowns. Dropdowns with fields and parameters are sorted alphabetically and contain a search box. Just start typing to narrow the list down.

Feature announcements

New features are announced directly on the page where they can be used. The window with the demo can be dragged aside so that you can try the feature straight away; use the arrows or the dots below the demo to move between individual announcements. A closed window can be reopened with the light bulb button, which can be moved anywhere on the screen.

Overview



In the **Overview** section, the signed-in administrator can build their own Dashboard and customise it to their preferences. The Dashboard is made up of widgets that can be freely added, moved by drag-and-drop, and resized. Widgets are added with the + button in the bottom-right corner of the Dashboard, or from any other page of the application by clicking the dashboard icon next to the relevant table or chart. The layout is saved per user.

Widgets can be moved by dragging the top edge and resized by dragging the bottom-right corner. Clicking the cross icon in the top-right removes the widget; clicking the link icon navigates to the related page in the application.

The screenshot shows the DNS PATROL Overview page. On the left is a sidebar with the user 'Pepa Uživatel' (Super User) and navigation links: Dashboard, DNS Management, Access Control, Analytics, Settings, About, What's new, and Logout. The main area contains several widgets:

- RCode Distribution ...**: A widget for monitoring DNS response codes, showing a time range (2026-09-20 11:22 to 2026-09-21 11:22) and a step (Day).
- Zones: All**: A table listing DNS zones.

Name	Gateway IPv4	Gateway IPv6	DoH URL
REGNET	10.20.0.1	2001:db8:200::1	-
LAN Org	10.30.0.1	2001:db8:300::1	-
- Subnets: All**: A table listing subnets.

Name	IPv4 ranges	IPv6 ranges
REGNET root subnet	10.20.0.0/16	2001:db8:200::/48
Nemocnice Praha fiktivní	10.20.10.0/24	2001:db8:200:10::/48
Nemocnice - ambulance	10.20.10.0/25	-
Nemocnice - lůžková oddělení	10.20.10.128/25	-
- Devices: All**: A table listing devices.

Name	Group	Device Token	Hostnam
NB-IT-001	Správci sítě	d340d493-6b3c-49f7-a089-e45beae0d0ce	nb-it-001
- Resolvers: All**: A table listing DNS resolvers.

Hostname	Zone	IPv4 addresses	IPv6 addresses	Master Resolver	Status
resolver-regnet-01.example.com	REGNET	10.20.0.10 10.20.0.11	2001:db8:200::10	Yes	✓
resolver-regnet-02.example.com	REGNET	10.20.0.12	2001:db8:200::12	No	✓
- Rule sets: All**: A table listing rule sets.

Name	Description	Rule set type	Source
003nic-wl-ti-denylisty	Whitelist internal safe domains CZ DENY LISTY	Whitelist	internal
001nic-bl-malware	Domény šířící malware, sdílené zdroje CZ NIC	Blocklist	feed

A '+ Collapse' button is at the bottom left, and a '+' button is at the bottom right.

Figure 3 The Overview page with configured widgets.

4.1 Adding a widget

Available widgets include overview tables for zones, subnets, resolvers, rule sets, users, devices and registration codes, as well as widgets with charts and tiles from the Statistics page.

Clicking the  icon in the bottom-right corner opens a picker that lets you choose a section (DNS management, Access control or Analytics), then a page within that section, and finally a specific tile on that page. Once you confirm the selection, the widget is added to the Dashboard.

Alternatively, you can add a widget directly from any other page of the application by clicking the dashboard icon next to the relevant table or chart.

DNS management



The DNS Settings section has several subsections: Zones, Resolvers, Subnets, Rule sets, and Logs history. Everything in this part of the administration portal relates to DNS configuration for use with the DNS PATROL application.

5.1 Zones

A zone is a logical network that the portal needs for resolver configuration.

After clicking on the [Zones](#) tab, a table appears displaying all created zones.

Name	Gateway IPv4	Gateway IPv6	DoH URL	External Zone
REGNET	10.20.0.1	2001:db8:200::1	-	No
LAN Org	10.30.0.1	2001:db8:300::1	-	No
Školy	10.40.0.1	-	https://doh.skoly.example.com/dns-query	No
Úřad	10.50.0.1	-	-	No
Knihovny	10.60.0.1	-	-	No
Guest Wi-Fi	172.16.0.1	-	-	No
Sociální služby	10.70.0.1	-	-	No
EXT	192.0.2.49	2001:db8:ffff::49	https://dns.example.com/dns-query	Yes

Figure 4 The zones table.

Each zone contains the following parameters:

Item	Description
Name	Name of the zone
Gateway IPv4	A device (router) with an IPv4 address that serves as a link between the local network and the external world
Gateway IPv6	A device (router) with an IPv6 address that serves as a link between the local network and the external world
DoH URL	Address of the DNS over HTTPS server
External Zone	Indicates whether this is an external zone

A new zone can be created using the [Add Zone](#) button in the top right corner of the administration portal. Then you need to fill in the individual parameters and click [Save](#).

After clicking on a specific zone in the table, its details appear, and it can be further edited using the gear icon button in the top right corner of the screen.

Besides the parameters entered when the zone was created, the details show **RPZ count** (how many RPZ files apply in the zone based on the rule sets used on its subnets) and **Config last published at** (when the zone configuration was last successfully published to the resolvers).

On this page, in the **Subnet** section, you can see the specific subnet to which the given zone belongs. In the **Resolvers** section, there is a table with resolvers belonging to this zone.

The screenshot shows the DNS PATROL interface. On the left is a sidebar with the user 'Pepa Uživatel Super User' and navigation links: Dashboard, DNS Management (expanded), Zones, Resolvers, Subnets, Rule sets, Access Control, Analytics, Settings, About, What's new, and Logout. The main content area is titled 'Zone: REGNET' and contains three sections: 'Zone' details, 'Subnet' details, and 'Resolvers' table.

Zone: REGNET

- Name: REGNET
- Gateway IPv4: 10.20.0.1
- Gateway IPv6: 2001:db8:200::1
- DoH URL: -
- External Zone: No
- RPZ count: 7
- Config last published at: 21/09/2026, 09:20:00 CEST

Subnet

- Name: REGNET root subnet
- IPv4 ranges: 10.20.0.0/16
- IPv6 ranges: 2001:db8:200::/48

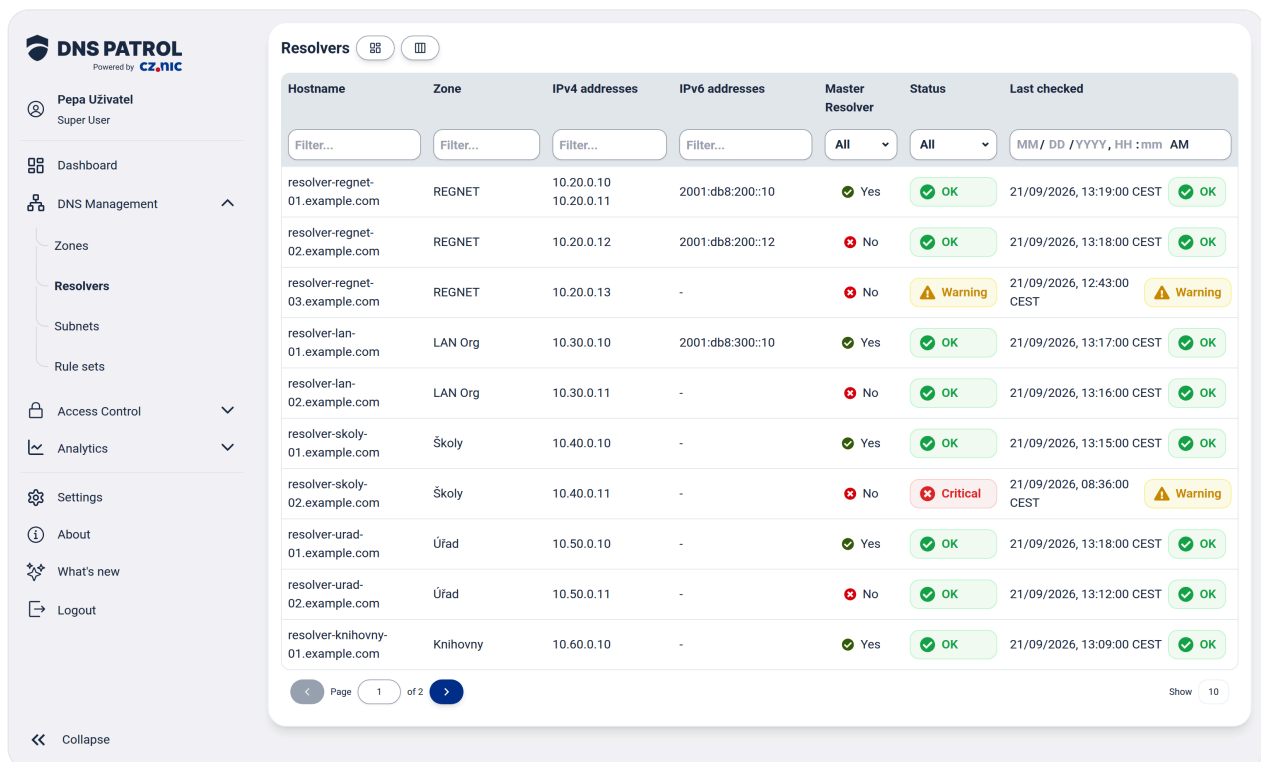
Resolvers

Hostname	IPv4 addresses	IPv6 addresses
resolver-regnet-01.example.com	10.20.0.10 10.20.0.11	2001:db8:200::10
resolver-regnet-02.example.com	10.20.0.12	2001:db8:200::12
resolver-regnet-03.example.com	10.20.0.13	-

Figure 5 Zone details with the linked subnet and its resolvers.

5.2 Resolvers

After clicking the **Resolvers** section, a table appears displaying all created resolvers.



The screenshot shows the 'Resolvers' section of the DNS PATROL interface. It features a table with columns: Hostname, Zone, IPv4 addresses, IPv6 addresses, Master Resolver, Status, and Last checked. The table lists 12 resolvers. The status column uses icons: a green checkmark for 'OK', a yellow warning triangle for 'Warning', and a red X for 'Critical'. The last checked column shows the date and time in CEST format. The interface also includes a sidebar with navigation links like Dashboard, DNS Management, Zones, Resolvers, Subnets, Rule sets, Access Control, Analytics, Settings, About, What's new, and Logout. The top of the table has filter inputs for Hostname, Zone, IPv4, and IPv6, and dropdowns for Master Resolver and Status.

Hostname	Zone	IPv4 addresses	IPv6 addresses	Master Resolver	Status	Last checked
resolver-regnet-01.example.com	REGNET	10.20.0.10 10.20.0.11	2001:db8:200::10	Yes	OK	21/09/2026, 13:19:00 CEST
resolver-regnet-02.example.com	REGNET	10.20.0.12	2001:db8:200::12	No	OK	21/09/2026, 13:18:00 CEST
resolver-regnet-03.example.com	REGNET	10.20.0.13	-	No	Warning	21/09/2026, 12:43:00 CEST
resolver-lan-01.example.com	LAN Org	10.30.0.10	2001:db8:300::10	Yes	OK	21/09/2026, 13:17:00 CEST
resolver-lan-02.example.com	LAN Org	10.30.0.11	-	No	OK	21/09/2026, 13:16:00 CEST
resolver-skoly-01.example.com	Školy	10.40.0.10	-	Yes	OK	21/09/2026, 13:15:00 CEST
resolver-skoly-02.example.com	Školy	10.40.0.11	-	No	Critical	21/09/2026, 08:36:00 CEST
resolver-urad-01.example.com	Úřad	10.50.0.10	-	Yes	OK	21/09/2026, 13:18:00 CEST
resolver-urad-02.example.com	Úřad	10.50.0.11	-	No	OK	21/09/2026, 13:12:00 CEST
resolver-knihovny-01.example.com	Knihovny	10.60.0.10	-	Yes	OK	21/09/2026, 13:09:00 CEST

Figure 6 The resolvers table with the status of each server.

A resolver is a program that responds to DNS queries and determines where the administration portal uploads configuration files.

Each resolver contains the following parameters:

Item	Description
Hostname	A unique name assigned to each device in the network, replacing numeric IP addresses
Zone	The zone in which the resolver is located
IPv4 addresses	IPv4 addresses of the individual devices in the network
IPv6 addresses	IPv6 addresses of the individual devices in the network
Master Resolver	Indicates whether this is the resolver to which queries are primarily sent
Status	Resolver status, whether it shows any errors
Last checked	Date and time when the resolver was last checked

After clicking on an individual resolver in the table, its details are displayed. In the **Zone** section, you can see which zone the resolver belongs to.

5.3 Subnets

In the Subnets section, you will find a table with created parent networks and child subnets.

The screenshot displays the DNS PATROL interface. On the left is a sidebar with navigation links: Dashboard, DNS Management (expanded), Zones, Resolvers, Subnets, Rule sets, Access Control, Analytics, Settings, About, What's new, and Logout. The main content area is titled 'Subnets' and features a '+ Add subnet' button. Below this is a table with columns: Name, IPv4 ranges, IPv6 ranges, and Parent subnet. The table lists several subnets, including 'REGNET root subnet', 'Nemocnice Praha fiktivní', and 'Účtárna'. Below the table is a 'Subnet structure' section with a 'Change subnet structure' button and a 'Graph layout' button. It shows a hierarchical tree diagram of the subnets. The tree starts with 'All roots (8)' and branches down into various subnets, including 'REGNET root subnet', 'Nemocnice Praha fiktivní', and 'Účtárna'. The diagram is interactive, with search and zoom controls on the right.

Name	IPv4 ranges	IPv6 ranges	Parent subnet
REGNET root subnet	10.20.0.0/16	2001:db8:200::/48	-
Nemocnice Praha fiktivní	10.20.10.0/24	2001:db8:200:10::/64	REGNET root subnet
Nemocnice - ambulance	10.20.10.0/25	-	Nemocnice Praha fiktivní
Nemocnice - lůžková oddělení	10.20.10.128/25	-	Nemocnice Praha fiktivní
Poliklinika Fiktivní	10.20.11.0/24	2001:db8:200:11::/64	REGNET root subnet
Hřbitov fiktivní Brno	10.20.12.0/24	-	REGNET root subnet
Záchraná služba Fiktivní	10.20.13.0/24	-	REGNET root subnet
LAN Org root subnet	10.30.0.0/16	2001:db8:300::/48	-
Ředitelství	10.30.1.0/24	2001:db8:300:1::/64	LAN Org root subnet
Účtárna	10.30.2.0/24	-	LAN Org root subnet

Figure 7 The subnets table and the diagram of their tree structure.

Each subnet contains the following parameters:

Item	Description
Name	Name of the subnet
IPv4 ranges	Range of IPv4 addresses in this subnet
IPv6 ranges	Range of IPv6 addresses in this subnet
Parent subnet	The subnet that is the parent of the current one

A new subnet can be created using the [Add Subnet](#) button in the top right corner of the administration portal. Then you need to fill in the parameters and click [Save](#). Multiple IPv4 or IPv6 ranges can be added to a single subnet.

Below the subnet table, there is a graphical structure of the networks, which can be edited using the [Change subnet structure](#) button on the right side of the screen. You can also adjust how graphs are displayed using the [Graph Layout](#) button. To add another subnet within the structure, click the [+](#) button next to the desired subnet.

After clicking on a subnet in the table or graph, you will see its details, which can be further edited. Here you will find information about the subnet, including the [Applied RPZ count](#) (how many RPZ files apply to this subnet and its child subnets), its parent subnet, and a list of child subnets.

You will also find a table of rule sets applied to the subnet. You can assign rule sets using the pencil icon above the table on the right side of the screen. From the list of rule sets, choose which one you want to use and set its state using the slider:

- **Enable:** the rule set is applied to the subnet, domains from the list are blocked or allowed according to the rule set type (Blocklist or Whitelist)
- **Audit:** domains from the rule set are monitored and logged only, without being blocked or allowed
- **Disable:** the rule set is not applied to the subnet
- Then click [Save](#) .

The opened subnet also contains a [Realtime logs](#) section, where you can monitor what was blocked and check access to domains from the rule set configured as [Audit](#) .

Subnet: Nemocnice Praha fiktivní

Name: Nemocnice Praha fiktivní
 IPv4 ranges: 10.20.10.0/24
 IPv6 ranges: 2001:db8:200:10::/64
 Applied RPZ count: 2

Parent subnet

Name: REGNET root subnet
 IPv4 ranges: 10.20.0.0/16
 IPv6 ranges: 2001:db8:200::/48

Child subnets

Name	IPv4 ranges	IPv6 ranges
Nemocnice - ambulance	10.20.10.0/25	-
Nemocnice - lůžková oddělení	10.20.10.128/25	-

Applied rule sets

Name	Description	Mode	Source
011-lokalni-whitelist	Výjimky schválené správcem sítě	Allow	manual
004nic-bt-tunely	Detekce DNS tunelů, model strojového učení	Audit	internal

Realtime logs

Date and time (local)	DNS query name	Protocol	IP Version	Response code	Query type	Policy action	Policy rule	Score
21/09/2026, 13:22	streaming.netflix.co	ICMP	IPv4	NOERROR	RESERVED	PASS	ad_tracking	192
21/09/2026, 13:22	streaming.netflix.co	ICMP	IPv4	NOERROR	RESERVED	PASS	malware_block	217
21/09/2026, 13:22	0.pool.ntp.org	ICMP	IPv4	NOERROR	RESERVED	PASS	phishing_list	1.1
21/09/2026, 13:22	www.google.com	ICMP	IPv4	NOERROR	RESERVED	PASS	modul201	172
21/09/2026, 13:22	static.facebook.coi	ICMP	IPv4	NOERROR	RESERVED	PASS	default_allow	8.8
21/09/2026, 13:22	update.apple.com	ICMP	IPv4	NOERROR	RESERVED	PASS	parental_control	172
21/09/2026, 13:22	0.pool.ntp.org	ICMP	IPv4	NOERROR	RESERVED	BLOCK	phishing_list	172
21/09/2026, 13:22	telemetry.microsof	ICMP	IPv4	NOERROR	RESERVED	PASS	modul201	172
21/09/2026, 13:22	fonts.googleapis.co	ICMP	IPv4	NOERROR	RESERVED	PASS	ad_tracking	10.1
21/09/2026, 13:22	ads.doubleclick.ne	ICMP	IPv4	NOERROR	RESERVED	PASS	parental_control	172
21/09/2026, 13:22	0.pool.ntp.org	ICMP	IPv4	NOERROR	RESERVED	PASS	default_allow	172
21/09/2026, 13:22	update.apple.com	ICMP	IPv4	NOERROR	RESERVED	BLOCK	ad_tracking	172

Figure 8 Subnet details with child subnets, applied rule sets and realtime logs.

Real-time logs

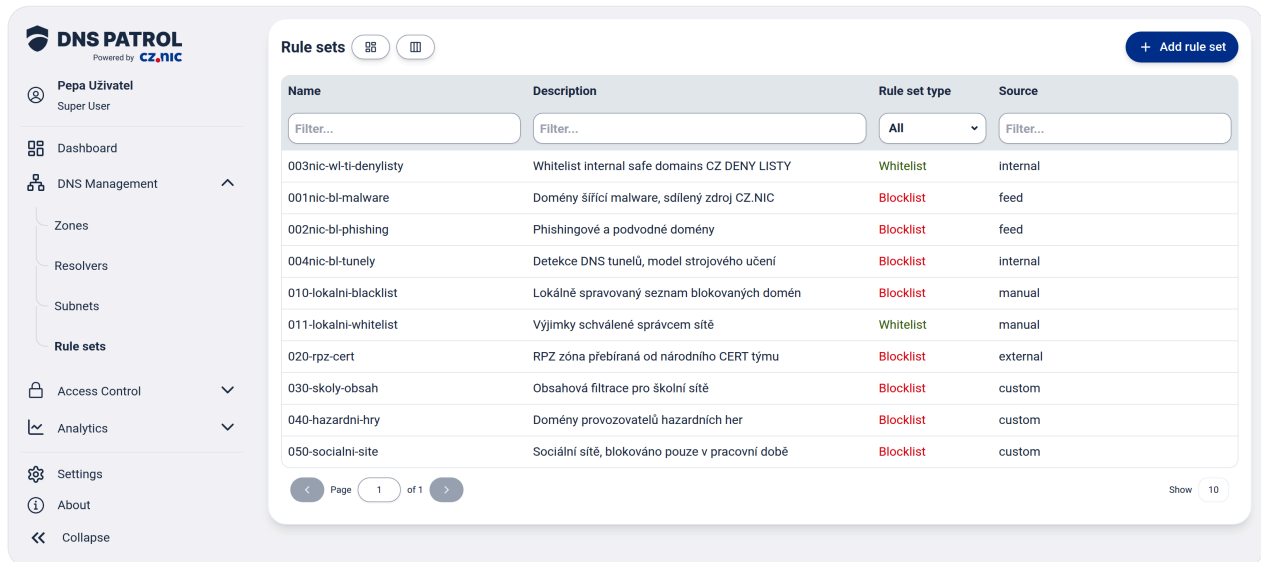
An example how to read the data in logs.

Response code	Policy action	Policy rule	Meaning
NXDOMAIN	-	-	domain is not accessible
NXDOMAIN	BLOCK	-	domain blocked by the resolver based on internal resolver rules
NXDOMAIN	BLOCK	modul201	domain blocked by the resolver based on given Rule set modul201 set up to Block

5.4 Rule Sets

Rule sets contain individual lists of domains that can be used as:

- **Blocklist:** these domains will be blocked (red color)
- **Whitelist:** these domains are allowed (green color)



Name	Description	Rule set type	Source
003nic-wl-ti-denylisty	Whitelist internal safe domains CZ DENY LISTY	Whitelist	internal
001nic-bl-malware	Domény šířící malware, sdílený zdroj CZ.NIC	Blocklist	feed
002nic-bl-phishing	Phishingové a podvodné domény	Blocklist	feed
004nic-bl-tunely	Detekce DNS tunelů, model strojového učení	Blocklist	internal
010-lokalni-blacklist	Lokálně spravovaný seznam blokovanych domén	Blocklist	manual
011-lokalni-whitelist	Výjimky schválené správcem sítě	Whitelist	manual
020-rpz-cert	RPZ zóna přebíraná od národního CERT týmu	Blocklist	external
030-skoly-obsah	Obsahová filtrace pro školní síť	Blocklist	custom
040-hazardni-hry	Domény provozovatelů hazardních her	Blocklist	custom
050-socialni-site	Sociální síť, blokováno pouze v pracovní době	Blocklist	custom

Figure 9 The rule sets table.

Each rule set contains the following parameters:

Item	Description
Name	Name of the rule set
Description	Purpose of the domain list associated with this rule
Domains	List of domains covered by this rule
Rule set type	Is the rule set Blocklist or Whitelist
Source	Origin of the rule set: internal for rule sets created and edited in the portal, or the name of the feed the rule set was imported from (e.g. external feeds picked up by the RPZ monitor)

A new rule set can be created using the **Add rule set** button in the top right corner of the administration portal. Then fill in the parameters and click **Save**. The rule set name must be alphanumeric with dashes only, no spaces or other special characters, and at least two characters long.

After clicking on a rule set in the table, more information about it is displayed.

The **Filtered Domains** table, a list of domains affected by this rule set, is only shown for rule sets with source **internal**. Imported rule sets are read-only and their domain list is managed by the import feed. For internal rule sets, individual domain patterns can be edited inline in the table, new domains can be added through the table's add-row input, and selected domains can be deleted with the trash bin button. The **Expand from CSV** button uploads a file of domains that will be added to the domain list. The **Replace from CSV** button replaces all domains in this set with domains from the uploaded file. The **Export to CSV** button downloads the domain list as a CSV file.

In the **Used on Subnets** section, you can see which subnets use this rule set.

The screenshot displays the DNS PATROL web interface. On the left is a sidebar menu with options: Dashboard, DNS Management (expanded), Zones, Resolvers, Subnets, Rule sets, Access Control, Analytics, Settings, About, What's new, Logout, and Collapse. The main content area shows the details for a rule set named '001nic-bl-malware'. The rule set type is 'Blocklist' and the source is 'feed'. Below this, a table titled 'Applied to subnets' lists subnets with their IPv4 and IPv6 ranges. The table has three filter input fields for Name, IPv4 ranges, and IPv6 ranges. The table contains five rows of data. At the bottom of the table, there is a pagination control showing 'Page 1 of 1' and a 'Show 10' button.

Rule set: 001nic-bl-malware

Name: 001nic-bl-malware
Description: Domény šířící malware, sdílený zdroj CZ.NIC
Rule set type: Blocklist
Source: feed

Applied to subnets

Name	IPv4 ranges	IPv6 ranges
REGNET root subnet	10.20.0.0/16	2001:db8:200::/48
LAN Org root subnet	10.30.0.0/16	2001:db8:300::/48
Úřad root subnet	10.50.0.0/16	-
Guest Wi-Fi root subnet	172.16.0.0/16	-
Sociální služby root subnet	10.70.0.0/16	-

Page 1 of 1 Show 10

Figure 10 Rule set details with the filtered domains.

On this page, it is also possible to edit the rule set's name, description, and type using the gear icon in the top right corner of the administration portal, or delete it using the red trash bin icon. The lock icon opens user permissions for the rule set.

Sorting: For better clarity, rule sets can be sorted by column by clicking on the column header. This works the same way in all other tables on all columns.

Access control



This section deals with user management: assigning permissions, organizing them into groups, and creating device codes.

6.1 Groups

Groups are a logical structure for categorizing users.

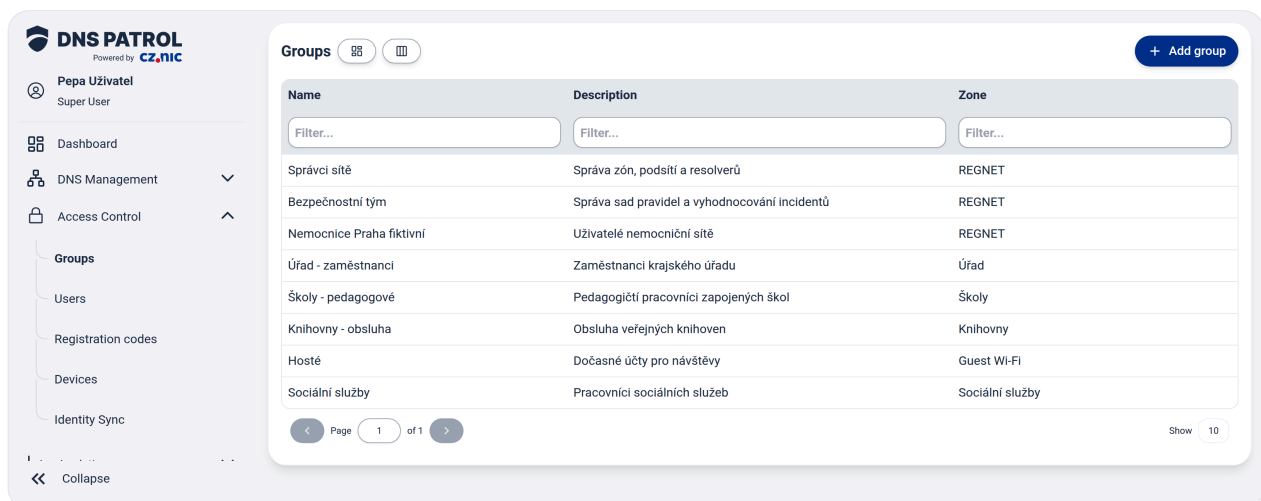


Figure 11 The groups table.

Groups contain the following parameters:

Item	Description
Name	Name of the group
Description	Description of the group
Zone	Zone to which the group belongs

After clicking on a group, you can edit it (gear icon in the top right corner) or delete it (red trash bin icon in the top right corner).

A new group can be created using the **Add Group** button in the top right corner of the administration portal. Then fill in the parameters and click **Save**.

Group: Nemocnice Praha fiktivní

Name: Nemocnice Praha fiktivní
 Description: Uživatelé nemocniční sítě
 Zone: REGNET
 Allow disabling app: ☒ Allow ☐ Prohibit
 App enabled: ☒ Enable ☐ Disable

Users in group

First name	Last name	E-mail	Role	Authorizations
Ondřej	Marek	ondrej.marek@example.com	Devices Access	mojeid
Markéta	Pospíšilová	marketa.pospisilova@example.com	Devices Access	mojeid
David	Král	david.kral@example.com	Subnets Access, Zones Access, Resolvers Access, Rulesets Access, Statistics Access, Users Access, Devices Access	mojeid

Figure 12 Group details with the list of its users.

6.2 Users

This subsection contains a list of users.

Users

Show deleted users ☐

First name	Last name	E-mail	Role	Group	Status	Created	Updated
Pepa	Uživatel	pepa.uzivatel@example.com	Super User	Správci sítě	Active	21/09/2025, 10:20:00 CEST	29/11/2025, 21:20:00 CET
Jana	Nováková	jana.novakova@example.com	Super User	Správci sítě	Active	03/10/2025, 08:20:00 CEST	19/12/2025, 21:20:00 CET
Petr	Svoboda	petr.svoboda@example.com	Subnets Access, Zones Access, Resolvers Access	Správci sítě	Active	15/10/2025, 10:20:00 CEST	16/11/2025, 14:20:00 CET
Lucie	Dvořáková	lucie.dvorakova@example.com	Subnets Access, Zones Access, Resolvers Access	Správci sítě	Active	27/10/2025, 05:20:00 CET	27/11/2025, 11:20:00 CET
Martin	Černý	martin.cerny@example.com	Rulesets Access, Statistics Access, Subnets Access	Bezpečnostní tým	Active	08/11/2025, 02:20:00 CET	29/01/2026, 12:20:00 CET
Tereza	Procházková	terez.prochazkova@example.com	Rulesets Access, Statistics Access, Subnets Access	Bezpečnostní tým	Active	20/11/2025, 09:20:00 CET	01/12/2025, 02:20:00 CET
Jakub	Kučera	jakub.kucera@example.com	Statistics Access	Bezpečnostní tým	Active	02/12/2025, 07:20:00 CET	21/02/2026, 13:20:00 CET
Eva	Veselá	eva.vesela@example.com	Statistics Access	Bezpečnostní tým	Active	14/12/2025, 04:20:00 CET	07/02/2026, 17:20:00 CET
Tomáš	Horák	tomas.horak@example.com	Devices Access, Users Access	Správci sítě	Active	26/12/2025, 09:20:00 CET	31/12/2025, 11:20:00 CET
Katerina	Němcová	katerina.nemcova@example.com	Devices Access, Users Access	Správci sítě	Active	07/01/2026, 02:20:00 CET	23/03/2026, 18:20:00 CET

Figure 13 The users table with assigned roles and groups.

Each user has the following parameters:

Item	Description
First Name	User's first name
Last Name	User's last name
Email	User's email address
Role	User role (Super user, access to selected parts of WA, no access)
Group	The group to which the user belongs
Created	When the user was created
Updated	When the user was last changed

A new user can be created using the **Add user** button in the top right corner of the administration portal. Then fill in the parameters and click **Save**.

After clicking on a user, detailed information appears. Users can be edited by clicking the gear icon in the top right corner of the portal, or deleted using the red trash bin icon.

In the **Devices** section, there is a list of devices used by the user. Here you can add a new device or generate a unique key (registration code) for DNS PATROL login by clicking the **+** button above the **Devices** table. You then need to fill in the following fields: Prefix (the prefix added before the device name), Usage Limit (how many devices can use the code), and **Expires At** (code validity in days), and click **Save**.

Each device contains the following parameters:

Item	Description
Hostname	Unique name assigned to each device in the network, replacing numeric IP addresses
Name	Device name
Device Token	Device identifier
MAC address	Device MAC address
Last login at	When the device last connected to the network

In the table, each device has a red trash bin icon that can be used to delete it.

User: Petr Svoboda Active

E-mail: petr.svoboda@example.com
 Role: Subnets Access, Zones Access, Resolvers Access
 Group: Správci sítě
 Authorizations: mojID

Allow disabling app: Allow Prohibit Reset
 App enabled: Enable Disable Reset
 Status: Restore Suspended

User permissions

Type	Name	User permissions
All	Filter...	All
Subnet	REGNET root subnet	Read + Write
Zone	REGNET	Read

Devices

Hostname	Name	Device Token	MAC address	Last login at	OS version
pc-it-003	PC-IT-003	17140708-4a1b-422e-8a9a-27cf67b5b3b9	02:00:92:dd:b4:c0	10/09/2026, 20:20:00 CEST	Windows 10 22H2
iph-it-029	IPH-IT-029	875c8d2a-b82c-47ae-995c-ae082442ad2e	02:00:06:6e:f0:ac	14/09/2026, 20:20:00 CEST	iOS 17.6

Page 1 of 1 Show 10

Figure 14 User details with the list of their devices.

User invitation

A user who has no login provider linked yet can be sent an invitation. The add-user icon in the top right part of the page opens the [Invite user](#) window, where the [Generate link](#) button creates a link with a limited validity. The link is single-use; generating a new one invalidates the previous one.

Opening the link takes the invited user to a welcome page where they link their login provider to the account. Whether they have already accepted the invitation is shown on the user detail in the [Authorizations](#) item.

Disabling the app

The user detail and the group detail control how the DNS PATROL application behaves on devices:

Item	Description
Allow disabling app	Allow / Prohibit : whether the user may turn the application off themselves
App enabled	Enable / Disable : whether the application is turned on

The values are inherited: a user takes over the settings of their group, a group takes over the system default. An inherited value is marked with an icon next to the selected option; picking another option overrides it for that user or group. The [Reset](#) button returns both items back to inheritance.

User Roles

User roles can be selected individually or multiple roles at once. Individual access rights are combined.

User Roles	Role ID	Displayed sections in WA
Super User	super_user	access to all sections in Administration portal
Subnet Access	subnets_viewer	access to section Subnets
Zones Access	zones_viewer	access to section Zones
Resolvers Access	resolvers_viewer	access to section Resolvers
Rulesets Access	rulesets_viewer	access to section Rule sets
Statistics Access	statistics_viewer	access to section Analytics: Statistics, Logs history, Passive DNS, Files
Users Access	users_viewer	access to sections Groups and Users
Devices Access	devices_viewer	access to sections Registration Codes and Devices
No Access to DNS Management	no_role	access only to Dashboard

Read, write, and delete access settings are configured as follows: [Access control](#) > [Groups](#) > click on the group I want to edit > information about the group and a list of users will be displayed > clicking on the lock icon in the upper right corner will open a dialog box with all users > I can choose one of three options for each user > save with the [Save](#) button.

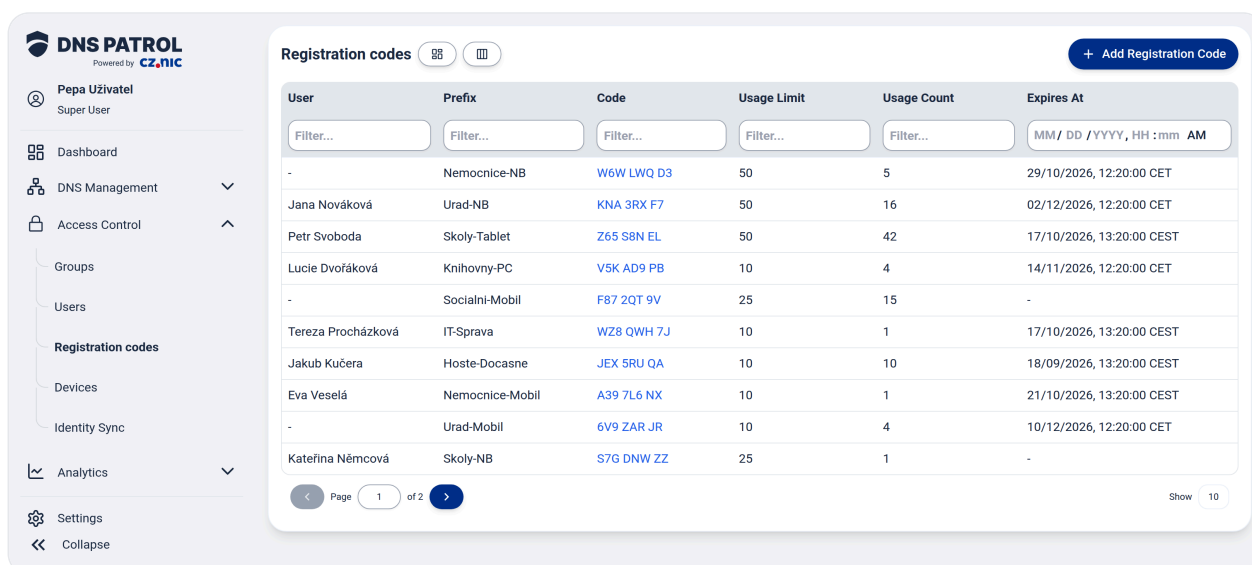
6.3 Registration Codes

This subsection lists the individual registration codes used when registering a device after launching the DNS PATROL application for the first time.

The individual registration codes then contain the following parameters:

Item	Description
First name	User's first name
Last name	User's last name
Prefix	Prefix preceding the device name
Code	Registration code for the DNS PATROL application
Usage limit	Number of devices on which the code may be used
Number of uses	Number of devices on which the code has been used
Expires on	Date on which the code will expire

A new registration code can be created using the [Add registration code](#) button in the upper right corner of the administration portal. Then, fill in the individual parameters and click on the [Save](#) button.



The screenshot shows the DNS PATROL interface. On the left is a sidebar with navigation links: Dashboard, DNS Management, Access Control, Groups, Users, Registration codes (selected), Devices, Identity Sync, Analytics, Settings, and Collapse. The main content area is titled 'Registration codes' and features a table with columns: User, Prefix, Code, Usage Limit, Usage Count, and Expires At. Each column has a 'Filter...' input. A '+ Add Registration Code' button is in the top right. The table contains 10 rows of data. At the bottom, there is a pagination bar showing 'Page 1 of 2' and a 'Show 10' button.

User	Prefix	Code	Usage Limit	Usage Count	Expires At
-	Nemocnice-NB	W6W LWQ D3	50	5	29/10/2026, 12:20:00 CET
Jana Nováková	Urad-NB	KNA 3RX F7	50	16	02/12/2026, 12:20:00 CET
Petr Svoboda	Skoly-Tablet	Z65 S8N EL	50	42	17/10/2026, 13:20:00 CEST
Lucie Dvořáková	Knihovny-PC	V5K AD9 PB	10	4	14/11/2026, 12:20:00 CET
-	Socialni-Mobil	F87 2QT 9V	25	15	-
Tereza Procházková	IT-Sprava	WZ8 QWH 7J	10	1	17/10/2026, 13:20:00 CEST
Jakub Kučera	Hoste-Docasne	JEX 5RU QA	10	10	18/09/2026, 13:20:00 CEST
Eva Veselá	Nemocnice-Mobil	A39 7L6 NX	10	1	21/10/2026, 13:20:00 CEST
-	Urad-Mobil	6V9 ZAR JR	10	4	10/12/2026, 12:20:00 CET
Kateřina Němcová	Skoly-NB	S7G DNW ZZ	25	1	-

Figure 15 The registration codes table.

6.4 Devices

This subsection contains a list of all registered devices with the option to display only those that are not assigned to any user.

Each device contains the following parameters:

Item	Description
Name	Device name (including the prefix from the registration code)
Hostname	Device system name
MAC address	Device MAC address
User	User name (or button with the option to assign a user)
Email	User email
Last login	When the device last logged into the system

A new device code can be created using the [Add Device Code](#) button in the top right corner of the administration portal. Then fill in the parameters and click [Save](#).

DNS PATROL
Powered by **CZ.NIC**

Pepa Uživatel
Super User

- Dashboard
- DNS Management
- Access Control
- Groups
- Users
- Registration codes
- Devices**
- Identity Sync
- Analytics
- Settings
- About
- What's new
- Logout

Devices

Show unassigned devices only

Name	Group	Device Token	Hostname	MAC address	User	E-mail	Last Login	OS vers
NB-IT-001	Správci sítě	d340d493-6b3c-49f7-a089-e45beae0d0ce	nb-it-001	02:00:df:c7:77:79	Pepa Uživatel	pepa.uzivatel@example.com	15/09/2026, 15:20:00 CEST	Win 11.2
NB-IT-002	Správci sítě	4f5bea85-b0e9-48a4-9086-2b3b8ea78b08	nb-it-002	02:00:ff:7f:ff:0a	Jana Nováková	jana.novakova@example.com	18/09/2026, 21:20:00 CEST	Win 11.2
PC-IT-003	Správci sítě	17140708-4a1b-422e-8a9a-27cf67b5b3b9	pc-it-003	02:00:92:dd:b4:c0	Petr Svoboda	petr.svoboda@example.com	10/09/2026, 20:20:00 CEST	Win 10.2
MBP-IT-004	Správci sítě	aecd255d-0eb5-4869-9234-1f6db19a088b	mbp-it-004	02:00:63:68:f9:21	Lucie Dvořáková	lucie.dvorakova@example.com	09/09/2026, 10:20:00 CEST	mac 15.3
MBA-SEC-005	Bezpečnostní tým	0292a77c-7002-4be3-b74a-272d039552e8	mba-sec-005	02:00:31:c6:d8:56	Martin Černý	martin.cerny@example.com	17/09/2026, 03:20:00 CEST	mac 14.7
IPH-SEC-006	Bezpečnostní tým	d21cfd8c-dca5-4403-90e5-09a9206cb86a	iph-sec-006	02:00:73:0c:97:aa	Tereza Procházková	tereza.prochazkova@example.com	17/09/2026, 15:20:00 CEST	iOS
IPH-SEC-007	Bezpečnostní tým	01696150-32a5-4c54-969b-5c6e82673eea	iph-sec-007	02:00:1e:c7:14:65	Jakub Kučera	jakub.kucera@example.com	09/09/2026, 21:20:00 CEST	iOS
AND-SEC-008	Bezpečnostní tým	7a20de95-ec46-4e0c-8236-	and-sec-008	02:00:52:e1:af:b0	Eva Veselá	eva.vesela@example.com	10/09/2026, 15:20:00 CEST	Andri 15

Figure 16 The devices table.

6.5 Identity Sync

This subsection is available to the Super User role only and is used to monitor the automatic import of users from external identity sources.

Identity Sources

The **Identity Sources** table lists the configured sources and their current state:

Item	Description
Name	Source name
Type	Source type
Status	Whether the source is active or disabled
Sync state	Whether a synchronisation is currently running or the source is idle
Sync interval	How often the source is synchronised
Next run	How long until the next synchronisation
Last run	The result of the last run together with the number of created and updated users and the finish time

The **Sync Now** button in the last column starts a synchronisation of an active source manually, without waiting for the next scheduled run.

Identity Sync Runs

The [Identity Sync Runs](#) table lists the individual runs. The dropdown above the table limits it to the runs of a selected source.

Item	Description
Status	Whether the run finished with success or an error
Trigger	Whether the run was scheduled or started manually
Started at	When the run started
Finished at	When the run finished
Created Users	Number of newly created users
Updated Users	Number of changed users
Deactivated Users	Number of users deactivated based on the source
Failed Records	Number of records that could not be processed
Skipped	Number of soft-deleted and manually created users the synchronisation did not touch
Collapsed runs	How many identical consecutive runs are collapsed into the row
Error	The error message if the run failed

Clicking a row opens the [Run details](#) window with a summary of the run (status, trigger, duration) and with lists of the individual affected records - created and updated users, deactivated and skipped users, created user groups, and failed records together with the reason for the failure.

Analytics



This category contains various statistics from resolvers, passive DNS, and data from Cesnet Warden.

7.1 Statistics

In this section, you can view statistics and graphs related to the application's operation.

You can set the parameters for the displayed graphs (Step (Day, Hour, Minute), Time Range (From Date - To Date), Resolver, Domain, IP, Subnet, Country) at the top of the page. You can show or hide the filters by clicking the corresponding text [Show Filters](#) or [Hide Filters](#) next to the section title.

The set of visible tiles can be customised through the [Manage](#) button next to the section title.

- **Query Count** - The development of the number of DNS queries processed by the application.
- **QType Over Time** - The development of DNS queries, distinguishable by their type (e.g., A, NS, SOA, etc.). You can toggle the visibility of individual types on or off by clicking their name in the legend on the right side of the graph.
- **Top Domains** - A ranking of domains sorted by the frequency with which the application processed them. The total number of queries is listed for each domain.
- **Top Sources** - A ranking of source IP addresses sorted by the frequency with which they generated DNS queries. The total number of queries is listed for each IP address.
- **Top Servers** - A ranking of resolvers/servers sorted by the total number of DNS queries they processed. It shows which ones carried the heaviest load.
- **Country Distribution** - A world heatmap illustrating the geographical distribution of DNS queries. Color intensity corresponds to the total number of queries originating from the given country. The exact value for a specific country will be displayed when you hover the mouse cursor over the area.
- **QType RCode Matrix** - Display of the distribution of DNS query types (QType) by the return codes (RCode) the queries received after processing. The graph is used for visual assessment of whether the given query types (e.g., A, AAAA, MX, etc.) return with the expected result (NOERROR) or encounter errors such as SERVFAIL (server failure), NXDOMAIN (domain does not exist), REFUSED (query rejected), or NOTIMP (requested function is not supported). The count of individual query types within the given RCode will be displayed when you hover the mouse cursor over the respective column. You can toggle the visibility of QTypes on or off by clicking their name in the legend on the right side of the graph.
- **RCode Distribution Over Time** - The graph visualizes the simultaneous development of the frequency of individual return codes. You can toggle the visibility of individual return codes on or off by clicking their name in the legend on the right side of the graph.
- **Policy Actions** - A pie chart illustrating the overall distribution of DNS queries according to the action applied by the configured rule sets. The graph serves to assess what proportion of queries are PASS (allowed), BLOCK (blocked), or AUDIT (allowed and monitored). Exact numerical values will be displayed when you hover the mouse cursor over the respective slice.
- **Policy Actions by Rule** - A stacked bar chart showing which specific rule sets contribute to the final action taken on the query (PASS, BLOCK, AUDIT). The graph is used for visual assessment of the effectiveness and engagement of individual rules. You can toggle the visibility of individual rules on or

off by clicking their name in the legend on the right side of the graph. The exact count of queries for specific rules within the given action will be displayed when you hover the mouse cursor over the respective column.

- **QType Distribution** - A pie chart illustrating the overall distribution of DNS queries according to their type. Exact numerical values will be displayed when you hover the mouse cursor over the respective slice.
- **QPS by Server** - Visualization of the simultaneous development of load on individual resolvers/servers, measured in Queries Per Second (QPS). You can toggle the visibility of individual servers on or off by clicking their name in the legend.
- **NXDomain Over Time** - The development of the count of queries ending with the NXDOMAIN error (domain does not exist).
- **ServFail Over Time** - The development of the count of queries ending with the SERVFAIL error (server failure/unsuccessful processing).
- **Domain in Rule Sets** - Shows the Rule Sets that contain the filtered domain.

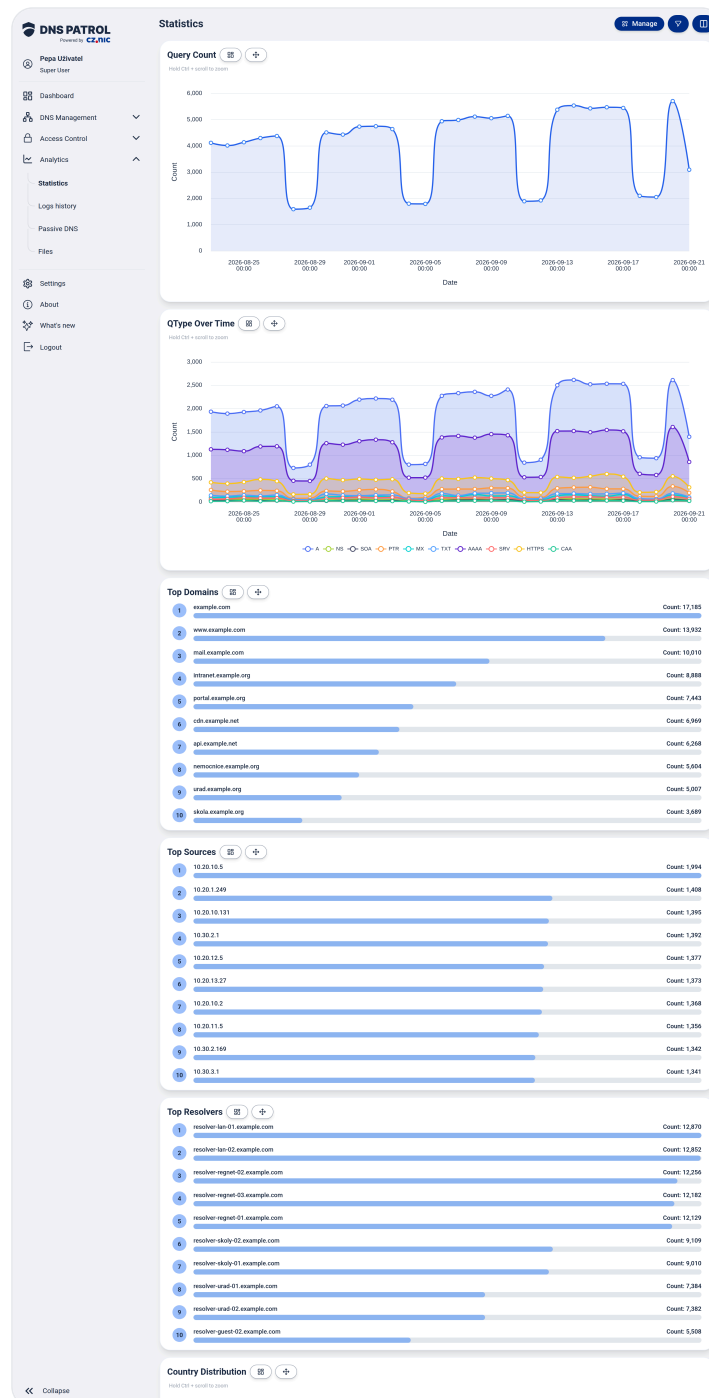


Figure 17 The Statistics page with charts for the last 30 days.

7.2 Logs history

This section allows you to obtain archival queries using filtering.

Searching works in basic and advanced modes. Basic mode allows filtering (with logical operators) and sorting, while advanced mode also supports aggregation and filtering within them. In the query builder, you can create the desired query and set a limit on the number of results. Results that meet the conditions are then displayed in the table below. Advanced mode can be enabled using the switch in the upper right corner of the screen.

The screenshot displays the DNS PATROL Analytics interface. On the left is a sidebar with the user profile 'Pepa Uživatel Super User' and a menu including Dashboard, DNS Management, Access Control, Analytics, Statistics, Logs history, Passive DNS, Files, Settings, About, What's new, and Logout. The main area is titled 'Query Builder' and includes a 'Conditions' section with a plus icon, a 'Sort' dropdown set to 'Select', and an 'Expression preview (SQL)' box showing 'SELECT * LIMIT 100;'. Below this are 'Search' and 'Reset' buttons, and 'Import JSON' and 'Export JSON' buttons with a 'Limit' of 100. The 'Logs history' section below features a table with columns: Date and time (local), DNS query name, Protocol, Response code, Query type, Policy action, Policy rule, Source IPv4, Source IPv6, Source IP (unified), User, Answer records, Authority records, and Additional records. Each column has a 'Filter' button. The table is currently empty, showing a 'No Data Available' message: 'The specified filter does not match any existing items.' The interface also includes a 'Collapse' button in the bottom left and an 'Advanced mode' toggle in the top right.

Figure 18 The Logs history page with the query builder.

Select field (advanced mode)

Specifies which columns are displayed in the table. In default mode, this field is not visible and all available columns are displayed. In SQL, this corresponds to the expression `SELECT [selection]`.

Aggregations (advanced mode)

Aggregations calculate a single summary value from several records (often defined in `Group by`) and store this value in a new field. Aggregations can be defined by a field and a function, and an alias can then be defined for this newly created field.

Aggregation can only be performed on selected fields (defined in `Select Field`).

Aggregation	Function
COUNT	Counts how many records contain a non-zero value in the field (supports wildcard *)
SUM	Adds up the numeric values in the field across all records (available only for numeric fields)
AVG	Calculates the average value of the field across all records (available only for numeric fields)
MIN	Finds the smallest value in the field across all records (works for both numbers and strings)
MAX	Finds the largest value in the field across all records (works for both numbers and strings)
COUNT DISTINCT	Counts how many unique non-zero records are in the field
MEDIAN	Calculates the median (middle value) across all records (available only for numeric fields)
STDDEV_POP	Calculates the population standard deviation - the measure of dispersion of numeric values
TO_START_OF_MINUTE	Groups the results of other defined aggregations by minutes
TO_START_OF_HOUR	Groups the results of other defined aggregations by hours
TO_START_OF_DAY	Groups the results of other defined aggregations by days
TO_START_OF_WEEK	Groups the results of other defined aggregations by week
TO_START_OF_MONTH	Groups the results of other defined aggregations by month
TO_START_OF_QUARTER	Groups the results of other defined aggregations by quarter
TO_START_OF_YEAR	Groups the results of other defined aggregations by year
TO_START_OF_FIVE_MINUTES	Groups the results of other defined aggregations by five minutes
TO_START_OF_TEN_MINUTES	Groups the results of other defined aggregations by ten minutes
TO_START_OF_FIFTEEN_MINUTES	Groups the results of other defined aggregations by fifteen minutes

Aggregations are not available in default mode.

Conditions

Conditions are applied to each record before aggregation (if applied). A condition can be applied to any item in the record. When you click on the [plus icon -> add condition](#), select the field, operator, and value. The selection of the operator is determined by the type of the field; for example, a number field can be filtered using mathematical operators such as less than/greater than, etc., and a string field can be filtered using the contains operator, etc. Fields can always be filtered using the operators [Equals](#), [Not equals](#), [Is null](#) (is empty), and [Is not null](#) (is not empty). In SQL, this corresponds to the expression [WHERE](#).

Individual conditions can be grouped using **groups**. A group can be created by clicking on the [plus icon -> add group](#). A group can contain other nested groups or conditions. Conditions/groups can then be combined using logical connectors AND/OR (and/or), which appear after adding two or more conditions/groups. The logical connector AND takes precedence over OR.

Filter	Function
Equals	Equality
Not equals	Inequality
Greater than or equal	Greater than or equal to (for numeric values)
Less than or equal	Less than or equal to (for numeric values)
Greater than	Greater than (for numeric values)
Less than	Less than (for numeric values)
In list	Present in the list of values
Not in list	Not present in the list of values
Contains	Contains (for text values; on IP fields, performs a substring match without IP validation)
Does not contain	Does not contain (for text values; on IP fields, performs a substring match without IP validation)
Starts with	Begins with the given prefix (for text values)
Ends with	Ends with the given suffix (for text values)
Is null	Is an empty value
Is not null	Is not an empty value

Some fields offer only a subset of these operators. **Country** accepts only **Equals**, **Not equals**, **Is null**, and **Is not null**. The IP source fields (**Source IPv4**, **Source IPv6**) accept only the equality, comparison, and list operators. The **User** and **Device** fields open a modal table from which one or more entities can be selected as the condition value; their button shows how many items are currently selected.

The date/time condition supports second-level granularity.

Group by (advanced mode)

Grouping combines records into groups where the specified field has the same value. Only fields that are selected (in **Select fields**) or created in **Aggregation** can be selected. Additional filters can be applied to these groups in **Having** .

Having (advanced mode)

Having applies conditions to the grouping created in **Group by** , unlike **Conditions** , which are applied earlier and for each record.

Filters are created similarly to **Conditions** , with the difference that only fields defined in **Aggregation** or **Group by** can be selected.

Sort by

Specifies the value by which to sort the results. After selecting a field, click the button next to the field name to select descending/ascending sorting.

If the user has applied the selected fields (**SELECT**) in advanced mode, filtering is only possible by these selected fields.

Search display

Displays the created query in a format similar to SQL. It serves illustrative purposes only; the actual query looks different (in reality, the executed query is more complex because, among other things, the access rights of the querying user are also applied to it).

Limit, saving queries, and search

In the lower right corner of the screen, you can apply a limit, i.e., how many results will be retrieved from the database and displayed. Using the 'Export JSON' button, you can download the current query as a file. It can be reused later by uploading it using the 'Import JSON' button.

In the lower left corner, you will find the Search button, which starts the search, and the Reset button, which clears the current query and returns the search to its default state.

Favorite queries

A query you use repeatedly can be saved. The heart button in the query builder header opens the favorite queries window, where the current query is saved under a name and an optional description.

The following actions are available for each saved query:

Action	Description
Apply	Loads the saved query into the builder
Update with current query	Overwrites the saved query with whatever is currently in the builder
Share	Opens the window for granting other users permissions to the query
Delete	Removes the saved query

The name of the active favorite query is shown on the heart button itself; it can be renamed with the pencil icon next to the name. If the query in the builder differs from the saved version, it is marked with an asterisk as unsaved changes, which can either be saved or discarded by reloading the saved version.

If someone else edits a saved query in the meantime, the portal points it out and lists which parts changed. Your unsaved changes are kept.

Next to the favorite queries button is the [Reset query](#) button, which returns the builder to its default state.

Sharing by link

The page address always carries the current query and the list of displayed columns. Copying the address from the browser therefore sends a colleague exactly what you have on screen; opening the link loads the query into the builder. For very large queries the link may get too long, in which case it is better to save the query as a favorite and share that.

Record history table

After running the filtering using the Search button, the results are displayed in the table at the bottom of the page. You can switch pages in the table if there are more results than the limit. Results can also be exported to a CSV file.

Above the table there are buttons for the column visibility settings and for switching the table to fullscreen. Fullscreen is left with the same button or with the Esc key. Adding a column fetches the data it needs on its own, there is no need to run the search again.

Cell context menu

Right-clicking any cell in the results opens a menu with the following options:

Option	Description
Equals	Adds a condition on the cell value to the builder
Not equals	Adds a condition excluding the cell value to the builder
Copy value	Copies the cell value to the clipboard
Open user details	Opens the user page from that row in a new tab (user column only)
Add domain to ruleset	Adds the domain from that row to a selected rule set (only when the domain column is shown)

The condition is added with an operator the given field supports; for an empty cell the first two options are replaced by `Is null` and `Is not null`. The builder updates immediately, the search then has to be run with the Search button.

Examples of complete queries

This query will display 500 (not necessarily the last) records with querying IP addresses in the specified range.

```
SELECT *
WHERE Source IPv4 >= '192.168.0.0'
AND Source IPv4 >= '220.0.0.0'
LIMIT 500;
```

This query will display the last date and time, DNS query name, and the number of unique clients from 100 records that meet the time inequality (at the time of writing, last week) and that, after grouping, have at least 10 unique querying clients. These records will be sorted in descending order by the number of queries.

```
SELECT MAX(Date and time (local)) AS last_seen,
COUNTDISTINCT(Source IP (unified)) AS unique_clients,
DNS query name
WHERE Date and time (local) >= 1762167600
GROUP BY DNS query name
HAVING unique_clients > 10
ORDER BY unique_clients DESC
LIMIT 100;
```

7.3 Passive DNS

This section is used to track the history of DNS record changes. In the upper right corner, you can enter the desired domain along with the record type. The corresponding results will be displayed in the table:

Item	Description
Record name	Domain searched
Record type	DNS record type
Response data	Corresponding record data
First sighting	This record was first sighted at this time
Last sighting	This record was last seen at this time
Count	Indicates how many times the resolver captured this record in DNS responses during the given time interval

7.4 Files

In the Files section, you can download lists of suspicious IP addresses from the Cesnet Warden project. These lists can then be used, for example, in a firewall.

The screenshot shows the DNS PATROL interface. On the left is a sidebar with navigation links: Dashboard, DNS Management, Access Control, Analytics, Statistics, Logs history, Passive DNS, Files, Settings, About, What's new, Logout, and Collapse. The main content area is titled 'Files' and shows a table of files with IP addresses from the Cesnet Warden project. The table has columns for Filename, Size, and Last Modified. Each row has a 'Download' button. The files listed are: README.txt, statistiky-2026-08.csv, tunnel-detection-v3.pt, allowlist-nemocnice.txt, denylist-2026-09-15.txt, rpz-cert-2026-09.rpz, dnspatrol-resolver-config.conf, and .gitkeep. The table also includes filter boxes for each column and pagination controls at the bottom.

Filename	Size	Last Modified	
Filter...	Filter...	Filter...	
README.txt	159.0 B	21/09/2026, 13:20:01	Download
statistiky-2026-08.csv	116.0 B	21/09/2026, 13:20:01	Download
tunnel-detection-v3.pt	61.0 B	21/09/2026, 13:20:01	Download
allowlist-nemocnice.txt	62.0 B	21/09/2026, 13:20:01	Download
denylist-2026-09-15.txt	126.0 B	21/09/2026, 13:20:01	Download
rpz-cert-2026-09.rpz	154.0 B	21/09/2026, 13:20:01	Download
dnspatrol-resolver-config.conf	125.0 B	21/09/2026, 13:20:01	Download
.gitkeep	0.0 B	21/09/2026, 13:15:46	Download

Figure 19 The table of downloadable files.

Item	Description
File name	File name
Size	File size
Last modified	Time of last file modification
Action	Button to download the file

Settings



In this section, you can change the language, color mode, or choose a different login method.

The **Save table filters** option turns on automatic saving of table filters and sorting. They are then restored when you return to the page; by default they are discarded once you leave it.

You can also set the buffer size for real-time logs. Higher values will cause more data to be stored and more frequent refreshing of results at the cost of higher memory and CPU usage.

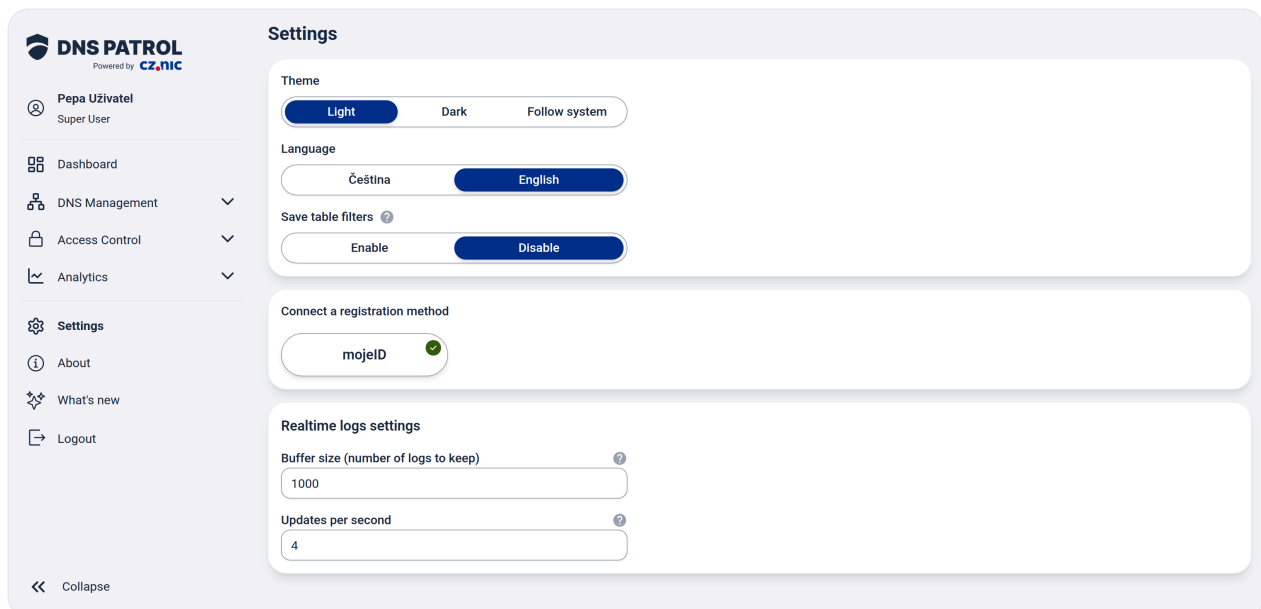


Figure 20 The Settings page.

What's new



On this page, you can see an overview of changes for each version of the application.

The [What's New](#) page provides an overview of changes in individual versions of the administration portal - new features, improvements, bug fixes, and removed features. A sidebar with a list of versions is located on the right side of the page, allowing you to quickly jump to the desired version.

The screenshot displays the 'What's new' sidebar in the DNS PATROL application. On the left is a navigation menu with items: Dashboard, DNS Management, Access Control, Analytics, Settings, About, What's new (active), and Logout. The main content area is titled 'What's new' and lists updates for versions v1.0.6, v1.0.5, v1.0.4, and v1.0.3. Each version entry includes a list of changes categorized as Added, Changed, or Fixed. A version sidebar on the right allows switching between these versions. At the bottom left of the sidebar is a 'Collapse' button.

What's new

v1.0.6 28/08/2026

- Added Controls to manage DNS Patrol app disablement permissions on the group and user level, along with new 'Created' and 'Updated' timestamp columns in tables
- Added Global column visibility controls for tables with customizable column toggles, persistent preference saving and a reset option
- Added Ability to resize columns by dragging their borders in the table header
- Added Improved table column layout with automatic width adjustment
- Added RPZ metrics and status on the Subnet and Zone detail pages
- Added Searchable dropdown menus with alphabetically sorted parameter lists, so finding and selecting specific fields is much faster
- Added Feature announcement system for onboarding, featuring a draggable modal with a GIF carousel and a restore button that can be minimized into the corner of the screen
- Added Add a domain to a ruleset directly from the Logs History table. Right-click the domain cell and you will find a new option in the menu
- Added Open the user's detail page from the Logs History results table. Right-click a user cell to see the menu option
- Added New user settings option to retain selected table filters and sorting even after leaving the page
- Added New button above the table to clear all filters and sorting at once
- Added Favorite Queries in Logs History allows you to save, manage and instantly load your filters, as well as share search stats with colleagues via a generated link
- Added User invitation system via time-limited links, a welcome onboarding page for login method selection, and invitation acceptance status tracking on the user profile page
- Added Enabled to build queries interactively by interacting directly with the data table on the Logs history page. Right-click any cell in the table to dynamically create a new condition node
- Changed The device condition node on the Logs History page now uses a modal table instead of a simple select, working the same way as the user condition node
- Fixed Adding a new column to the Logs History table now automatically refetches and displays the corresponding data without requiring a manual search click
- Fixed Values in the sort section dropdown on the Logs History page are now ordered alphabetically

v1.0.5 24/04/2026

- Added The possibility to create a widget from any page. When you open the page, you will see a button near header, which allows you to create a widget of this page
- Added Added a sidebar to the 'What's New' page to help you quickly jump between version updates
- Added You can now collapse the navigation bar to maximize your workspace
- Added Added a domain search table to Statistics. Use it to quickly find the specific rulesets associated with a given domain
- Added Statistics filters now include presets to easily filter data by different time ranges
- Added Updated the 'Logs History' user condition from a dropdown to a searchable table for faster results
- Added You can now hide or reveal columns on the 'Devices' page, including the new 'Group' column
- Added User permissions table on the User detail page
- Added Modal window to manage graph visibility on statistics page
- Added Support filtering statistics by subnet
- Added Optimized GenericTable performance and selection handling
- Changed Chart design for better clarity and user experience
- Fixed Performance issues on the Statistics page
- Fixed Performance issues on the Dashboard page
- Fixed Subnet overlap in the subnet tree when switching to an IP mask array
- Fixed User permissions table
- Fixed Table pagination

v1.0.4 20/02/2026

- Added Support for multiple IP ranges in a subnet
- Added Filtering by Subnet and Device names in the Query Builder
- Added 'E-mail' column in the Devices table
- Changed Improved dashboard widget UX/UI (ghost states, drag-and-drop, and minor design tweaks)
- Changed Minor design improvements
- Changed Optimized application performance
- Changed Improved sorting algorithm for inherited rule sets in the subnet details page
- Changed Added slider to manipulate rule set states in the subnet details page
- Fixed Navigation bar animation
- Removed IP range support for zones

v1.0.3 11/02/2026

- Added Dashboard widgets: configurable drag-and-drop dashboard with multiple widget types
- Added Ability to export queries to a file and import them later

⏪ Collapse

Version sidebar:

- v1.0.6 -
- v1.0.5 -
- v1.0.4 -
- v1.0.3 -

Figure 21 The What's new page with the version sidebar.

About



Contains information about the application, such as the current version, links to documentation, etc.

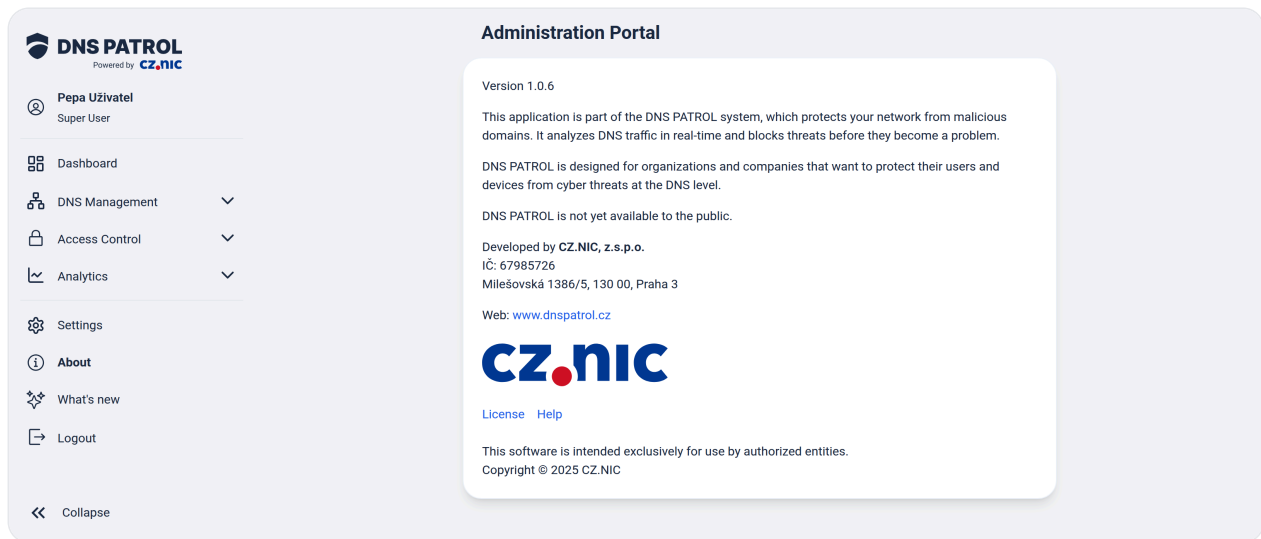


Figure 22 The About page.

Client applications



The client application is used by end devices that operate outside the organisation's network. Once registered, it routes all of the device's DNS traffic to the unique DoH URL of an [external zone](#), so the same [rule sets](#) apply to its queries as inside the network.

A device is registered with a one-time [registration code](#) issued to the user by an administrator in the portal. The code is 8 characters long and consists of uppercase letters and digits. Once verified, the device appears in the portal under [Access control](#) > [Devices](#).

The application has no further settings. The policy applied to a device is determined solely by the configuration in the administration portal.

11.1 Contents

[iOS](#): Application for iPhone and iPad [Android](#): Application for Android phones and tablets [Windows](#): Application for Windows computers [Browser extension](#): Explains blocks in Chrome and Edge

iOS



{/* TODO: add download links */}

The application for iPhone and iPad is installed from the App Store. On iOS, DNS traffic is not routed through a VPN but through the system DNS proxy interface, which has to be activated manually after installation.

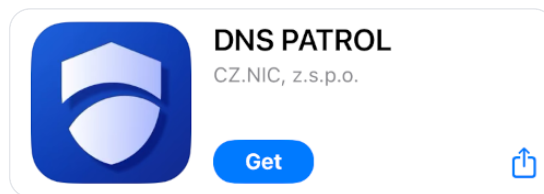


Figure 23 DNS PATROL in the App Store.

12.1 First launch

On first launch the application asks for a [registration code](#) issued by an administrator from the administration portal. The code is 8 characters long, consists of uppercase letters and digits, and is entered character by character into the fields below the [Enter the registration code](#) heading. The [Send](#) button verifies the code and the application moves on to its main screen.

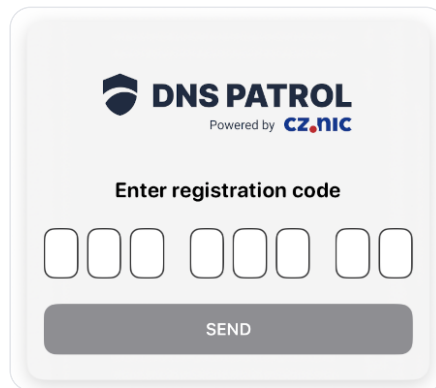


Figure 24 Entering the registration code on first launch.

12.2 Activating the DNS settings

Registration alone does not redirect the device's traffic yet. DNS PATROL has to be selected as the device's DNS in the system settings. A short version of the procedure is also available in the application under the [How to Activate](#) link.

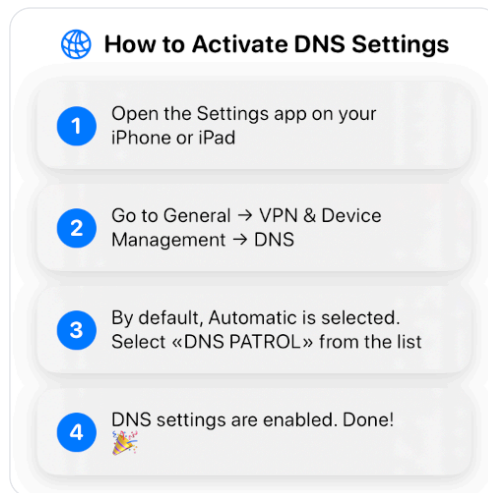


Figure 25 The **How to Activate** help screen in the application.

In the **Settings** app, open **General** and select **VPN & Device Management**.

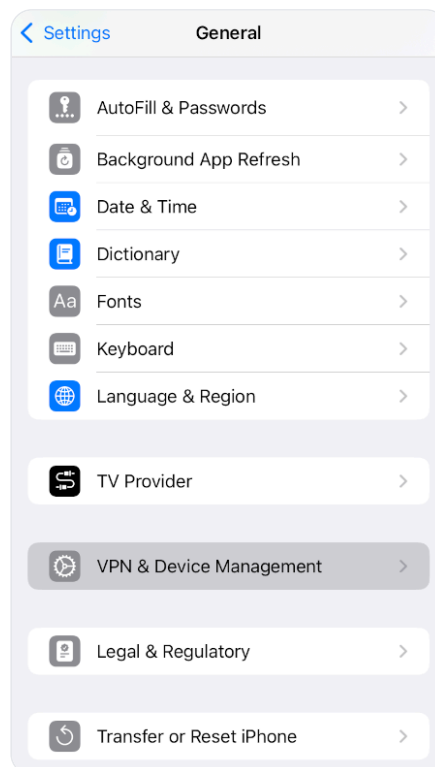


Figure 26 Settings > General > VPN & Device Management.

Under **RESTRICTIONS AND PROXY**, tap **DNS**.

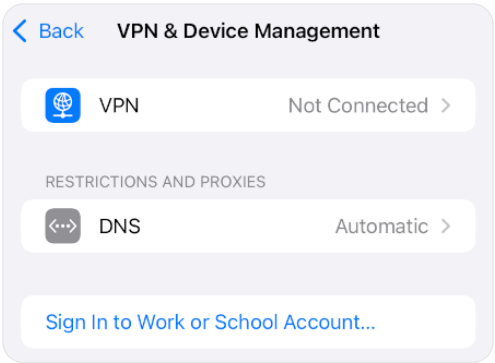


Figure 27 The DNS entry is set to Automatic by default.

Under **DNS PROXY AND DNS SETTINGS** , select **DNS PATROL** .

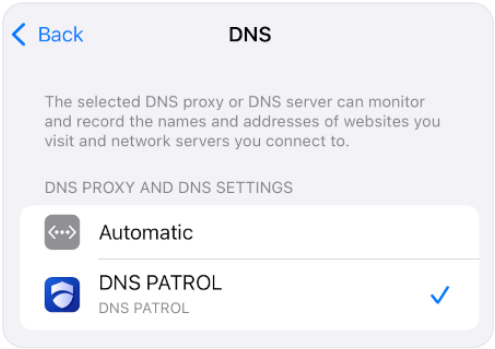


Figure 28 Selecting DNS PATROL instead of the automatic setting.

DNS PATROL is now active on the device. The setting can be verified by returning to the application, where the status changes to **Active** .

12.3 Main screen

The main screen shows the current status of the service:

Status	Description
Active	DNS PATROL is selected as the device's DNS and malicious traffic is blocked
Inactive	DNS PATROL is not active, queries are handled by the device's default DNS

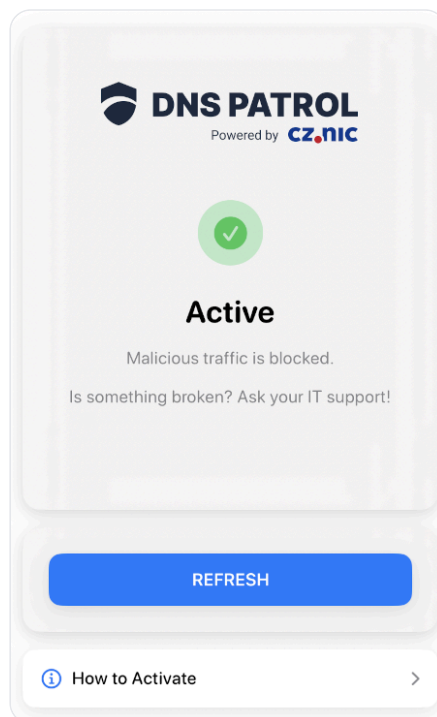


Figure 29 The Active status.

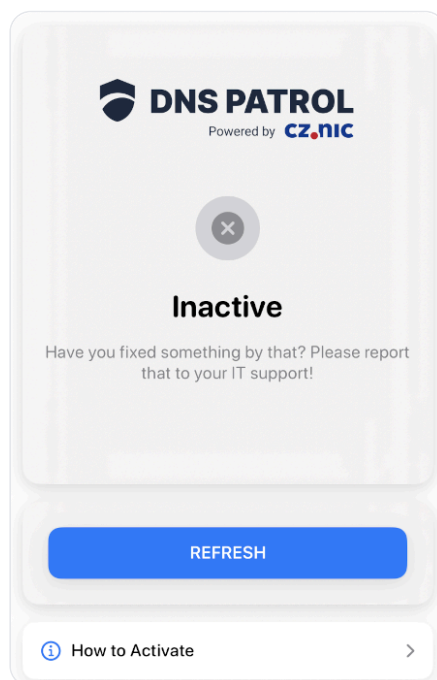


Figure 30 The Inactive status.

The [Refresh](#) button reloads the status of the service, for example after a change in the system settings. The [How to Activate](#) link expands the procedure for [activating the DNS settings](#).

12.4 Clearing the application data

The iOS application does not allow its data to be cleared from within. If the device needs to be registered again, that is with a different registration code, the application has to be uninstalled and installed from the App Store again.

The original device record stays in the portal under [Access control](#) > [Devices](#), where it can be deleted.

12.5 Reporting issues

Problems with the application or with websites and applications being unavailable are handled by the organisation's IT support.

Android



The application for Android phones and tablets is installed from Google Play. It routes the device's DNS traffic through a local VPN that the application creates on the device. The traffic does not leave the device through a VPN server. The interface only serves to capture DNS queries.

13.1 First launch

On first launch the application asks for a [registration code](#) issued by an administrator from the administration portal. The code is 8 characters long, consists of uppercase letters and digits, and is entered character by character into the fields below the [Enter the registration code](#) heading. The [Send](#) button verifies the code and the application moves on to its main screen.

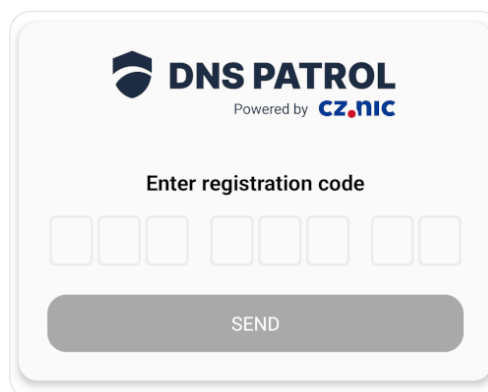


Figure 31 Entering the registration code on first launch.

13.2 Main screen

The main screen shows the current status of the service:

Status	Description
Active	DNS PATROL is running and malicious traffic is blocked, a key icon is shown in the status bar
Inactive	DNS PATROL is not running, queries are handled by the device's default DNS

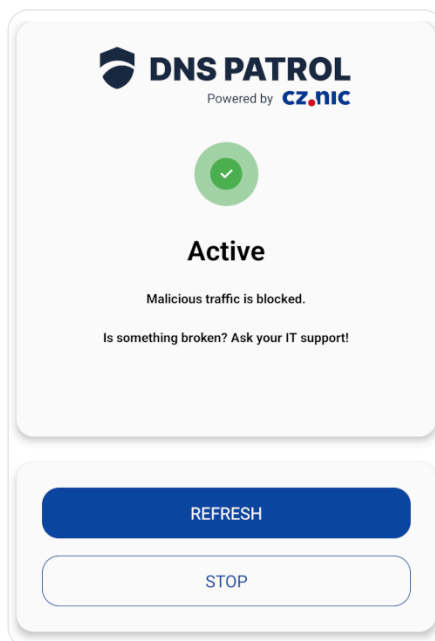


Figure 32 The Active status.

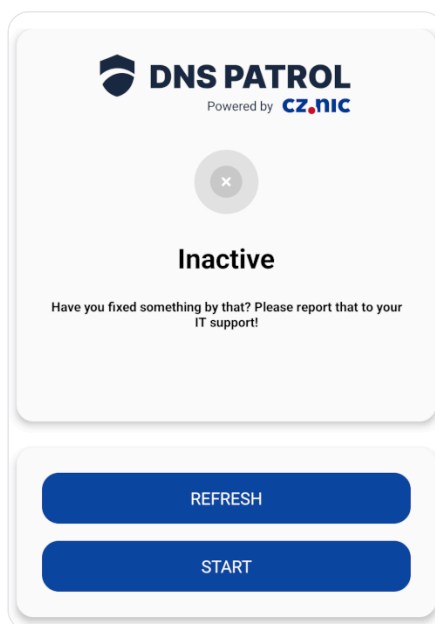


Figure 33 The Inactive status.

The available buttons depend on the status:

Button	Function
Refresh	Reloads the status of the service
Stop	Stops a running DNS PATROL (the Active status)
Start	Starts DNS PATROL (the Inactive status)

13.3 Starting up and permissions

The first time **Start** is tapped, the application warns that it needs permission to set up a local VPN in order to encrypt the device's DNS queries. The **Proceed** button continues the start-up.

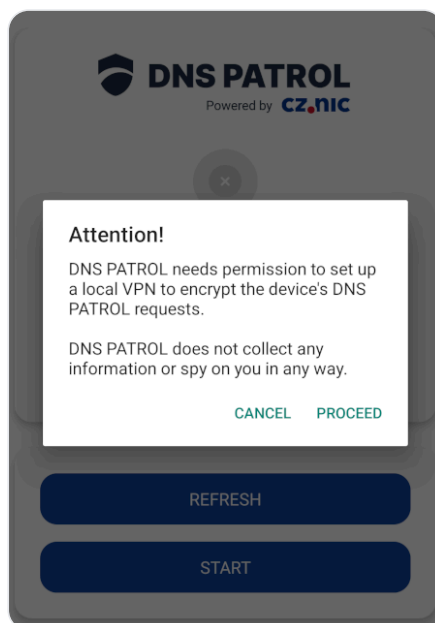


Figure 34 Warning about the VPN permission.

The system [Connection request](#) dialog follows, in which Android asks for the VPN to be allowed. It is confirmed with [OK](#).

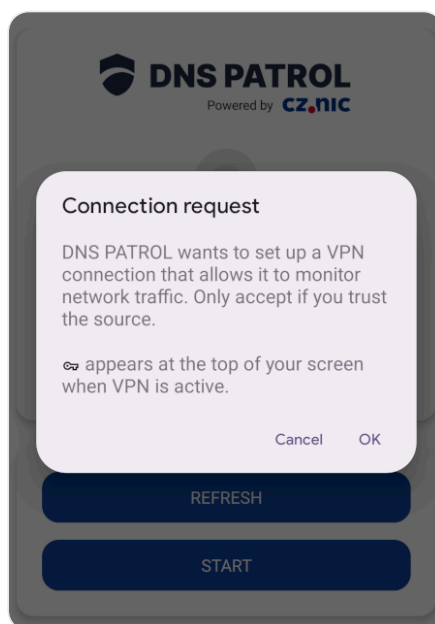


Figure 35 The system request to allow the VPN connection.

If the application does not have background data enabled, another dialog points it out. Restricting background data can lead to a loss of connectivity, because the application cannot serve DNS traffic while it is not in the foreground. The [Proceed](#) button opens the system [App battery usage](#) settings, where the restriction is lifted with the [Allow background usage](#) toggle.

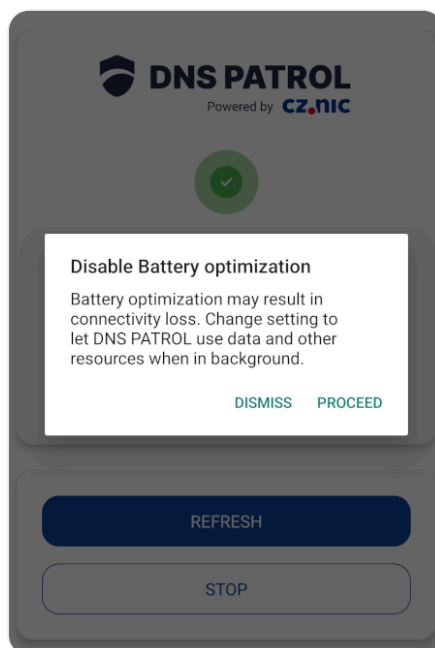


Figure 36 Warning about background data restrictions.

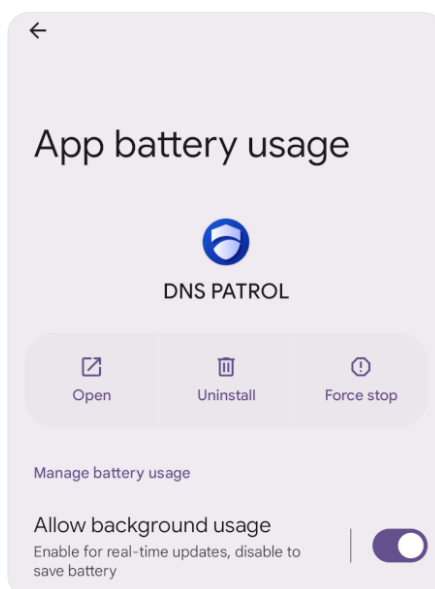


Figure 37 Allowing the application to run in the background in the device settings.

13.4 Clearing the application data

If the device needs to be registered again, that is with a different registration code, the application can either be uninstalled and installed from Google Play again, or its storage can be cleared, which is faster.

In the device settings, select **Apps** .

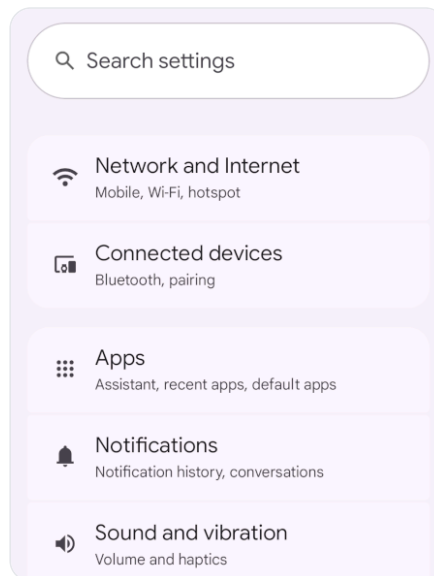


Figure 38 Device settings.

Choose DNS PATROL from the list. From here the application can be removed with the **Uninstall** button. To clear the data, continue to **Storage and cache**.

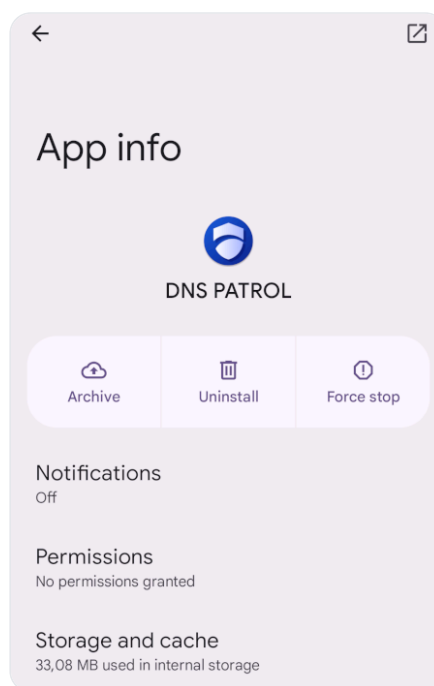


Figure 39 DNS PATROL app info.

Select **Clear storage**.

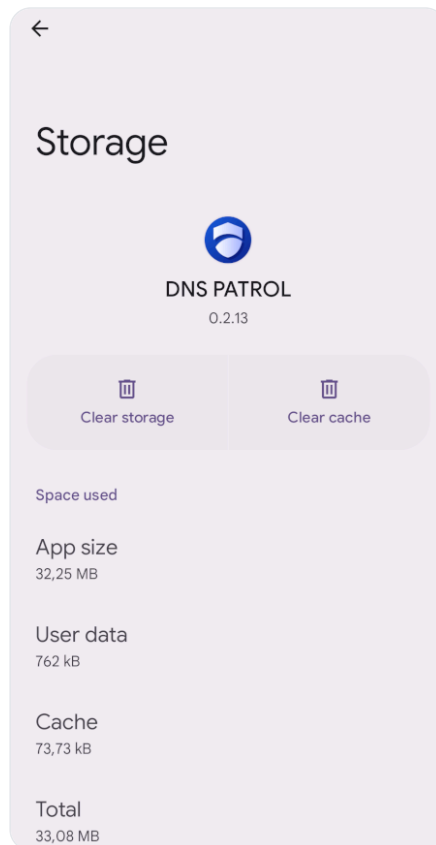


Figure 40 Application storage.

Confirm the dialog with **Delete**. The next time it is launched, the application asks for a registration code again.

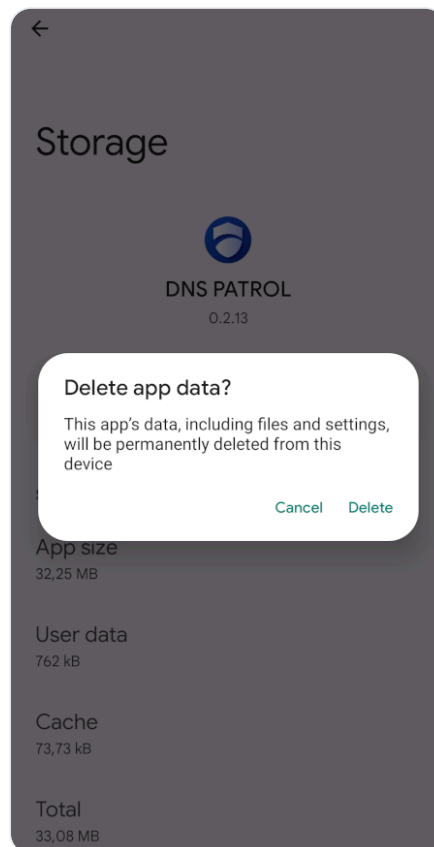


Figure 41 Confirming the deletion of the application data.

The original device record stays in the portal under [Access control](#) > [Devices](#) , where it can be deleted.

13.5 Reporting issues

Problems with the application or with websites and applications being unavailable are handled by the organisation's IT support.

Windows



The Windows application consists of a control window and the `DnsPatrolAgent` system service running in the background. The service runs a local DNS proxy on `127.0.0.1` and forwards queries to the DoH URL assigned to the device. When protection is started, `127.0.0.1` is set statically as the DNS server on the network interfaces; when it is stopped, the interfaces are returned to the DNS servers from DHCP.

14.1 Installation

The application is installed with an installer, which requires the dialog allowing it to make changes to the computer to be confirmed. Restarting the computer after the installation completes is recommended.

14.2 First launch

On first launch the application asks for a [registration code](#) issued by an administrator from the administration portal. The code is 8 characters long, consists of uppercase letters and digits, and is entered into the field below the [Please enter your registration code to continue](#) text. The [Register](#) button verifies the code and the application moves on to its main screen.

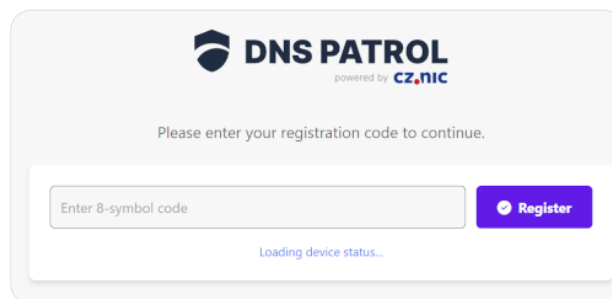


Figure 42 Entering the registration code on first launch.

14.3 Main screen

The main screen shows the current state of the protection:

Status	Description
Active	DNS PATROL is running and malicious traffic is blocked
Inactive	DNS PATROL is not running, queries are handled by the DNS server from DHCP

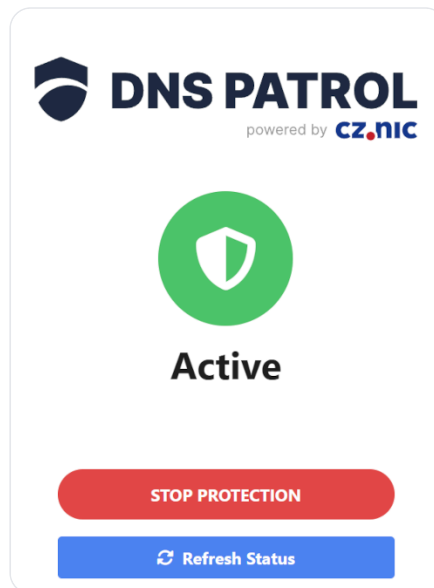


Figure 43 The Active status.

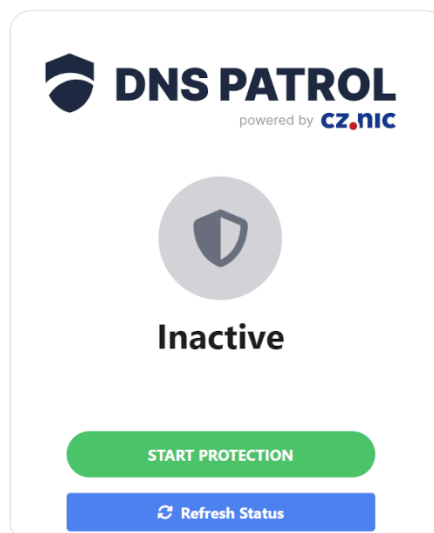


Figure 44 The Inactive status.

The available buttons depend on the status:

Button	Function
Stop protection	Stops the protection and returns the DNS settings to DHCP (the Active status)
Start protection	Starts the protection (the Inactive status)
Refresh Status	Reloads the status of the service

14.4 Device information

Hovering over the information icon in the top-right corner shows the details under which the device is recorded in the portal: the computer name, the MAC address and the device token. The same device can be found in the portal under [Access control](#) > [Devices](#).

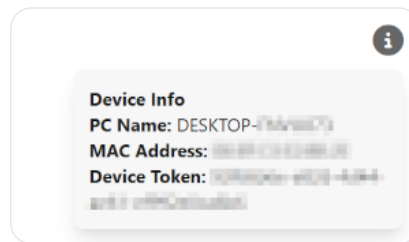


Figure 45 Device information.

14.5 Browser extension

The installation also includes an [extension for Chrome and Edge](#) that explains why a site was blocked instead of showing the browser's default error page.

14.6 Uninstallation

Uninstall the application only while it is in the **Inactive** state. The uninstaller stops and removes the **DnsPatrolAgent** service, but it no longer reverts the DNS settings on the network interfaces. Uninstalling in the **Active** state therefore leaves the interfaces statically set to **127.0.0.1**, where nothing listens once the service is gone, and name resolution on the computer stops working.

14.7 Reporting issues

Problems with the application or with websites and applications being unavailable are handled by the organisation's IT support. If the application does not work right after installation, try restarting the computer first.

Browser extension



When DNS PATROL blocks a domain, the browser on its own only shows its default “site can’t be reached” page. It shows the same page for a typo in the address or a server outage. The resolver does attach the reason for the block to its answer as an Extended DNS Error ([RFC 8914](#)), but browsers ignore it.

The DNS PATROL extension for Chrome and Edge replaces that page with its own page showing the reason the resolver gave. For a blocked domain it tells the user the site is blocked and advises them to contact their administrator. For other errors, such as a failed DNSSEC validation, it says the site isn’t working.

The extension resolves nothing itself and makes no network connections. It passes the domain to `DnsPatrol.NativeHost.exe`, a helper the application installs as a native messaging host. The helper queries the local DNS proxy on `127.0.0.1` and returns the response code and Extended DNS Error from the answer. The extension therefore works only on a computer with the [Windows application](#) without it, the extension shows nothing.

The screenshot displays the DNS PATROL browser extension interface. On the left, a window titled "DNS PATROL" shows a green shield icon and the word "Protected". Below this, it displays a "Device token" (94f0aea7-84ac-4948-bb8b-30dfca0b1e7a) and "Protected Ethernet 4". A "Refresh" button and a "Deregister this device" link are at the bottom.

On the right, the main interface shows the DNS PATROL logo and a warning icon. The heading "Tato stránka je blokována" (This page is blocked) is followed by the text "Přístup na falesna-banka.cz zablokoval váš DNS resolver." (Access to falesna-banka.cz was blocked by your DNS resolver). Below this, it says "Pokud si myslíte, že byla stránka zablokována omylem, obraťte se na svého správce." (If you think the page was blocked by mistake, contact your administrator).

A search bar shows the URL "http://falesna-banka.cz/". Below this, a section titled "Technické podrobnosti" (Technical details) is expanded, showing the following information:

Reference	U6CQ
Response	NXDOMAIN
EDE	17 (Filtered)
Meaning	Filtered at the request of the client's own policy.
Rule tag	999ext-bl-adam-test
Triggered on	falesna-banka.cz
Raw EXTRA-TEXT	U6CQ: tag 999ext-bl-adam-test triggers on falesna-banka.cz.
Queried domain	falesna-banka.cz
URL	http://falesna-banka.cz/
Time	2026-09-08T10:34:08.885Z
Extension	1.0.0

At the bottom of the technical details section are two buttons: "Zkusit znovu" (Try again) and "Kopírovat podrobnosti" (Copy details). Below the entire interface, a small note reads: "Důvod poskytl váš resolver jako Extended DNS Error (RFC 8914)." (Reason provided by your resolver as Extended DNS Error (RFC 8914)).

Figure 46 The application in the Protected state and the blocked domain page with technical details expanded.

15.1 Technical details

The [Technical details](#) drop-down holds information for administrators and IT support:

Item	Description
Reference	Four-character reference code identifying the event in the resolver's logs
Response	DNS response code
EDE	Extended DNS Error code
Meaning	Meaning of the EDE code
Rule tag	Tag of the rule that caused the block
Triggered on	Domain the rule matched
Raw EXTRA-TEXT	Original text the resolver attached to the answer
Queried domain	Domain that was queried
URL	Address of the page being opened
Time	Time of the event
Extension	Extension version

Items for which the resolver supplied no value are not shown.

The [Try again](#) button reloads the page, the [Copy details](#) button copies a plain-text summary to the clipboard. When reporting a problem, it is enough to paste the text with the reference code instead of a screenshot.

15.2 Toolbar popup

The extension's toolbar popup lists the last 20 errors and can check any domain on demand. The list stays on the computer and holds domain names only, never the addresses of the pages being opened.

15.3 Deployment

The extension is installed from the Chrome Web Store. The application installer force-installs it in Chrome and Edge through the [ExtensionInstallForcelist](#) policy, so users cannot remove it. Uninstalling the application removes the policy entry again. If the organization manages [ExtensionInstallForcelist](#) through group policy (GPO), the next GPO refresh overwrites the installer's entry. In that case, install the application with the [EXTENSION_POLICY=0](#) parameter and add the extension to the GPO directly:

```
hjfghghkohajmhhillcmbpmkbnleaidgo;https://clients2.google.com/service/update2/crx
```