# Protective Domain Name Service (PDNS)

**The NCSC's Protective Domain Name Service (PDNS), is now live – here is what it is and how to register to use it.**

## Domain Name System (DNS) - an introduction

DNS is often referred to as "The address book of the internet". It acts as a directory containing:

- The contact name (domain name)
- Telephone numbers associated with that name (IP address)

Every time you enter a web address in your browser, your computer uses DNS to translate the domain name of the site (for example *www.google.com* could be translated into 216.58.200.164).

DNS is not just used in response to user-initiated actions like viewing a website, it is used for everyday machine-initiated actions like getting software updates. Unfortunately, it also often plays a part in the distribution and operation of malware.

---

## About PDNS

PDNS was built to hamper the use of DNS for malware distribution and operation. It has been created by the National Cyber Security Centre (NCSC), and is implemented by Nominet.

PDNS is a recursive resolver, which means it finds answers to DNS queries. Management of your own domains (authoritative DNS) is done separately to this NCSC service and will not be affected by the adoption of PDNS.

It is a free and reliable internet accessible DNS service and is one of the NCSC's widely deployed Active Cyber Defence capabilities. It has been mandated for use

by central government departments by the Cabinet Office but is also available to other organisations that wish to use it (see eligibility section below).

PDNS prevents access to domains known to be malicious, by simply not resolving them. Preventing access to malware, ransomware, phishing attacks, viruses, malicious sites and spyware at source makes the network more secure.

In addition, PDNS provides organisations that use it with metrics about the health of their networks and gives them access to NCSC outreach support to resolve any issues. The data from PDNS is also used to inform and support UK government cyber incident response functions in the event of a cyber attack.

---

## Eligibility for PDNS

PDNS is currently available to:

- Central Government
- Local Authorities (including any schools using Local Authority managed networks)
- Devolved Administrations (including any schools using Devolved Administration managed networks)
- Emergency Services
- NHS Organisations
- Ministry of Defence
- UK Registered Social Housing Providers and Arms Length Management Organisations (pilot users only)

**PDNS is not currently available to the private sector, unless specifically mentioned above.**

You can register for the service and you will be approved immediately if your organisation is eligible.

We will retain your details and contact you if your organisation is likely to become eligible shortly.

We will notify you if your organisation is not eligible and delete your details.

If you think your organisation may be eligible for PDNS, and would like to find out more, please get in touch by contacting us at pdnssupport@nominet.uk

> **UK Registered Social Housing Providers and Arms Length Management Organisations (ALMOs) pilot**
>
> We are currently running a pilot for a limited number of UK Registered Social Housing Providers & ALMOs.
>
> We may ask you for feedback during the pilot & access to PDNS may be withdrawn once the pilot has ended.
>
> If you are interested in being part of the pilot please sign up and register.

---

## How PDNS works

- We curate a set of rules for how the DNS response should be modified if the user queries a malicious domain. This is codified in a database called a Response Policy Zone (RPZ) which our DNS resolver operates on
- The rules are created based on knowledge of malicious domains we obtain from commercial, internal and open sources
- We review our rules to ensure we do not accidentally block sites that are used for legitimate purposes
- When a domain is blocked, users will see a block page that states:

> You tried to visit: [http:address of site]. This site may be involved in malicious activity or associated with malware and so access has been blocked.

## PDNS Roaming

If your users work remotely or from home without a VPN or enterprise DNS resolver, you might not know the IP addresses of their devices but still want to protect them with PDNS. With PDNS Roaming, end users can benefit from the protection of PDNS wherever they connect to the internet.

PDNS Roaming is available for Windows, macOS and iOS operating systems and directs DNS traffic to PDNS. It allows devices to connect to PDNS when they are outside the office network using the encrypted DNS over HTTPS (DoH) protocol.

For more information about PDNS Roaming, visit the PDNS Portal and search for 'PDNS Roaming' in the "Knowledge and Guides" section.

## Benefits of PDNS

Benefits of PDNS include:

- Blocking malware and malicious sites - PDNS prevents access to sites hosting malware, ransomware and spyware. It also blocks malware communication, which serves to contain active threats
- Dashboard and data logs are available to help customers monitor the status of their networks and resolve any issues
- Subject matter expertise from the NCSC and Nominet, including world leading analysis and incident management capabilities
- It is free - the service is centrally funded by the NCSC

PDNS block data can be ingested into Security Information and Event Management (SIEM) tools as a source of threat intelligence to help identify and remediate threats. By consuming the data into a SIEM, organisations can consolidate various security logs into a single view, providing further context for blocks by PDNS.

Connectors are available for Microsoft Sentinel and Splunk to simplify and enhance ingesting data. To get started, visit the PDNS Portal and search for SIEMs in the "Knowledge and Guides" section.

---

## How to register for PDNS

1. Go to the NCSC PDNS online support tool
2. Choose " Register Interest":

- This should be requested by your primary technical contact (the person responsible for your organisation's network).
- They will be given an account on the PDNS online support tool, can make changes to your DNS configuration, and give access to other team members

3. Upon receipt of your request we will review the information you have provided, add your IP address or network to our access control list, and respond via email within 3 working days

4. To start using the PDNS, you will need to make changes to your organisation's DNS configuration:

- You can test and implement the configuration changes to your DNS servers once your networks have been added to the access control list
- Guidance for implementing the change can be found in the Knowledge Base in the PDNS online support tool

If circumstances change, you can change your account details through the "Update your organisation's details" option in the PDNS online support tool. You can also change the contacts on your account through the "Manage your team" option available in the PDNS online support tool.

If you are having difficulties registering, please contact pdnssupport@nominet.uk.

# Frequently asked questions (FAQs)

### How is NCSC's PDNS changing and why?

The National Cyber Security Centre has chosen a new partnership to deliver PDNS. A three-year contract has been awarded to Cloudflare in collaboration with Accenture.

PDNS will migrate to a Cloudflare platform, and the current provider Nominet will exit.

A refresh of PDNS supports a continuous improvement drive, having listened to user feedback. NCSC undertook a fair and competitive tender process to ensure PDNS continues to meet the highest technical standards and offers the best value for the British taxpayer.

### When will the change take place?

A transition period from the incumbent supplier Nominet started in April 2024.

Accenture & Cloudflare will take over NCSC's PDNS during September 2024. Specific dates for migration will be communicated in due course.

### Who are Accenture and Cloudflare?

Cloudflare is a connectivity cloud company with one of the world's largest and most interconnected networks. Cloudflare provides security at scale, blocking billions of threats online for its customers every day, managing approximately 35 million DNS queries per second globally. In Quarter 4 of 2023, Cloudflare blocked an average of 182 billion cyber threats each day. 95% of the world's internet users are within 50ms of Cloudflare's network.

Accenture is a global professional services company that helps the world's leading businesses, governments and other organisations build their digital core, optimise their operations, and enhance citizen services — creating tangible value at speed and scale. Accenture Security is a leading provider of end-to-end cyber security services, including strategy, protection, resilience, and industry-specific cyber services with over 20,000 security professionals serving over 4,500 clients across 67 countries.

**Will PDNS Roaming change?**

The Nominet PDNS client will be replaced with the Cloudflare client, known as Cloudflare One Agent.

The Nominet PDNS client will cease to work once the migration takes place later this year. Existing users of the Nominet PDNS client will be engaged with over the summer in advance of this change to ensure a smooth transition.

For further information, please see https://developers.cloudflare.com/cloudflare-one/connections/connect-devices/warp/

**Will there be a pilot or early adoption phase?**

An Early Adoption phase has been planned with the option for some organisations to come onboard early.

We will engage with users in due course for Early Adoption eligibility.

**Where can we find out more?**

We will engage with users over the next few months to provide updates, key information about the changes, and any actions you may need to take. Please keep an eye on this page and the MyNCSC portal.

You may also send enquiries to acdenquiries@ncsc.gov.uk

### How do I connect to PDNS?

You can configure your organisation's local DNS resolvers to query PDNS or you can use PDNS Roaming. PDNS accepts DNS queries from IP addresses added to our allow list and PDNS Roaming devices.

PDNS has primary and secondary IP addresses (IPv4 and IPv6) which can be found in the PDNS Portal. If you are using them, it is essential that both are configured on your local DNS resolver(s). As good practice, we recommend a tertiary DNS IP address from a 3rd party provider is configured for failover in the unlikely event of an outage. If necessary, read your service provider's documentation for instructions on how to implement these changes.

To confirm a device is using PDNS you can use https://testpage.protectivedns.service.ncsc.gov.uk/

Technical support is available by:
- Using the PDNS Portal
- Emailing pdnssupport@nominet.uk
- Calling our dedicated phone line on 0330 2369473

Our core business hours are 8am to 6pm, Monday to Friday. For emergency support there is on-call cover provided outside of core business hours via the same phone number.

### How do you prevent the incorrect blocking of legitimate domains?

The NCSC and Nominet continually refine the blocking process. We implement allow-listing algorithms, ask users for their critical domains, and ensure everything is overseen by experienced DNS engineers. However, in the uncommon case of a domain being blocked incorrectly, we work with users and our threat intelligence sources to establish the best course of action.

If you do find a domain which you think is incorrectly blocked, you can contact us by:

- Using the PDNS Portal
- Emailing pdnssupport@nominet.uk
- Calling our dedicated phone line on 0330 2369473

### Does PDNS filter content?

No. PDNS does not provide content filtering. PDNS solely limits its blocking to sites known to contain malicious content like malware or viruses.

**PUBLISHED**

17 August 2017

**REVIEWED**

10 May 2024

**WRITTEN FOR**

Public sector

Cyber security professionals