DNS Filtering
Quick Start Guide

This guide explains how to get started using the DNSFilter® AI-powered threat blocking and content filtering tool. In particular, it explains how to deploy its roaming client agents (small software components) on vessel devices that you want to protect.

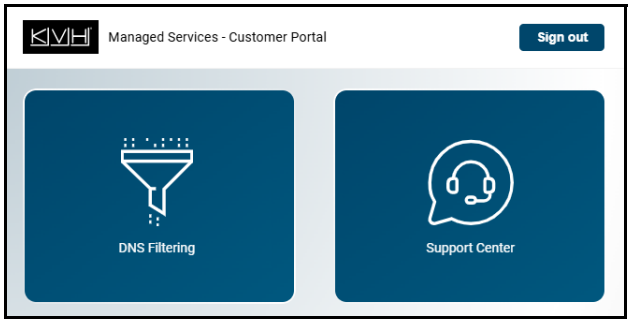
Accessing DNSFilter

The DNSFilter dashboard is available via the KVH Managed Services Customer Portal. To access the portal, open a web browser and go to **https://ms.kvh.com**. Then log in with the credentials KVH provided during the onboarding process.

Note: *If you are a KVH Airtime customer, use the email address and password you use to log into KVH Manager.*

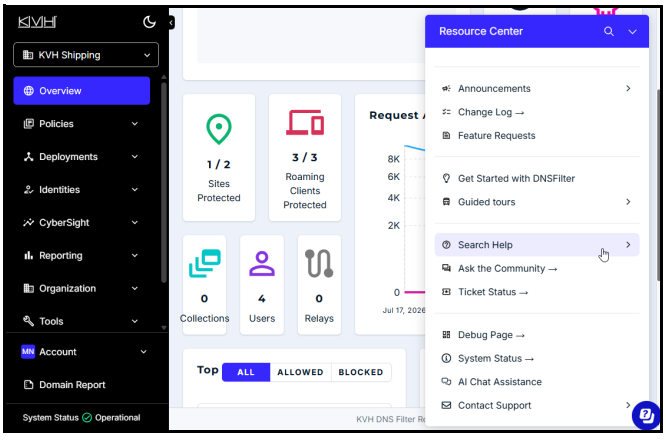
Note: *For initial access, you will first need to enter a verification code provided in an email from Zitadel.*

Once you are logged in, select **DNS Filtering** to launch the DNSFilter dashboard. From there, you can download its roaming client agent installers.



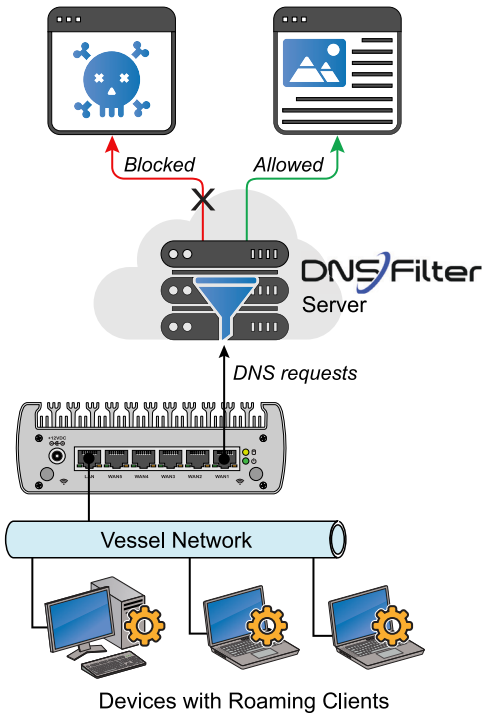
For More Information

These instructions only provide basic information. For complete details and advanced options, refer to the comprehensive DNSFilter Help Center – select the help button in the bottom-right corner of the DNSFilter dashboard or go to https://help.dnsfilter.com.



Planning Agent Deployment

You need to install a roaming client agent on every endpoint device (e.g., computer) you want to protect on your network. This lightweight agent will forward all DNS requests originating from that device to DNSFilter's cloud-based servers to block malicious, risky, and inappropriate domains while enforcing your custom filtering policies and allow/block lists.



Note: *As an alternative, you may install a DNS Relay on an onboard server to protect an entire network, rather than just individual devices. Refer to the DNSFilter Help Center for details.*

Technical Support

If you have any questions or need technical assistance, please submit a support ticket at the Customer Portal or contact KVH Technical Support 24/7/365:

- Continental USA: 1-866-701-7103
  Worldwide: +1 401-851-3806
- WhatsApp: +1 401-851-3842
- Email: help@kvh.com

System Requirements for Agents

Before installing the DNSFiler roaming client on a vessel device, be sure its operating system meets the following minimum requirements.

Windows

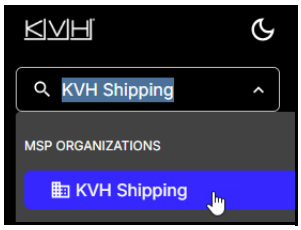
- Windows 10 or later (x64)
- .NET Framework 4.8.1 or later
- .NET Desktop Runtime 8.0 required to run agent versions 2.1.0 or later

Mac

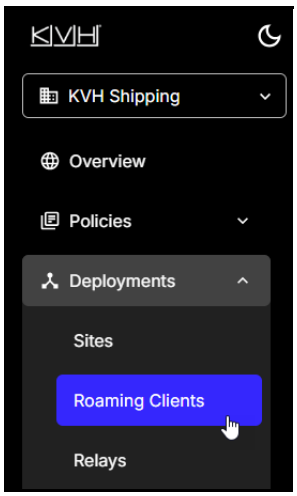
- macOS Ventura (13) or later
- macOS Big Sur (11) and Monterey (12) cannot run agent versions 2.4.4 or later

Installing Roaming Clients

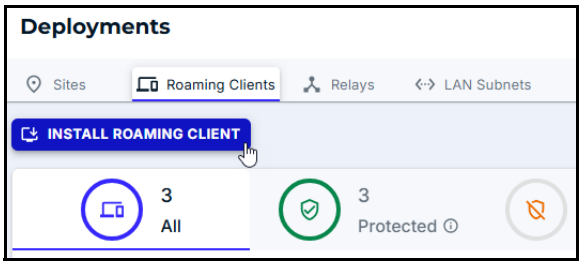
1. If you manage multiple organizations (i.e., companies or fleets), select the org associated with the desired vessel(s).



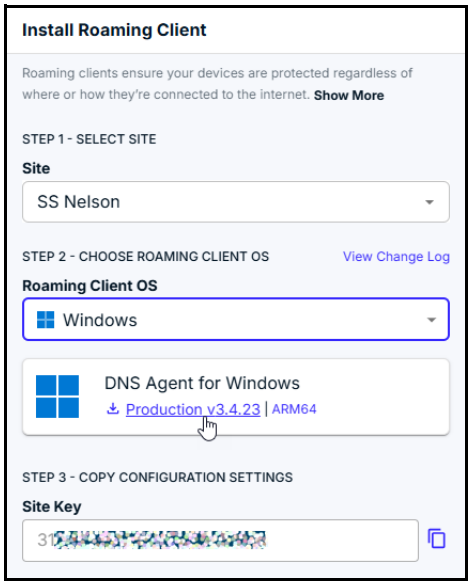
2. Select **Roaming Clients** under the Deployments menu.



3. Select **Install Roaming Client**.

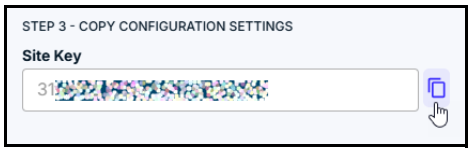


4. Select the applicable site (i.e., vessel) and the operating system of the device where you will install the roaming client. Then click the link to download the appropriate DNS Agent installation package to your computer.



Note: *If an RMM (Remote Monitoring and Management) tool is deployed on your network, you may push the agent installer to multiple devices using a deployment script.*

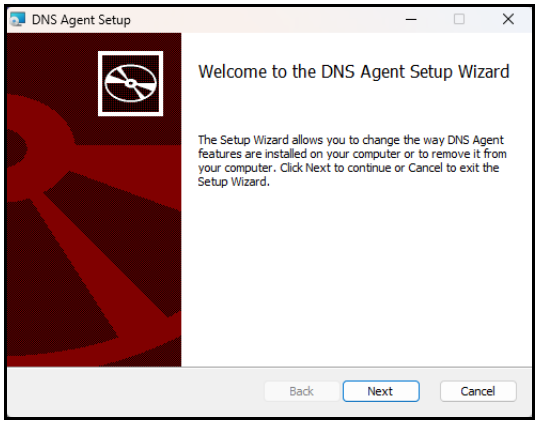
5. Copy the site key and save it to a text file. You will need it during the agent installation process.



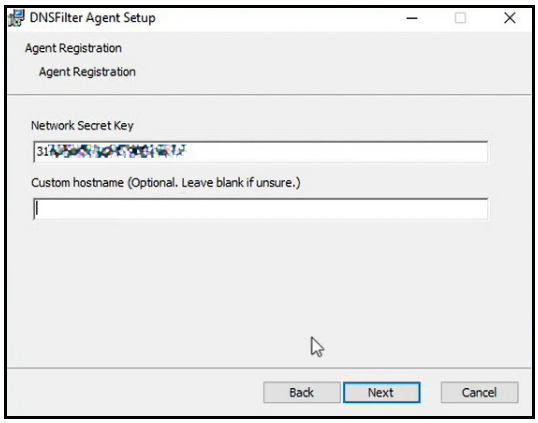
IMPORTANT!
Protect your site key like any other security credential.

6. Find the agent installation package in your Downloads folder. The filename starts with "DNS Agent."

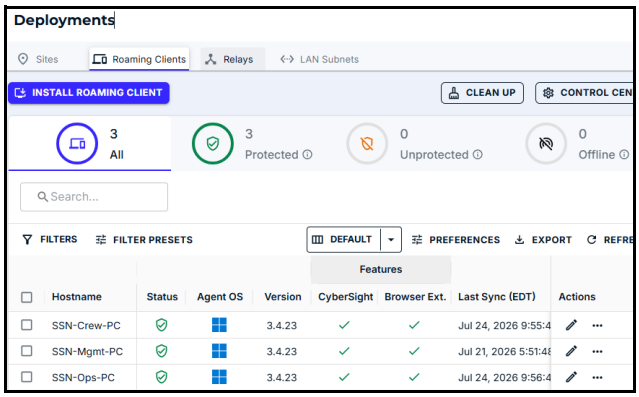
7. Copy and run the installer on every vessel device you want to protect, assuming they share the same operating system. *For any device that differs, simply download and install the appropriate agent for that device.*



During the installation process, you will need to enter the site key when prompted.

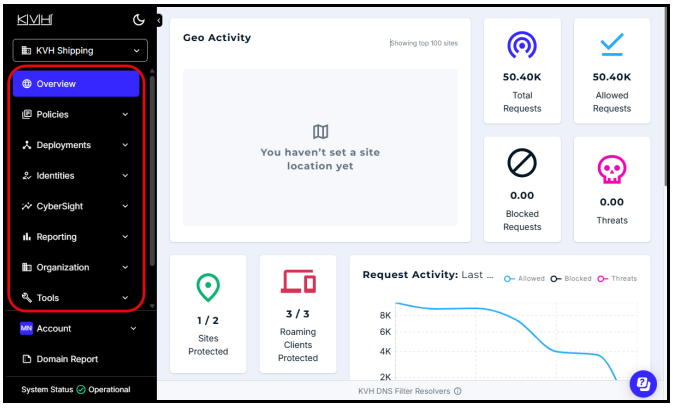


8. When you are done installing the agents, your devices should appear in the list of Roaming Clients, assuming they all have access to the Internet.



Exploring the DNSFilter Dashboard

Once your roaming clients are deployed, you can view their activity and set up filtering policies and allow/block lists by selecting the desired option from the main menu.



- **Overview**: View a summary of DNSFilter activity: see how many DNS requests have been allowed, blocked, or deemed threats within the past week; see how many sites/devices are currently protected; see a list of top domains/sites
- **Policies**: Set/schedule filtering policies; allow or block specific content categories, threats, applications, ads/trackers, and domains
- **Deployments**: View/manage sites (vessels) and roaming clients (devices); download agent installers; apply filtering policies to specific devices; install a DNS Relay to a server via a command-line interface (CLI); add local domains and resolvers
- **Identities**: Apply filtering policies to specific users or groups (e.g., based on role or department)
- **CyberSight**: Analyze time-stamped DNSFilter activity and user activity; identify trends
- **Reporting**: View granular DNSFilter data in comprehensive logs and charts; export detailed reports
- **Organization** and **Tools**: KVH admin use only

Note: *Refer to the DNSFilter documentation at the Help Center (https://help.dnsfilter.com) for complete details.*