DNS Filtering

Overview

DNS Filtering provides Administrators an easy way to filter network traffic to ensure users are accessing approved sites. It is organized in 7 tabs: Overview, Settings, Filtering, Security, Allowed/Blocked, Alerts, and Logs.

DNS Filtering profiles and configurations can be assigned to individual users and groups, or to all devices. Complete assignment based on what is needed for the school or district environment. Profiles can be quickly toggled ON and OFF using the toggle in the left menu.

When the DNS Filtering is assigned to a user/device, the necessary configuration profiles (DNS Settings and DNS Proxy Extension) will be automatically installed. Mosyle's DNS Filtering requires iOS/iPadOS 14+ and macOS 11+.

The Mosyle DNS Filtering requires specific domains and ports. Please see the help center article titled “Domains and Ports for DNS Filtering” for more information.

Overview

The Overview tab provides query data on the devices assigned to the individual profile. View the total number of queries, number of blocked queries, global traffic, number of queries per day, and filter by the list of top domains resolved and/or blocked.

overview.png

Settings

The Settings tab can be configured to specify Privacy & Logging settings, settings for macOS and iOS management, and any DNS Bypass rules. Assign the profile to the users/devices to be filtered. When using the DNS Filtering, it's strongly recommended not to apply any other content filtering solutions or profiles to avoid conflicts.

settings.png

Filtering

The Filtering tab can be configured to apply a Standard set of filters to filter network traffic. Custom filters can be created and applied.

filtering.png

Security

Configure the Security tab to block domains based on malicious activity, domain age, or hosting country.

security.png

Allowed/Blocked

Customize specific domains that should be always allowed or always blocked, despite their categorization. Add domains that require custom resolution.

allowed-blocked.png

Alerts

Configure alerts so that Administrators are notified when users attempt to access a domain or site that is not allowed.

alerts.png

Logs

View logs to see any blocked and/or allowed sites. The logs provide the device identifier, serial number, URL visited, the action (blocked/allowed), the reason for the block based on URL categorization, the IP address, and date & time stamp.

Click the gear icon to add the URL as an always blocked domain, always allowed domain, report as wrong classification, or set to exclude the domain in the logs.

The logs can be filtered by specific URLs, dates, devices, or by status (allow/block). Once filtered, the results can be exported.

logs.png

Configuring DNS Filtering

To configure DNS Filtering

1. Go to DNS Filtering
2. Click + Create New Profile
3. Name the profile and select the users/devices the filtering will be assigned to
4. Configure the following tabs: Settings, Filtering, Security, Allowed/Blocked, and Alerts

Settings

The following options can be configured in the Settings tab. When finished, click Save.

- Privacy & Logging Settings
  - Log all resolved requests. By default all blocked requests will be logged. Checking this box will ensure all requests, even allowed requests are logged.
  - Include device identifier in the logs: Indicate the device identifying information that will be displayed in the logs - either device name or assigned user. Leave this unchecked to exclude the device identifier from the logs.
  - Include device IP in the logs: Check this option to include the device IP. By default the device IP will not be included in the logs.
  - Select the duration of time to retain logs of blocked requests: 10 days, 15 days, or 30 days
  - Exclude common system domains in the logs: Customize the list of domains to be excluded in the logs. Domains trusted and frequently used can be excluded, such as *.apple.com.

- macOS management
  - Extend the DNS Filtering to Google Chrome or Firefox by checking the appropriate boxes
  - Automatically block other third party internet browsers and applications that can conflict with the DNS Filtering: Click “Customize this selection” to choose the browsers and apps to block. By default, Google Chrome and Firefox will be included in the list. If users are permitted access to these browsers, be sure to deselect them from the list.

- iOS management
  - Automatically block other third party internet browsers and applications that can conflict with the DNS Filtering: Click “Customize this selection” to choose the browsers and apps to block.
  - The DNS Filtering utilizes the Mosyle Manager application on iOS/iPadOS devices. To ensure end users cannot remove the app from the devices, check the box “For the DNS Filtering to work on the iOS Devices, the Mosyle Manager app must be installed….”

- Mosyle DNS Bypass for flights, hotels, and local domains / DNS Rules

- Configure the DNS Bypass rules so devices can connect to captive portals on flights or in hotels to allow network connectivity or enter custom domain configuration for the DNS Filtering to bypass. bypass.png

Filtering

Toggle ON any of the Standard filters to be blocked. If any additional filters need to be applied, create a custom filter by clicking “Create new filter”. Choose the site categories to be blocked. If needed, enter a URL in the URL checker to check the site categorization.

If desired, toggle on the options to enforce Safe Search and/or YouTube restricted mode. When finished, click Save.

Security

Toggle ON any of the options to block domains based on malicious activity, domain age, or hosting country. To add a hosting country click the button “Select / Edit Countries”. When finished, click Save.

Allowed/Blocked

Domains added in the Allowed list will always be allowed, even if they are configured to be blocked due to site categorization. Domains added in the Blocked list will always be blocked, even if their site categorization is not blocked.

If a domain requires custom resolution, such as an internal resource, enter the domain in the Allowed list and check the box for “Customize resolution” and enter the IP address.

Alerts

Configure to receive email alerts if users attempt to access a restricted domain, or attempt to access a site that is blocked due to its categorization. Choose how long devices will remain in the alerts until they are removed if there are no additional occurrences.

Email Preferences can be configured to receive a daily report, receive an email for every alert, or not receive email alerts. Choose the Administrators to receive the alert emails. When finished, click Save.

Revision #1
Created 2025-10-08 00:48:05 UTC by joliveira
Updated 2025-10-08 00:48:40 UTC by joliveira