REST API overview

All administration and configuration of SafeDNS Shield is performed through the REST API. The API listens on port 8080 of the same IP address that handles DNS queries. By default, access is restricted to a set of whitelisted IP addresses specified during deployment.

Initial Configuration Example

The following example demonstrates the initial configuration workflow. Send the following request:

- Type: POST
- URL: `<domain>/init/`
- Data:

```
{
    "profiles": [
        {
            "profile": {
                "id": 1,
                "page_id": 1
            },
            "cat_ids": [3, 4, 12],
            "app_ids": [1, 12, 93]
        }
    ],
    "blockpages": [
        {
            "id": 1,
            "type": 0
        },
        {
            "id": 2,
            "type": 1
        }
    ],
    "bw_lists": [
       {
            "profile_id": 1,
```

```
            "type": "deny",
            "domains": [
                "example1.com",
                "example2.com",
                "example3.com"
            ]
        }
    ],
    "nets": [
        {
            "ip": "100.100.100.100",
            "profile_id": 1,
            "prefix_len": 32
        },
        {
            "ip": "100.110.110.0",
            "profile_id": 1,
            "prefix_len": 24
        },
        {
            "ip": "100.120.0.0",
            "profile_id": 1,
            "prefix_len": 16
        }
    ],
    "nets6": [],
    "napts": []
}
```

The initialization query defines the full configuration applied to SafeDNS Shield. The following settings are processed in sequence:

1. **Filtering profile and block page** – A filtering profile (ID=1) and a block page (ID=1) are created.
2. **Blocked categories** – Three DNS categories are blocked for the profile: malware, phishing, and botnets.
3. **Blocked applications** – Three AppBlocker categories are blocked: Slack, AnyDesk, and Netflix.
4. **Block pages** – Two block pages of different types are created:
   - Type 0 – displays the blocked domain name.
   - Type 1 – does not display the blocked domain name.
5. **Blacklist** – Three domains are added to the blacklist for filtering profile 1.

6. **IP assignment** – The profile is assigned one specific IP address and two subnets (/16 and /24). DNS requests from these sources are filtered according to the profile's policy.
7. **IPv6 and NAT-port identification** – The `nets6` (IPv6) and `napts` (NAT port-based identification) sections are included but left empty. These fields must be present in the request even if not used, to trigger the creation of the initial configuration.

Once the request is sent and a successful response (HTTP status `204`) is received, the initial configuration is complete. All subsequent DNS traffic processed by the server is handled according to the specified rules.

Modifying Filtering Categories

To modify the filtering categories for an existing profile, you must update the entire list of categories assigned to that profile. Adding new categories requires sending the full set (both current and new categories) in a single request.

For example, the initial configuration created profile `id=1` with three blocked categories: malware, phishing, and botnets. To add Cryptojacking, DGA, and Ransomware, the request must include all six categories:

- Type: PATCH
- URL: `<domain>/profiles/1/`
- Data:

```
{
  "cat_ids": [3, 4, 12, 66, 70, 71],
  "app_ids": [1, 12, 93],
  "profile": {
    "page_id": 1
  }
}
```

In this request, the profile ID is specified directly in the URL. The request body contains the updated list of categories (original three and three new) while the AppBlocker categories and block page remain unchanged.

Adding a Domain to the Allowlist

To exempt a specific domain from category-based blocking, add it to the allowlist of the relevant filtering profile. For profile `id=1`, send the following request:

- Type: POST
- URL: `<domain>/profile/1/bw_list`
- Data:

```
{
  "type": "allow",
  "domain": "example4.com"
}
```

This adds the domain to the allowlist, giving it priority over category-based blocking.

Adding Domains to the Denylist

To block specific domains that are not covered by the configured categories, add them directly to the denylist for the filtering profile. The following request adds domains in a batch operation for profile `id=1`:

- Type: POST
- URL: `<domain>/profile/1/bw_list/batch`
- Data:

```
{
  "type": "deny",
  "domains": ["example5.com", "example6.com", "example7.com", "example8.com", "example9.com"]
}
```

Adding a Network or IP Address for Filtering

To assign a new IP address or subnet to a filtering profile, send the following request. The example adds a single IP address by specifying a `/32` network prefix for profile `id=1`:

- Type: POST
- URL: `<domain>/net/`
- Data:

```
{
    "ip": "100.100.100.101",
    "profile_id": 1,
    "prefix_len": 32
}
```

To add an entire subnet, adjust the prefix length accordingly. For instance, a `/24` subnet would be specified as:

```
{
    "ip": "100.100.101.0",
    "profile_id": 1,
```

```
    "prefix_len": 24
}
```

Removing an IP Address from Filtering

To remove a previously assigned IP address or subnet from a filtering profile, send the following request:

- Type: DELETE
- URL: `<domain>/net/**1684300901**`
- Data: None

This request has no body. The IP address must be provided in decimal format in the URL. Use the exact address originally submitted, without the mask - for example, `100.100.100.101` or `100.100.101.0` from the earlier examples. You can convert an IP address to decimal format using a tool like this one.

Modifying the Filtering Profile for a Specific IP

To change the filtering profile assigned to an existing IP address or subnet, send the following request. The IP address must be provided in decimal format in the URL. This example reassigns the address `100.100.101.0` (originally a `/24` subnet) from profile `id=1` to profile `id=2`:

- Type: PATCH
- URL: `<domain>/net/**1684301056**`
- Data:

```
{
    "ip": "100.100.101.0",
    "profile_id": 2,
    "prefix_len": 24
}
```

To change the network prefix (for example, from `/24` to `/16`), you must delete the existing record and add a new one with the correct network address. In this case, you would delete `100.100.101.0` and add `100.100.0.0` with the `/16` prefix.

Creating a New Filtering Profile

Before an IP can be reassigned to a different profile, that profile must exist. The following request creates a new filtering profile:

- Type: POST
- URL: `<domain>/profiles/`

- Data:

```
{
    "profile": {
        "id": 2,
        "page_id": 1
    },
    "cat_ids": [3, 4, 12, 66, 70, 71, 13],
    "app_ids": [1, 12, 93]
}
```

This creates profile `id=2`, configured with the same block page type and the same categories and AppBlocker settings as profile `id=1`, with the addition of the "Adult Related" category.

Revision #19
Created 6 March 2026 08:42:09 by Ryan Lane
Updated 26 May 2026 13:33:45 by Andrew Lem