



## FQDN Filter Profile

---

- [FQDN \(Fully Qualified Domain Name\) Filter Profile, on page 1](#)
- [Create a Standalone FQDN Filter Profile, on page 2](#)
- [Create a Group FQDN Filter Profile, on page 3](#)

## FQDN (Fully Qualified Domain Name) Filter Profile

An FQDN Filter Profile evaluates the FQDN associated with traffic and applies an action to either allow or deny the traffic. In order to evaluate the FQDN, traffic must be TLS encrypted and contain an FQDN in an SNI in a TLS hello header. The FQDN can be evaluated for traffic that is processed by either a **Forwarding** or **Forward Proxy** Rule. The set of FQDNs in the Profile can be specified as strings representing the full domain or as strings represented by a Perl Compatible Regular Expression (PCRE). If only domain filtering is required, it is best to use an FQDN Filtering Profile. An FQDN Filtering Profile can also be used in conjunction with a URL Filtering Profile, where the domain is evaluated using the FQDN Filtering Profile and the URL is evaluated using the URL Filtering Profile.

The FQDN Filtering Profile can use a set of pre-defined Categories. To view more information on Categories, please see .



---

**Note** The FQDN Filter Profile is organized as a table containing user-specified rows (FQDNs and Categories) along with two default rows (Uncategorized and ANY). Categories and FQDNs can be combined within each row if desired.

The limits for each FQDN Filter Profile are as follows:

- Maximum user-specified rows:254 (Standalone or Group of Standalones)
- Maximum Categories and FQDNs per row:60
- Maximum FQDN character length:255

When specifying a multi-level domain (e.g., 'www.example.com'), it's important to escape the '.' character (e.g., 'www\\.example\\.com') otherwise it will be treated as a wildcard for any single character.

---

### Standalone vs. Group

A FQDN Filter Profile can be specified as Type Standalone or Group.

A FQDN Filter Standalone Profile contains FQDNs and Categories. The Profile will be applied directly to a set of one or more Policy Ruleset Rules or associated with a FQDN Group Profile.

A FQDN Filter Group Profile contains an ordered list of Standalone Profiles that can be defined for different purposes and combined together into a Group Profile. The Group Profile can be applied directly to a set of one or more Policy Ruleset Rules. Each team can create and manage specific Standalone Profiles. These Standalone Profiles can be combined together into a Group Profile to create hierarchies or different combinations based on use case. An example combination could be a global FQDN list that would apply to everything, a CSP-specific list that would apply to each different CSP, and an application-specific list that would apply to each different application.

### Uncategorized

1. The penultimate row in an FQDN Filter Profile, which is represented as **Uncategorized**.
2. Specifies the Policy action to take for FQDNs that do not match the user-specified FQDNs or do not have a Category.
3. If a Standalone Profile is used in a Group Profile and the Group Profile is applied to a Policy Ruleset Rule, the **Uncategorized** row will be taken from the Group Profile. The **Uncategorized** row of a Standalone Profile is only applicable if the Standalone Profile is directly applied to a Policy Ruleset Rule.

### Default (ANY)

1. The final row in an FQDN Filter Profile, which is represented as **ANY**.
2. Specifies the Policy action to take for FQDNs that do not match the user-specified FQDNs or Categories, or are not Uncategorized.
3. If a Standalone Profile is used in a Group Profile and the Group Profile is applied to a Policy Ruleset Rule, the **ANY** row will be taken from the Group Profile. The **ANY** row of a Standalone Profile is only applicable if the Standalone Profile is directly applied to a Policy Ruleset Rule.

## Create a Standalone FQDN Filter Profile

- 
- Step 1** Navigate to **Manage > Profiles > FQDN Filtering**.
- Step 2** Click **Create**.
- Step 3** Provide a Profile Name and Description.
- Step 4** Specify the Type as Standalone.
- Step 5** Click **Add** to create a new row.
- Step 6** Specify individual FQDNs (e.g., 'www.twitter.com', '\*.google.com').
- a) Each FQDN is specified as a PCRE (Perl Compatible Regular Expression).
  - b) Consider escaping the . character else it will be treated as a single character wildcard.
- Step 7** Specify Categories (e.g., Gambling, Sports, Social Networking).
- Step 8** Specify the Policy action for the user-specified FQDNs/Categories, Uncategorized and ANY rows.
- a) **Allow Log** - Allow the requests and log an event.
  - b) **Allow No Log** - Allow the requests and do not log an event.

- c) **Deny Log** - Deny the requests and log an event.
- d) **Deny No Log** - Deny the requests and do not log an event.

**Step 9** (Optional) Specify Decryption Exception for any FQDNs where decryption is not desired or possible. Possible reasons for considering Decryption Exception include:

- a) Desire to not inspect encrypted traffic (financial services, defense, health care, etc.).
- b) SSO authentication traffic where decryption is not possible.
- c) NTLM traffic that cannot be proxied.

**Step 10** Click **Save** when completed.

---

#### What to do next

##### Associate the FQDN Filter Profile:

Check [this document](#) to create/edit Policy Rules.

## Create a Group FQDN Filter Profile

---

**Step 1** Navigate to **Manage > Profiles > FQDN Filtering**.

**Step 2** Click **Create**.

**Step 3** Provide a Profile Name and Description.

**Step 4** Specify the Type as Group.

**Step 5** Select an initial Standalone Profile (at least one Standalone Profile is required).

**Step 6** Specify additional Standalone Profiles.

**Step 7** Click **Add FQDN Profile** to create a new row.

**Step 8** Select a Standalone Profile.

**Step 9** Specify the Policy action for **Uncategorized** FQDNs.

**Step 10** Specify the Policy action for **ANY** FQDNs (default).

**Step 11** Optional: Specify Decryption Exception for Uncategorized or ANY if decryption is not desired or possible. Possible reasons for considering Decryption Exception include:

- a) Desire to not inspect encrypted traffic (financial services, defense, health care, etc.)
- b) SSO authentication traffic where decryption is not possible
- c) NTLM traffic that cannot be proxied

**Step 12** Click **Save** when completed.

---

#### What to do next

##### Associate the FQDN Filter Profile:

Check [this document](#) to create/edit Policy Rules.

