

App Profiles

<https://campus.barracuda.com/doc/92767289/>

By adding URLs, you can decide which types of protection pertain to all or a portion of your application. The main panel shows the URL and the right panel displays the features that are or can be enabled for it.

Features for *Root* will apply to your entire application with the exception of any other URLs defined here. For example, adding the URL */file-upload.php* creates a new feature group. Features enabled in the right panel will apply to *<yourdomain.com/file-upload.php>*. Adding the URL */admin/** also creates a new feature group. Features enabled in the right panel will apply to all files in the *<yourdomain.com/admin/>* branch of your application.

The following features can be configured for each URL:

- **[URL Profiles](#)** – Determine how Barracuda WAF-as-a-Service detects and blocks attacks in URLs and URL parameters, respectively, across your application.
- **[Extended Match Profile](#)** – Establish expressions to specifically define which requests/responses are allowed or rejected.
- **[Parameter Profiles](#)** – Establish rules to defend from attacks sent inside URL parameters.
- **[Form Protection](#)**
 - **[Brute Force Protection](#)** – Stops attacks from making multiple automated submissions using forms in your applications. It also stops attackers from systematically trying to access pages over and over again with the intention of trying multiple username/password combinations to brute force entry in to your application.
 - **[Data Theft Protection Usage](#)** – Prevents unauthorized disclosure of confidential information. Rules must be created globally at the [Data Theft Protection Policy](#) component before they can be applied here.
 - **[File Upload Protection](#)** – This incorporates both Advanced Threat Protection (BATP) and Virus Scanning.
 - **[Login Form Information](#)** – For credential protection to work you need to specify the format and details for the login form.
 - **[Credential Attack Protection](#)** – Protects against Credential Stuffing and/or Credential Spraying.
 - **[Privileged Account Protection](#)** – Watches for signs of account takeover by evaluating session elements such as the connecting entity's geolocation, user agent, header value, and network details.
- **GraphQL security** – Secures your GraphQL APIs with capabilities that include native parsing of requests and enforcement of security checks. See [GraphQL Security](#) for more information.
- **JWT validation** – Uses the received JSON Web Token (JWT) to validate the authenticity of the client sending HTTP requests and the token claims. See [JSON Web Token \(JWT\) Validation](#) to learn more.
- **[JSON Profiles](#)** – JSON-based applications are enforced with input validations and other security checks to ensure that the attacks are not tunneled inside HTTP requests with the JSON content.

Notes

- Only features that are licensed or made available for your application will appear in the right panel.
- Privileged account protection, GraphQL security, JWT validation, Parameter Profiles and Extended match profile are only available on [datapath](#) v12.0 and later.
- Global Parameters can still be found under the Parameters Protection component. Parameters described above are URL specific.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.