# Privileged Account Protection

https://campus.barracuda.com/doc/98216434/

Privileged Account Protection (PAP) is a part of the Account Takeover Protection provided by Barracuda WAF-as-a-Service. In Privileged Account Protection, various session data elements, such as the connecting entity's geolocation, user agent, header value, and network details, are evaluated. If the risk found by Privileged Account Protection for connecting a client is deemed acceptable based on configured settings, then the client is allowed to access the back-end application without issue. If not, actions are taken as described below.

## Privileged Account Protection Workflow

1. User sends a login request to an application for which Privileged Account Protection is enabled.
2. The Barracuda WAF-as-a-Service evaluates the request for risk based on the **Sensitivity** setting you have configured.
3. If the risk level is deemed acceptable, the request is forwarded to the server. If it exceeds acceptable limits, an attack event alert is generated and added to the Firewall Logs. Also, a notification is sent to your application by HTTP POST if a Webhook has been configured.
    - The action taken for risky requests can be changed by adjusting **ATO Deviation (High/Medium/Low) Detected** in the Violation Responses - Response Policies. The default setting is to allow the request.

## Enable Privileged Account Protection

1. From App Profiles, add Form Protection to the desired URL.
2. In the right side panel find **Privileged Account Protection** and click on it.
   You must add Login Form Information for PAP to be effective.
3. Configure Privileged account protection:
    - **Privileged account protection** – Set to **Enable**.
    - **Sensitivity** – Choose the level of sensitivity regarding behavior that could represent an account takeover. The higher the sensitivity, the more likely it is that a behavior will trigger a PAP alert.
    - **Webhook URL** – If you would like your application to receive generated alerts, add a Webhook URL here.
    - **Webhook authentication type** – Select the type of Webhook used above. Options are **HTTP Header** and **URL Parameter**.
        - **Http Header** – If this was your selection, add a **HTTP header name** and **HTTP header value**. These can be used by your application to identify PAP alerts.
        - **URL Parameter** – If this was your selection, add a **URL parameter name** and **URL parameter value**. These can be used by your application to identify PAP alerts.

4. Click **Save**.

## More Information

to learn more, see on premise Web Application Firewall Privileged Account Protection documentation.