# Client Profile

https://campus.barracuda.com/doc/91131590/

## Prerequisite

This feature is enabled only if you have subscribed to the Advanced Bot Protection service.

## Overview

When the **Advanced Bot Protection** feature is enabled, all incoming clients are assigned a unique fingerprint. The fingerprint is computed based on browser attributes and is designed to retain and accurately identify the client even in incognito/private window mode or when the browser data is purged. If a non-browser client is accessing the protected application, the fingerprint is computed based on the incoming IP address and a few other connection parameters.

This unique identifier is used to create a profile of the client’s activities on the protected application and to arrive at a risk score. The risk score is calculated based on the access patterns of the client, which can then be used to configure an action policy to apply to similar clients.

The client’s risk score is recorded in the logs and can be seen on the **BASIC > Access Logs** page.

## Configure the Risk Score Levels for the Client

1. Navigate to **SECURITY POLICIES > Client Profile**.
2. For **Enable Client Profile Validation**, set to **Yes** to enable client risk score validation on client fingerprints.
   Recommended: **Yes**
3. In the **Client Risk Score Thresholds** section, do the following:
   1. **Suspicious Clients** - Configure the risk score levels for suspicious clients.
      Range: 1 to 100
      Recommended: **60**
   2. **Bad Clients** - Configure the risk score levels for bad clients.
      Range: 1 to 100
      Recommended: **80**
4. In the **Exempted Clients** section, do the following:
   1. **Exempted Fingerprints** - Specify the fingerprints that need to be exempted from the risk score validation. Ensure that you add each fingerprint separately.

   2. **Exempted IP Addresses** - Specify the client IP addresses that need to be exempted from the risk score validation. You can add a single IP address or a range of IP addresses. Each entry should be added separately. The range of IP addresses must be separated with a hyphen (-).

5. Click **Save**.