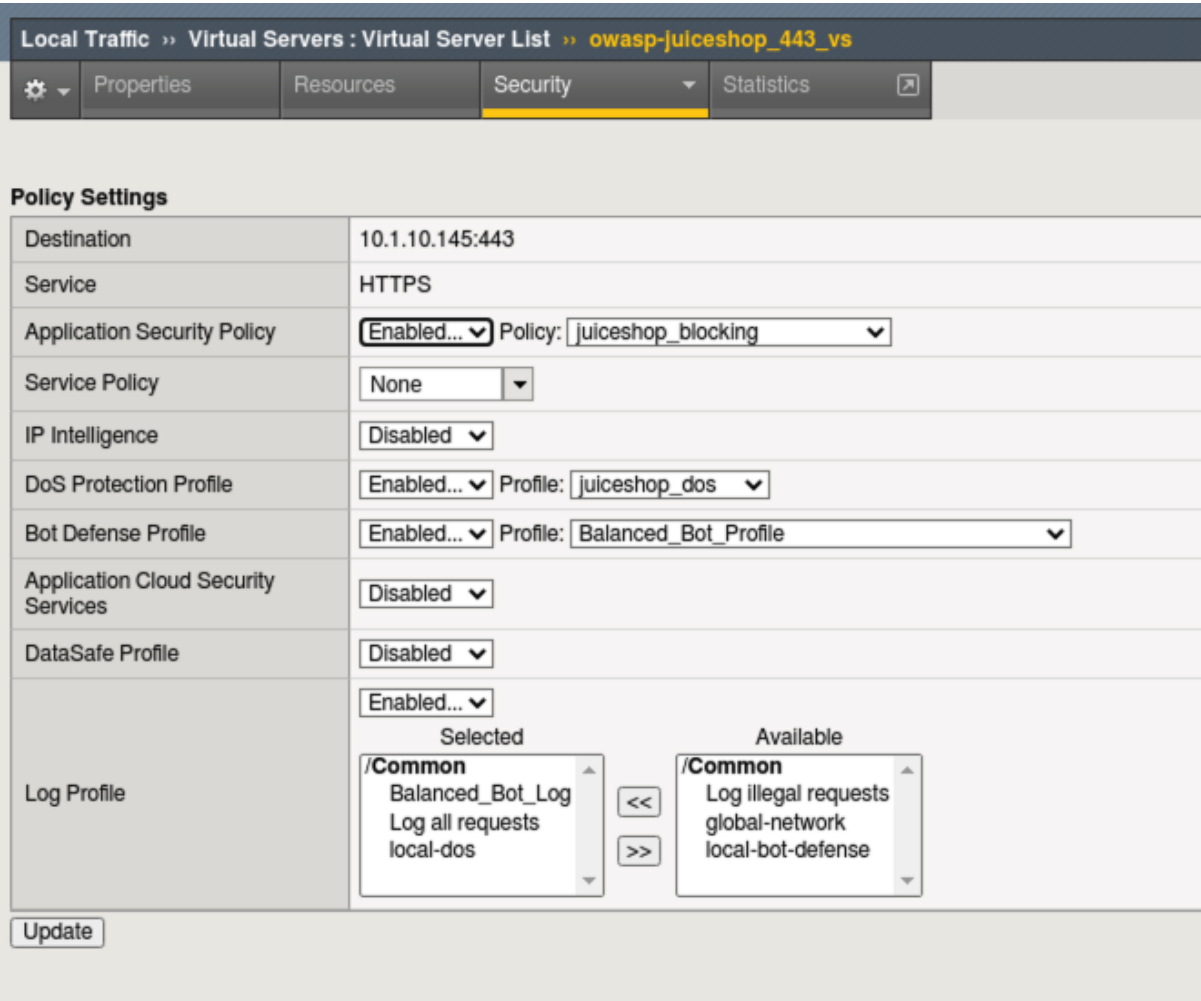


Lab 4: Login Page Protection¶

In this final lab we will explore some of the login protection and session tracking capabilities present in F5 Advanced WAF and end with a fully configured Virtual Server. F5 Advanced WAF not only has the capability to gather user identity details from login pages and APM, but can also generate a unique Device-ID for each connected client.

Virtual Server Configuration¶

1. Navigate to **Local Traffic > Virtual Servers > owasp-juiceshop_443_vs > Security > Policies** and enable the Application Security Policy: **juiceshop_blocking**.
2. **Enable** the **Balanced_Bot_Profile** and add both the **Log all requests** and **Balanced_Bot_Log** logging profiles and click **Update**. You can leave the DoS profiles in place. Your fully configured Virtual Server config should look like this:



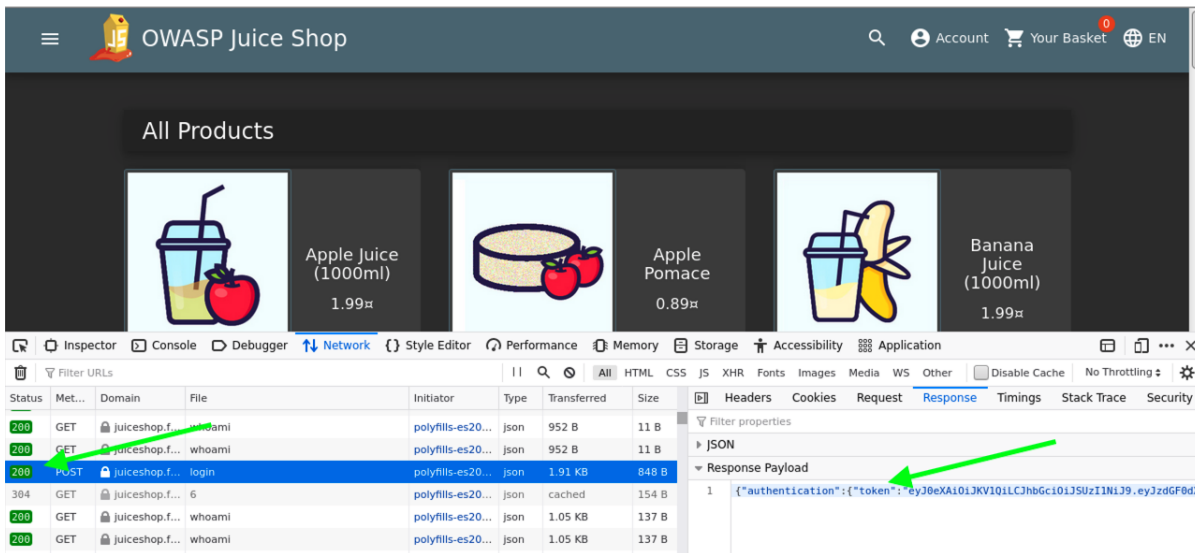
(../_sources/_images/login_vs.png)

Define Login & Logout Pages¶

1. To configure a login page, go to **Security > Application Security > Sessions and Logins > Login Pages List**. Ensure the **juiceshop_blocking** is selected at the top-middle-left of

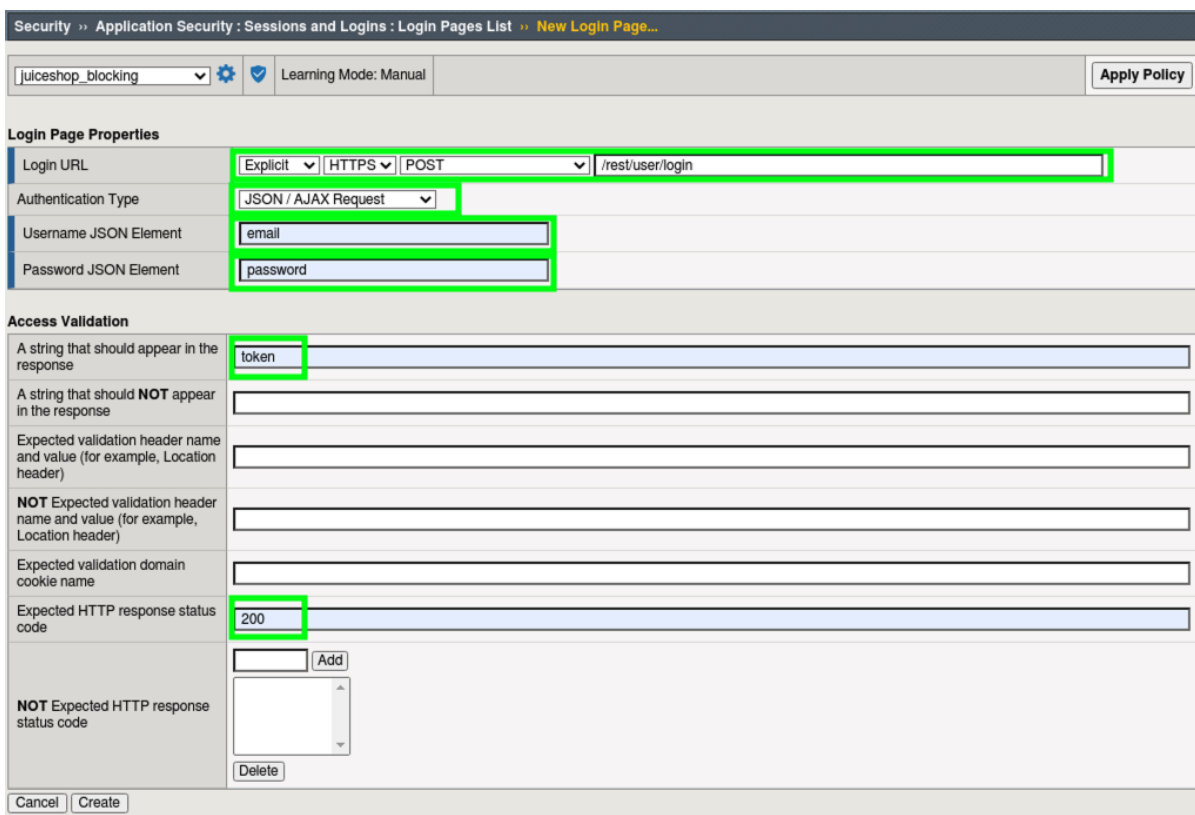
the GUI and click **Create**.

2. We'll now populate the form with data gathered from the browser inspection tools during a login attempt as shown below.



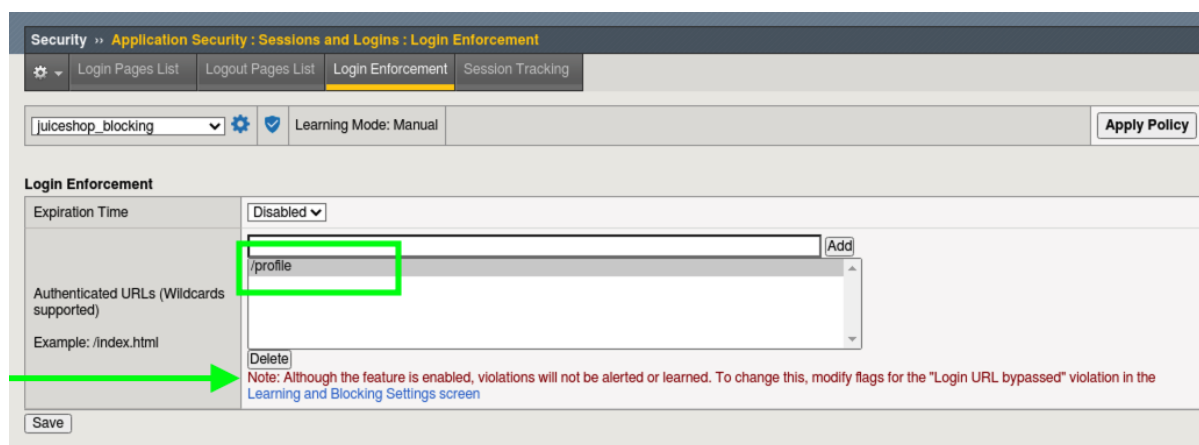
(../../../../_images/response.png)

3. Fill out the **Login Page Properties** and **Access Validation** fields as shown and then click **Create**.



(../../../../_images/loginp.png)

4. From the tab bar at the top middle of the GUI, select **Login Enforcement** and populate the form as shown below. The **/profile** URI should never have attempted access without authentication.
5. Click **Save** and make note of the **Note** in red txt. We will configure **Learning and Blocking Settings** momentarily.



(../../../../images/le.png)

Enable Session Tracking¶

1. Click the **Session Tracking** tab at the top middle of the screen and under **Session Hijacking** click the **Enabled** button. Read through the notes paying close attention to the ones in **red**.
 - For the first red note, regarding the bot profile, we are covered since DeviceID is enabled in our **Balanced_Bot_Profile** by default and it is applied to the VS.
 - The second is more informational and let's us know that non-browser entities will be blocked if they can not run the JS and produce a DeviceID.
 - The third is regarding **Learning and Blocking Settings** which we will configure in a moment.
2. Under **Session Tracking Configuration** Check the box for **Session Awareness** and click **Save** and **Apply Policy**.

Security » Application Security : Sessions and Logins : Session Tracking

Learning Mode: Manual

Session Hijacking

Detect Session Hijacking by Device ID Tracking	<input checked="" type="checkbox"/> Enabled Note: Session cookies will be matched with the unique Device ID that originally received them Note: Device-ID mode must be configured in bot profile for this option to work. Note: Although ASM Cookie Hijacking does not block requests, using device id will block requests from clients that do not support JavaScript Note: Although the feature is enabled, violations will not be alerted or learned. To change this, modify flags for the "ASM Cookie Hijacking" violation in the Learning and Blocking Settings screen
--	---

Session Tracking Configuration

Session Awareness	<input checked="" type="checkbox"/> Enabled
Application Username	<input type="text" value="Use All Login Pages"/> Note: Configure the login page that the system uses to detect the application's user name and associate it with the HTTP session.

Violation Detection Actions

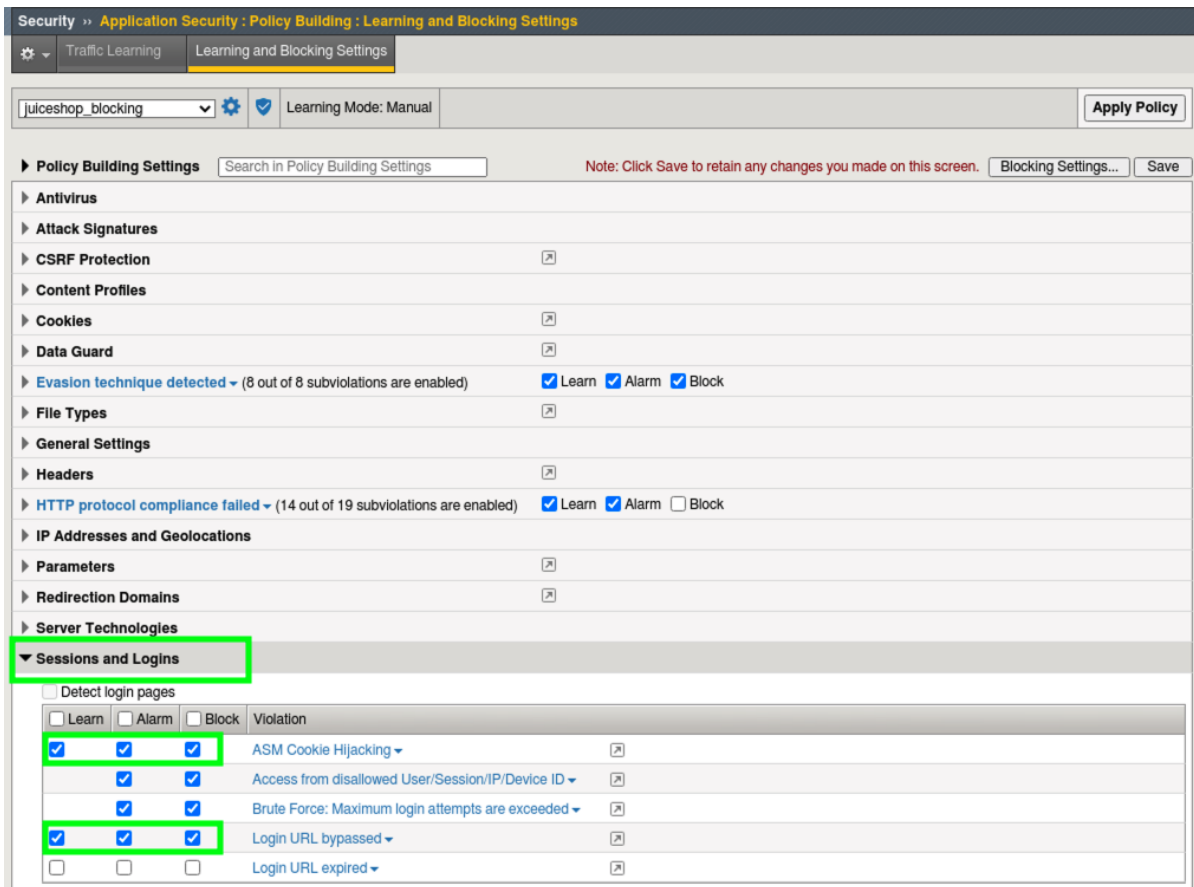
Track Violations and Perform Actions	<input checked="" type="checkbox"/> Enabled
Violation Detection Period	<input type="text" value="900"/> seconds Note: The Violation Action thresholds will track the configured number of violations by counting the number of violations within this time period. For example, a threshold might be "count 10 violation in the last 900 seconds", where the time period used is this value.

[View Session Tracking Status...](#)

Description	When this action is triggered, the system blocks all requests from the user, session, device ID, or IP address, respectively. Which URLs are blocked can be configured with the "Blocked URLs" setting, to allow blocking all URLs or only the Authenticated URLs which are protected by the configured Login Page(s).
Username Threshold	<input type="checkbox"/> Enable <input type="text" value="20"/> violations Note: For users which caused 20 violations in the last 900 seconds , the system will block all requests.
Session Threshold	<input type="checkbox"/> Enable <input type="text" value="20"/> violations Note: For HTTP sessions which caused 20 violations in the last 900 seconds , the system will block all requests.
Device ID Threshold	<input type="checkbox"/> Enable <input type="text" value="30"/> violations Note: For Device IDs which caused 30 violations in the last 900 seconds , the system will block all requests. Note: Device-ID mode must be configured in bot profile for this option to work.
IP Address Threshold	<input type="checkbox"/> Enable <input type="text" value="60"/> violations Note: For IP addresses which caused 60 violations in the last 900 seconds , the system will block all requests.
Blocked URLs	<input checked="" type="radio"/> Block all URLs <input type="radio"/> Block Authenticated URLs [Change Login Enforcement Settings]
Block All Period	<input type="radio"/> Infinite <input checked="" type="radio"/> User-defined: <input type="text" value="600"/> seconds

(../..../_images/session.png)

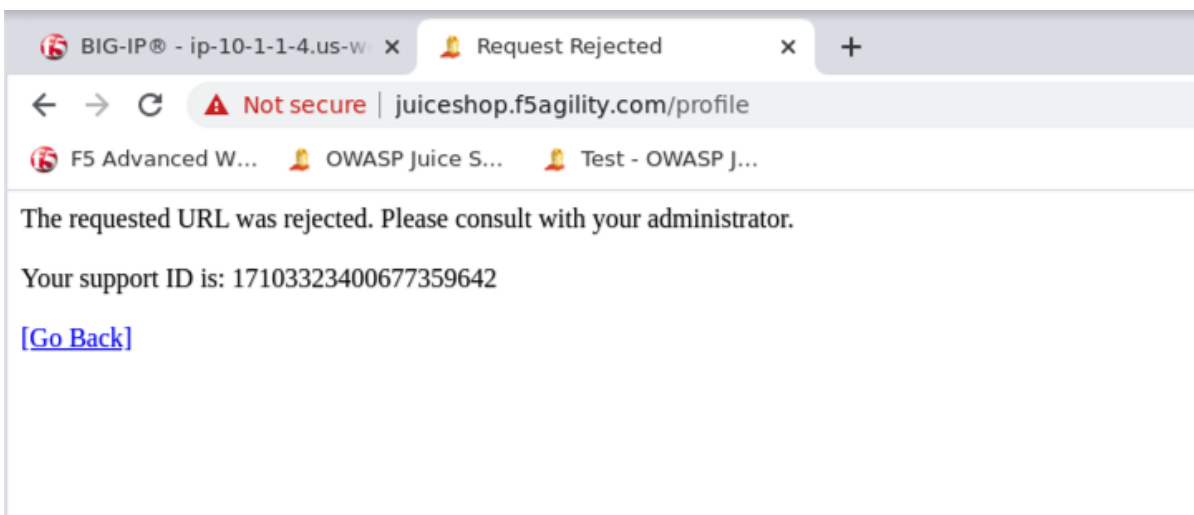
- Navigate to **Security > Application Security > Policy Building > Learning and Blocking Settings > Sessions and Logins**
- Check the box for **Learn, Alarm and Block** for both **ASM Cookie Hijacking** and **Login URL bypassed** and click **Save** and **Apply Policy**.



(../../../../_images/sessionaware.png)

Test Login Enforcement¶

1. Open a new tab in Chrome Browser and paste in the following "login enforced" URL:
https://juiceshop.f5agility.com/profile
2. Your attempt should be blocked:



(../../../../_images/block.png)

3. Back in Advanced WAF tab, navigate to **Security > Event Logs > Application > Requests** and locate the blocked request for **/profile**. Note the reason for the block then click on **View** under Suggestions to open a new tab to the learning suggestions screen.

The screenshot shows the Security console with the 'Event Logs : Application : Requests' tab selected. A list of requests is displayed on the left, including [HTTPS] /profile, [HTTPS] /favicon.ico, and [HTTPS] /assets/public/images/produ... with status icons and scores. The right pane shows the details for a triggered violation: 'Login URL bypassed'. The violation details include a request from 10.1.10.100:52436 to /profile, with a violation rating of 5 (Request is most likely a threat) and enforcement action 'Block'. The request details show a GET request for /profile with various headers and a body size of 607 bytes.

(.././../_images/blocked1.png)

4. You will notice a learning suggestion for this since we enabled learning for this violation in **Learning and Blocking Settings**.
5. Look at this suggestion very carefully. It has a score of 100% and comes from a trusted IP. The suggested action is to **Remove /profile from Authenticated URLs** which is something we definitely DO NOT want to do.
6. Learning suggestions can be tricky especially if they are coming from a trusted source and have a high confidence learning score. Always take a close look at the suggested action. For this suggestion click **Ignore** so no further suggestions are created.

The screenshot shows the Security console with the 'Application Security : Policy Building : Traffic Learning' tab selected. A learning suggestion is displayed for 'Login URL bypassed' with a score of 100%. The suggested action is 'Remove /profile from Authenticated URLs'. The suggestion details include a sample request from 10.1.10.100:52436 to /profile, with a violation rating of 5.0 and a learning score of 100%. The right pane shows the details for the triggered violation, including the request details and enforcement action 'Block'.

(.././../_images/learn1.png)

Test Session Tracking

1. Open a new Chrome Incognito tab by typing (CTRL+SHIFT+N) then open Juice Shop and login with the account you created earlier for f5student@f5agility.com

(mailto:f5student%40f5agility.com).

- Return to the Advanced WAF and navigate to **Security > Event Logs > Application > Requests** and click on any of them except for `/socket.io`. Click **All Details** to the right.

The screenshot shows the F5 Advanced WAF interface. The top navigation bar includes 'Security > Event Logs > Application > Requests'. Below this, there are tabs for 'Application', 'Protocol', 'Network', 'DoS', 'Bot Defense', and 'Logging Profiles'. The 'Requests' tab is active, showing a list of requests on the left and the 'Request Details' for a selected request on the right. The 'Request Details' section is divided into two panes: 'Basic' and 'All Details'. The 'All Details' pane is currently selected, showing various fields such as 'Geolocation', 'Source IP Address', 'Device ID', 'Time', 'Username', 'Session ID', 'Source IP Intelligence', 'Host', 'Destination IP Address', 'Client Type', 'Accept Status', 'Support ID', 'Protocol Info', 'Enforcement Action', 'Enforced By', 'Violation Rating', 'Attack Types', 'Request Status', 'Blocking Exception Reason', 'Security Policy', 'Virtual Server', 'Method', 'Response Status Code', 'Challenge Failure Reason', 'Severity', and 'Signatures CVEs'. The 'Device ID' field is highlighted with a green box.

(../..../_images/sessions.png)

- Click the down arrow next to **Device ID** to open the Session Tracking details. Check the box to enable **Log All Requests** and click **Change**. You are now tracking all sessions from this Device ID.

The screenshot shows the F5 Advanced WAF interface. The top navigation bar includes 'Security > Event Logs > Application > Requests'. Below this, there are tabs for 'Application', 'Protocol', 'Network', 'DoS', 'Bot Defense', and 'Logging Profiles'. The 'Requests' tab is active, showing a list of requests on the left and the 'Request Details' for a selected request on the right. The 'Request Details' section is divided into two panes: 'Basic' and 'All Details'. The 'All Details' pane is currently selected, showing various fields such as 'Geolocation', 'Source IP Address', 'Device ID', 'Time', 'Username', 'Session ID', 'Source IP Intelligence', 'Host', 'Destination IP Address', 'Client Type', 'Accept Status', 'Support ID', 'Protocol Info', 'Enforcement Action', 'Enforced By', 'Violation Rating', 'Attack Types', 'Request Status', 'Blocking Exception Reason', 'Security Policy', 'Virtual Server', 'Method', 'Response Status Code', 'Challenge Failure Reason', 'Severity', and 'Signatures CVEs'. The 'Device ID' field is highlighted with a green box, and the 'Session Tracking details' dialog is open, showing the 'Log All Requests' checkbox checked.

(../..../_images/did.png)

- Repeat this process for the username field as well to track all sessions from **f5student**

Security » Event Logs : Application : Requests

Application Protocol Network DoS Bot Defense Logging Profiles

Order by Date Newest

Requests

Delete Export

[HTTPS] /assets/public/images/products/ccg_foil.png

Request Details

Geolocation N/A

Source IP Address 10.1.10.100:54074

Device ID 87b983d1

Microservice N/A

Time 2021-03-11 10:48:39

Username f5student@f5agility.com

Session Tracking details

Action Flag	State at Log Time	Current State
Log All Requests	Disabled	<input checked="" type="checkbox"/> Enabled
Delay Blocking	Disabled	<input type="checkbox"/> Enabled
Block All	Disabled	<input type="checkbox"/> Enabled

Change Release All

Support ID 17103323400677360937

Protocol Info HTTP/1.1

Enforcement Action

Enforced By

Violation Rating

Attack Types

Request Status

Blocking Exception Reason

Security Policy

Virtual Server

Method

Response Status Code

Challenge Failure Reason

Severity

Signatures CVEs

(../_images/user.png)

5. Navigate to **Reporting > Application > Session Tracking Status** and review the entries that were just created from the application request event log.
6. Click "View Requests" for either of them to see all requests filtered by either the Device ID or Username. You may also use this page to release the Username or Device ID from Session Tracking.
7. These features are useful for forensic purposes as well as blocking access to applications by Device-ID, Username, etc.
8. Finally, navigate to **Security > Application Security > Sessions and Logins > Session Tracking** and review the other more detailed actions you can take based off of Device ID, Username etc.

This concludes Lab 4