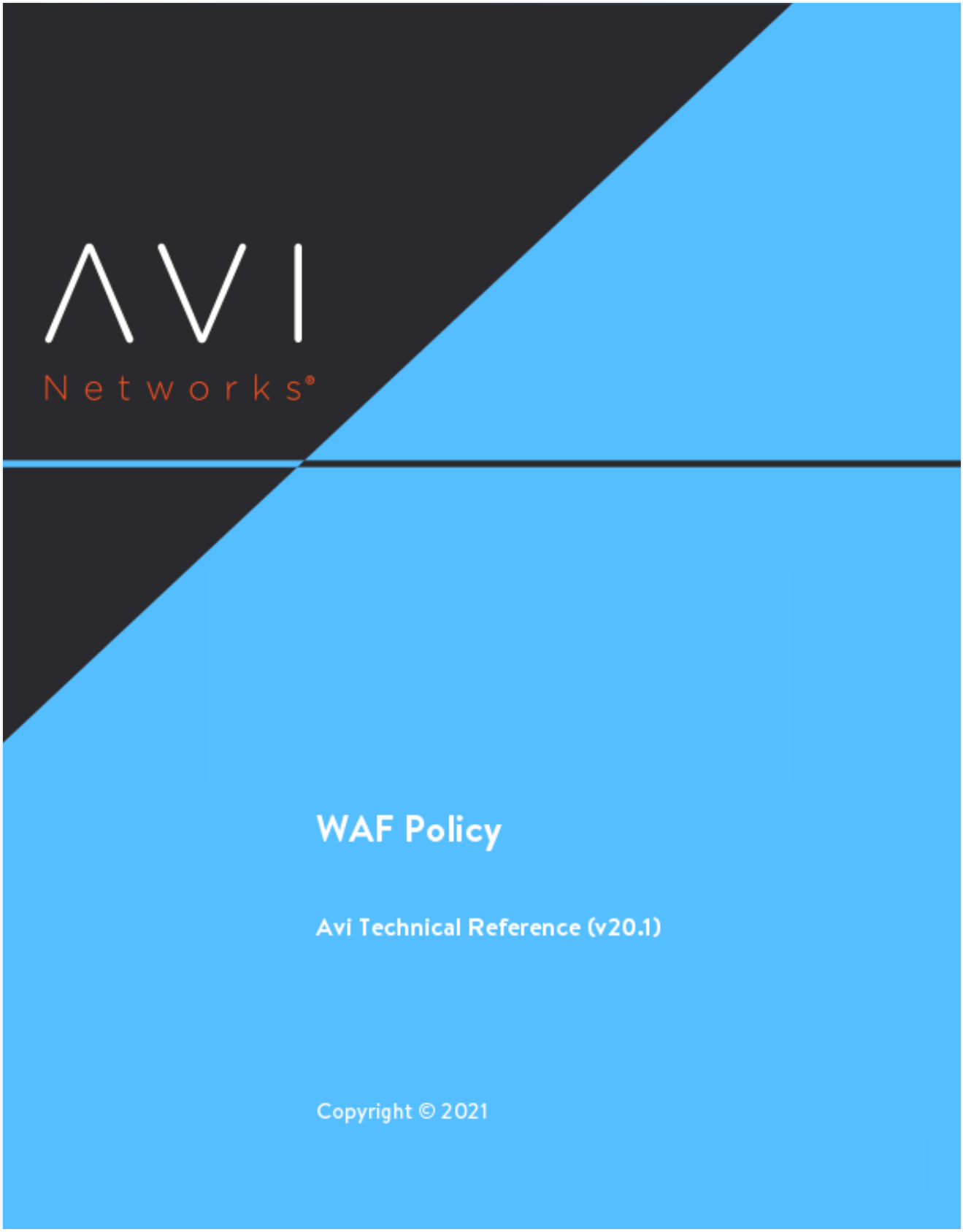


WAF Policy

Avi Technical Reference (v20.1)

WAF Policy

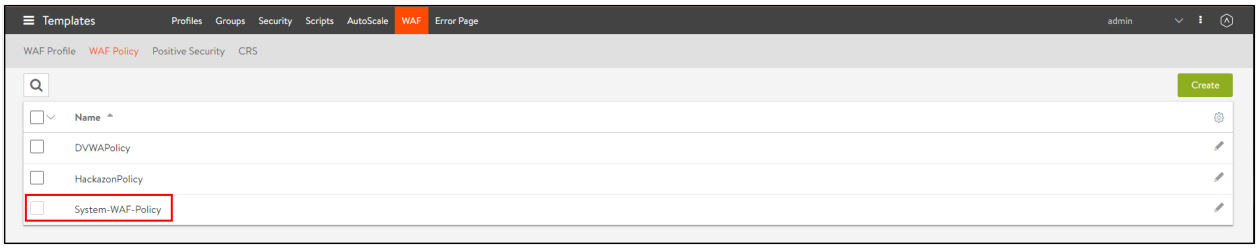
view online

Overview

WAF policy is a specific set of rules that protects the application. This policy is enabled by associating it with a virtual service.

System-WAF-Policy is the default policy in Avi Vantage that contains the latest curated Avi release of the OWASP CRS rules.

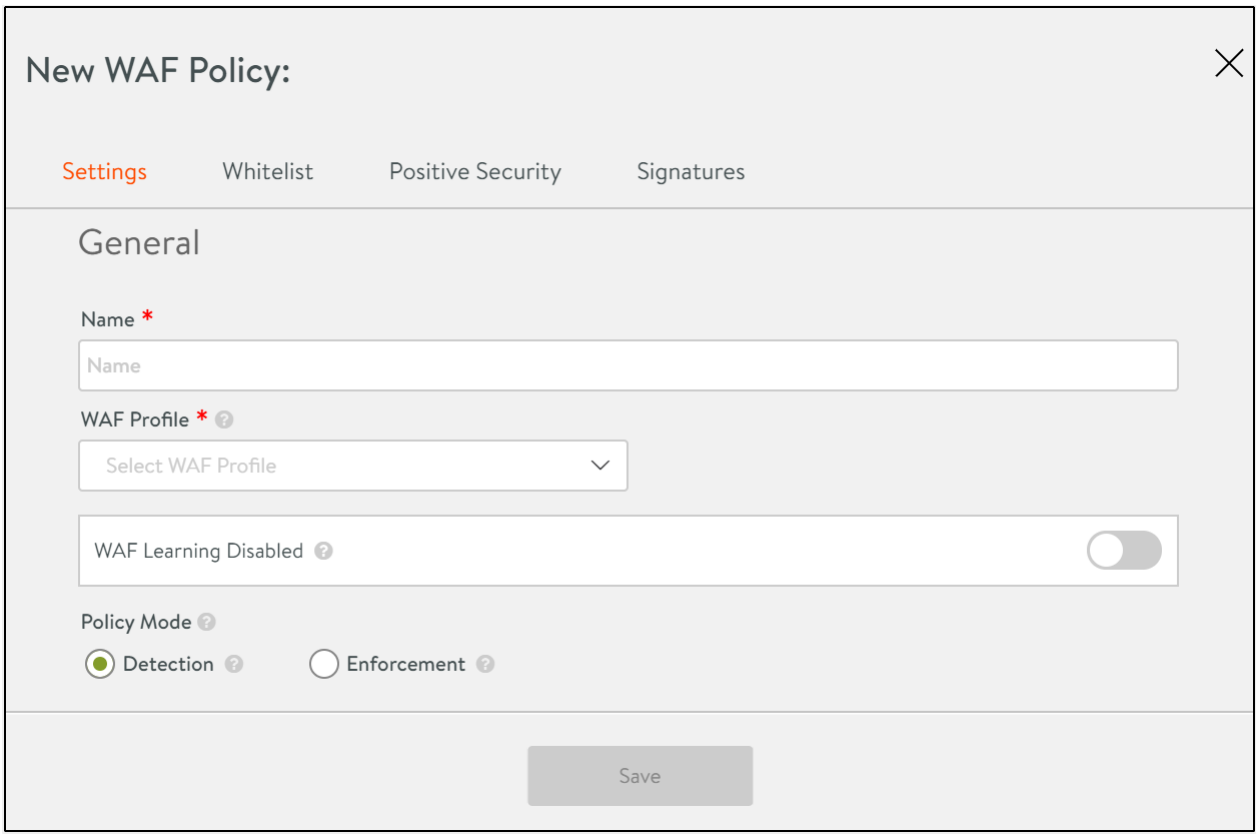
Navigate to Templates > WAF > WAF Policy to find System-WAF-Policy.



Note: For customizing a policy, it is recommended to create a new policy instead of editing the default policy (System-WAF-Policy).

Creating a WAF Policy

To create a new policy, 1. Navigate to Templates > WAF > WAF Policy. 2. Click on Create.
The New WAF Policy screen is as shown below:



3. Configure the new WAF policy under the following tabs: * Settings * Allowlist * Positive Security * Signatures 4. Click on the Save button to create the WAF policy.

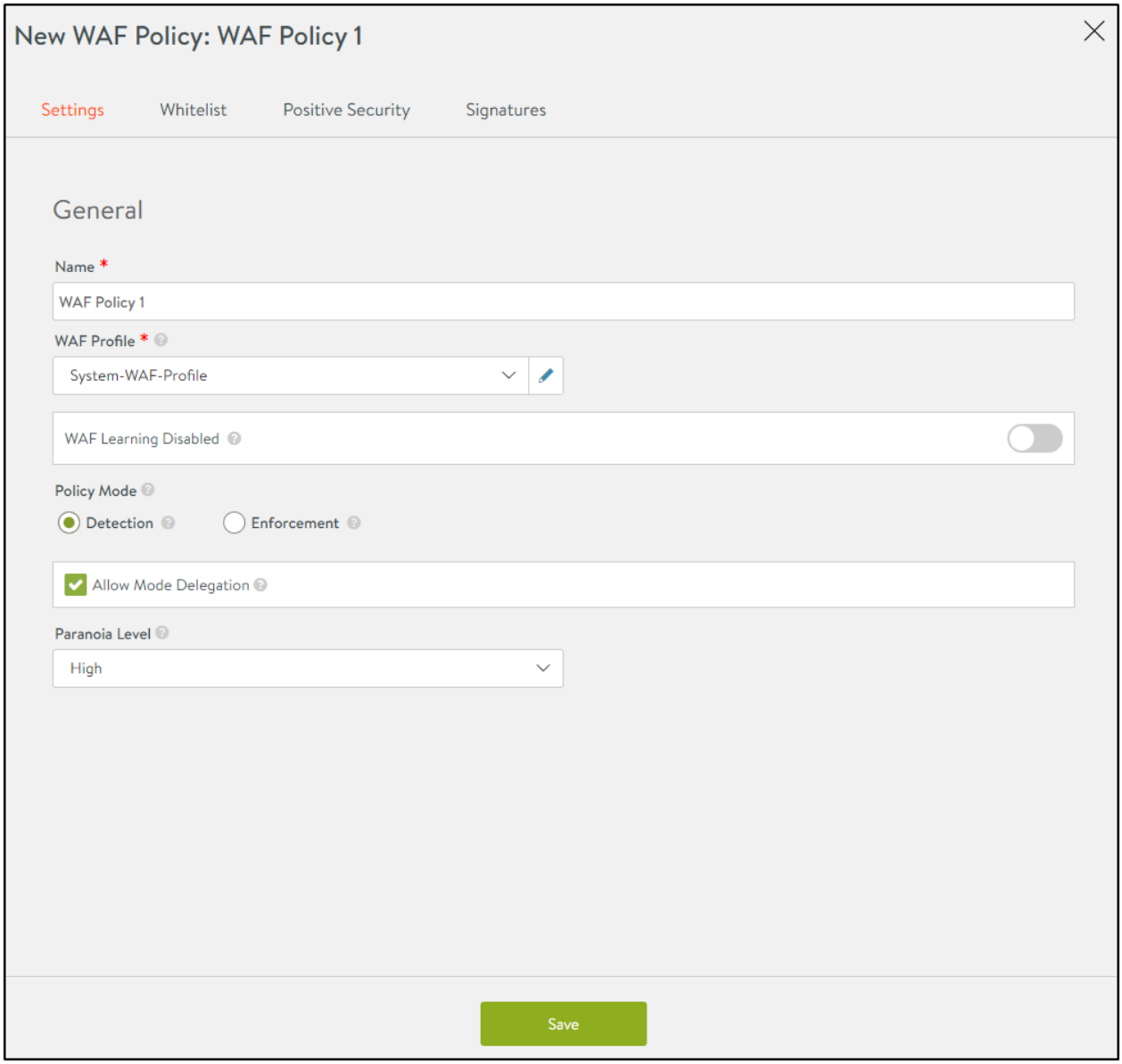
Settings

Under the settings tab, basic information about the WAF policy is configured. This is where the WAF profile for the policy is selected. Note: The new WAF policy inherits the configuration of default policy System-WAF-Policy.

In the New WAF Policy screen, enter information as shown below:

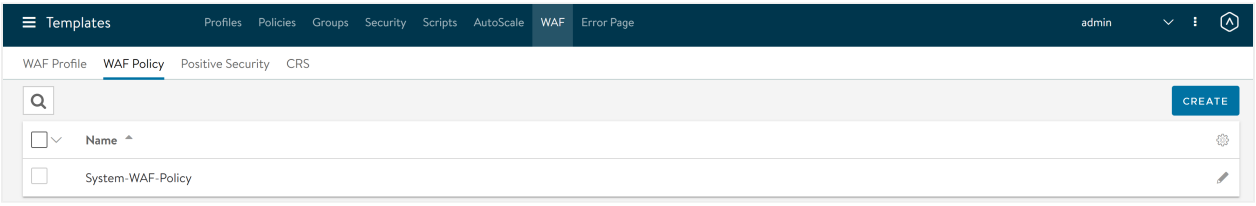
Field	Description
Name	Enter a relevant name for the policy.
WAF Profile	Choose a WAF Profile that should be attached to this policy. The profile contains common reusable settings that complement the WAF policy. The drop down menu allows to create a new WAF Profile as well.
WAF Learning Disabled	Click on the toggle button to switch to WAF Learning Enabled. This will enable Application Learning for this policy as well as setup the Positive Security learning group.
Policy Mode	Select a WAF policy mode: • Detection: The WAF rules are processed but HTTP transactions are not intercepted, even when the rules are configured to do so. • Enforcement: WAF rules are processed and HTTP transactions are intercepted, as per the rules. Note: Individual rules can overwrite the WAF Policy policy mode if Allow Mode Delegation is configured.
Allow Mode Delegation	Enable this option to allow rules to overwrite the policy mode selected. Note: The Allow Mode Delegation check box is only enabled if the policy mode selected is Detection, since it is required for Enforcement mode.
Paranoia Level	Set the paranoia level for the WAF policy. This is used to determine the rigidity of the policy and has a direct impact on potential false positive rate. For more information, refer to the Paranoia Mode.

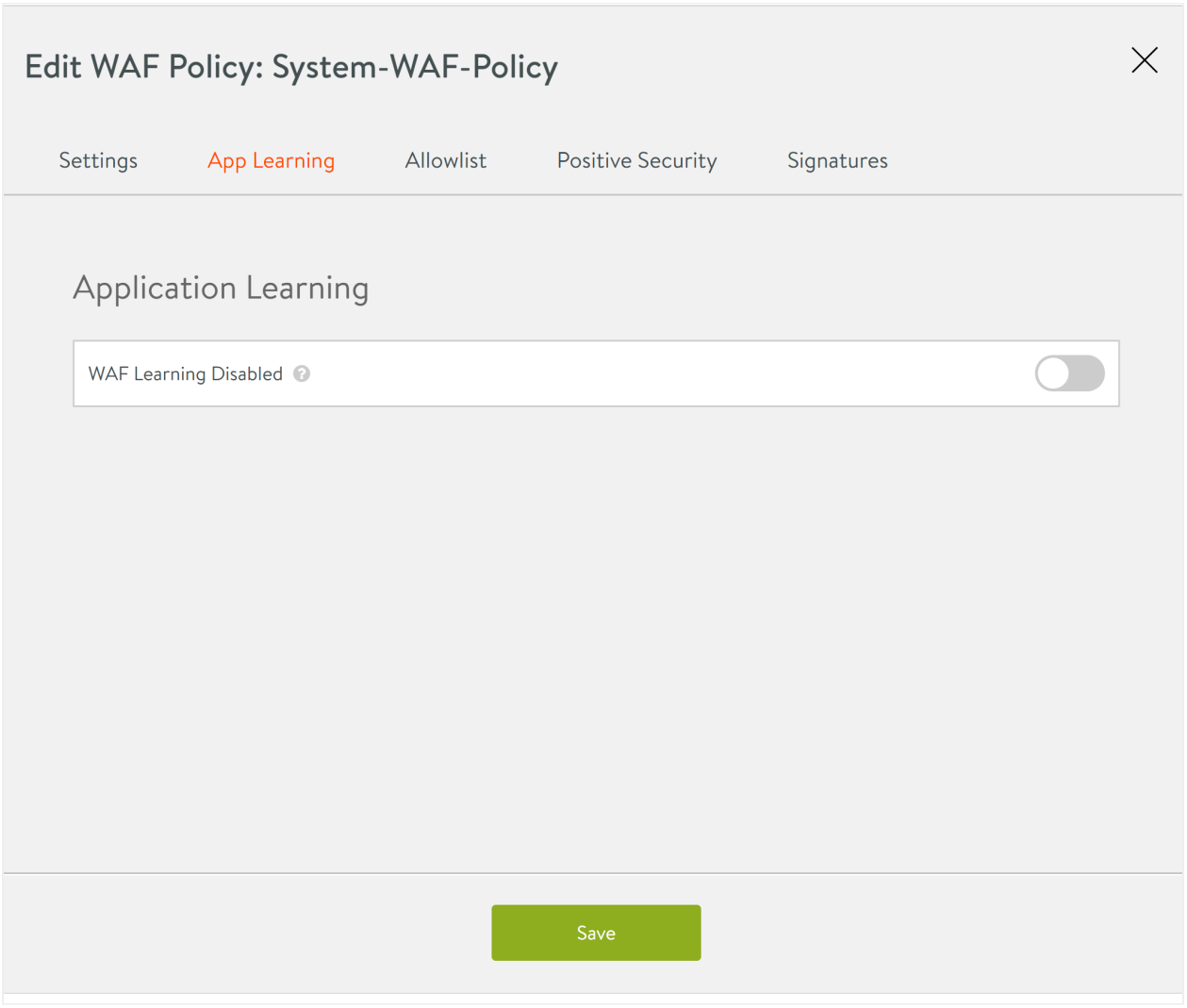
The New WAF Policy screen is as shown below:



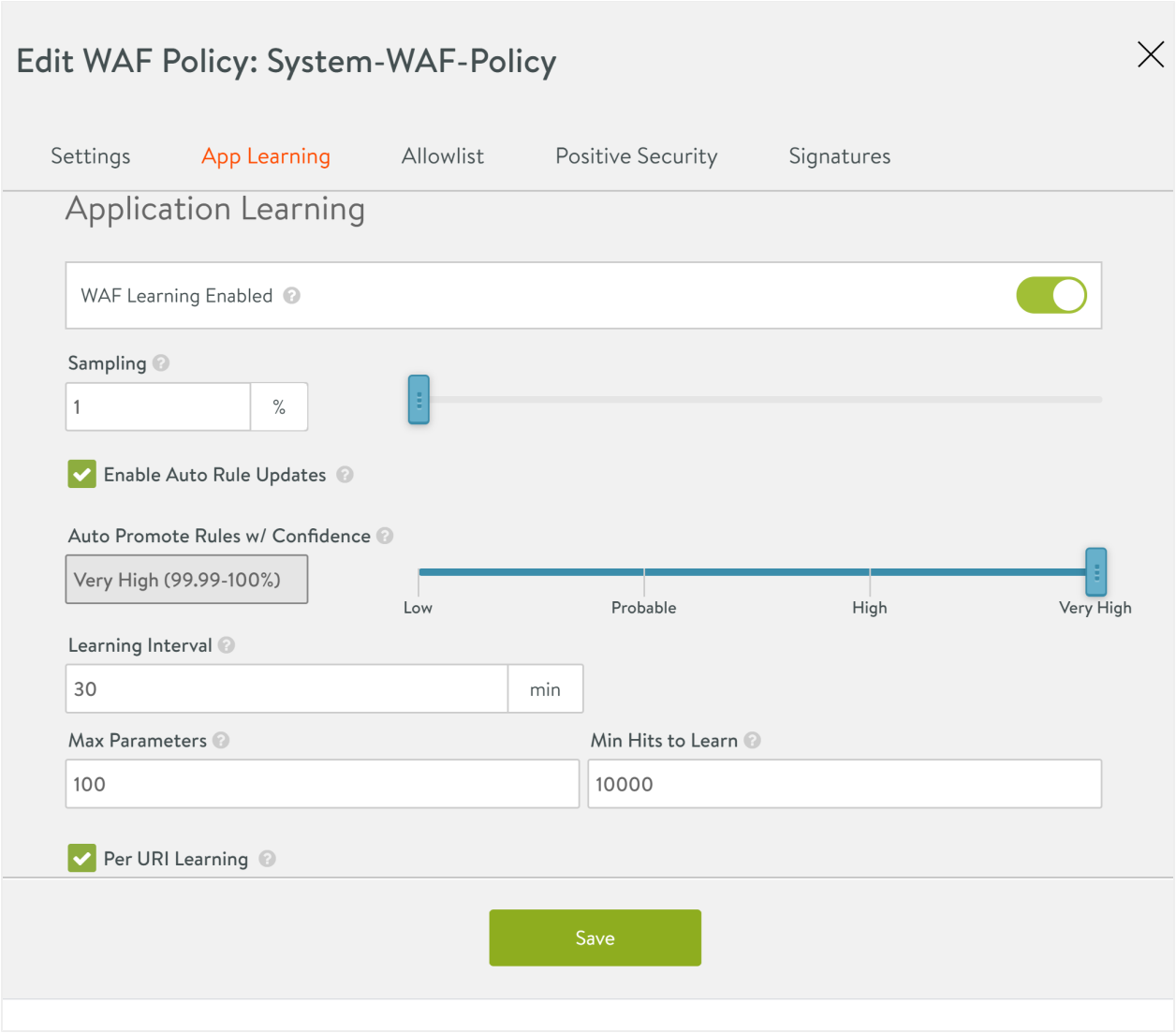
App Learning Option for Avi Vantage Release 20.1.1

Starting with Avi Vantage release 20.1.1, the *App Learning* option is available under the WAF Policy tab. Prior to Avi Vantage release 20.1.1, this option is available under the WAF Profile tab.
The screenshot below exhibits the option to enable *Appl Learning* under the WAF Policy tab. Navigate to Template > WAF > WAF Policy. Select the policy for which *App Learning* should be enabled.





Enable the App Learning for the selected WAF policy. Once the option is enabled, the additional configuration options will be available to edit, as shown below.



Allowlist

A allowlist is a set of conditions which when matched by a request, directs WAF to skip parts or the whole of the WAF policy. Under the Allowlist tab, configure allowlist rules and set match types.

Refer to the Allowlist article for more information.

Positive Security

The Positive Security rules describe how valid application behaviour should look like. Under the Positive Security tab positive security groups can be defined that consist of locations and argument rules.

Refer to the Positive Security article for more information.

Signatures

The final step in WAF processing is a Signature check. Under the Signatures tab, configure Pre-CRS, CRS, and Post-CRS rules.

Refer to the WAF Policy Signatures article for more information.

Changes Introduced in Avi Vantage release 20.1.6

Starting with Avi Vantage release 20.1.6, the following two fields are deprecated while creating the WAF policy using the CLI and the API: * *crs_groups* * *application_signatures.rules* The above mentioned groups and rules are now taken directly from the referenced *wafcrs* and the respective *wafapplicationsignatureprovider* object.

The following new fields are available instead of the deprecated fields as mentioned above: * *crs_overrides* * *application_signatures.rule_overrides*

These fields are used to perform configuration changes, like setting the mode attribute or adding the exclude_list settings for a rule or group.

The code snippet below exhibits the change introduced in the Avi Vantage 20.1.6 release.

```
{
    "name": "Example Policy 1",
    "waf_mode": "WAF_MODE_ENFORCEMENT",
    "waf_profile_ref": "/api/wafprofile?name=System-WAF-Profile",
    "waf_crs_ref": "/api/wafcrs?name=CRS-2020-3",
    "crs_overrides": [
        {
            "name": "CRS_903.9002_Wordpress_Exclusion_Rules",
            "enable": true
        },
        {
            "name": "CRS_920_Protocol_Validation",
            "rule_overrides": [
                {
                    "rule_id": "920310",
                    "enable": false
                },
                {
                    "rule_id": "920311",
                    "enable": false
                }
            ]
        },
        {
            "name": "CRS_930_Application_Attack_LFI",
            "rule_overrides": [
                {
                    "rule_id": "930120",
                    "exclude_list": [
                        {
                            "match_element": "ARGS:path",
                            "match_element_criteria": {
                                "match_case": "INSENSITIVE"
                            }
                        }
```

```
                    ]
                }
            ]
        }
    ]
}
```