AppViewX

ASM Policy Creation

Operations Guide

Version	Remarks	Date
1.0	Provisioning Template Operation Guide for ASM Policy creation.	18/01/2017

1. CREATING ASM POLICY.

1. Login to AppViewX.
2. On the left navigation menu, select ***Provisioning***; and click ***Request.***
3. On the upper right portion of the screen, click the + ***Create*** button.
4. Select the provisioning template name from the list –‘**ASM_Policy_Creation_Template_v5**’

Note: *If no template is available, this indicates that the user role does not have permission to the requesting template.*

5. Enter the provisioning request description – ‘*ASM Policy Creation*’.
6. Enter the Request Scenario Name relevant to the template. ***E.g***.: ASM Policy Creation.
7. In the Device List field, list of F5 device versions are populated. Please select the version of F5 device on which the ASM policy has to be created.
8. In the **Policy Name** field, Please enter a Relevant Policy name.
9. In the **Description** field, enter the description of the security policy. Type in any helpful details about the policy.
10. In the **Select Partition** field, list of the available partitions are populated based on the *F5 device*. Please select the relevant partition. ***E.g***.: Common.
11. In the **Auto Policy Builder** field, select the necessary option (Enabled or Disabled).
12. In the **Predefined Template** field, list of available Predefined Templates are populated. Please select the appropriate Template.
13. In The **Enforcement Mode** Field, Select the option of how the system processes a request that triggers a security policy violation (Transparent or Blocking).
14. In the **Enforcement Readiness Period** Field, Enter the number of days for the Enforcement Readiness period.
15. In the **Encoding Method** field, select the relevant method of encoding from the list populated.
16. Click on the ‘***Get Virtual Server***’ to fetch the list of Virtual servers available in the inventory for the selected F5 device.

17. In the **Virtual Server(S) field,** select the relevant virtual servers which are needed from the populated list.

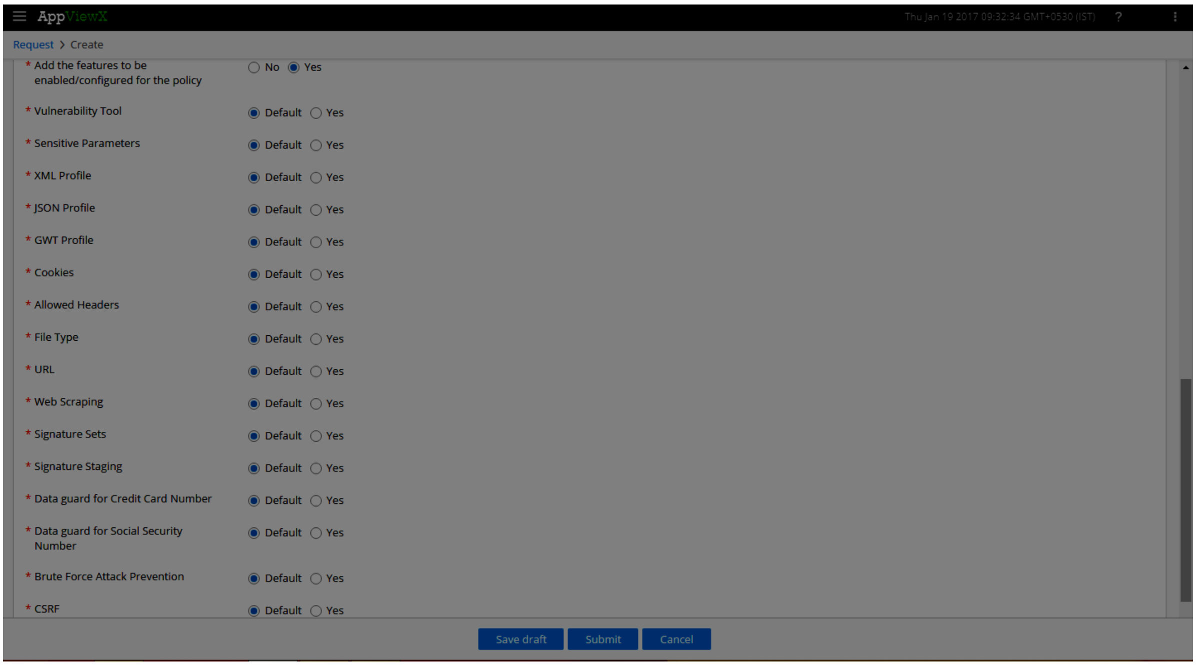
18. In the **Source filter – Whitelist IP/Mask** field, enter the source IP which has to be in the Whitelist IP.

19. In the **Whitelist IP/Mask** field, enter the IP list which have to be in the Whitelist IP.

20. In the **Source filter – Disallowed locations** field, select the location(s) which are to be disallowed from the given list.

21. Added Features can be enabled/Configured for the policy by selecting it. If not needed, please select no.

    If yes is selected, the following features are displayed.



* Add the features to be enabled/configured for the policy ○ No ● Yes

* Vulnerability Tool ● Default ○ Yes

* Sensitive Parameters ● Default ○ Yes

* XML Profile ● Default ○ Yes

* JSON Profile ● Default ○ Yes

* GWT Profile ● Default ○ Yes

* Cookies ● Default ○ Yes

* Allowed Headers ● Default ○ Yes

* File Type ● Default ○ Yes

* URL ● Default ○ Yes

* Web Scraping ● Default ○ Yes

* Signature Sets ● Default ○ Yes

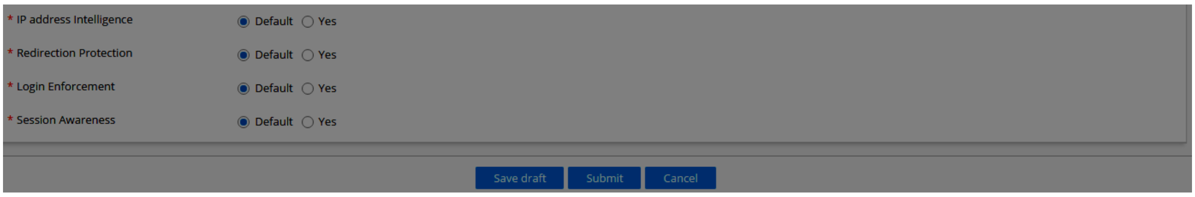
* Signature Staging ● Default ○ Yes

* Data guard for Credit Card Number ● Default ○ Yes

* Data guard for Social Security Number ● Default ○ Yes

* Brute Force Attack Prevention ● Default ○ Yes

* CSRF ● Default ○ Yes



* IP address Intelligence ● Default ○ Yes

* Redirection Protection ● Default ○ Yes

* Login Enforcement ● Default ○ Yes

* Session Awareness ● Default ○ Yes

There is a Default option for all these features which will have the default settings.

If yes is selected for these added features:

i. If **Vulnerability Tool** is selected as yes,

   a) Select the Vulnerability tool name from the populated list.

ii. If **Sensitive Parameters** is selected as yes,

a) Specify the sensitive Parameters in the sensitive parameters field and click + button. If parameters are already present we can select it from the populated list.

iii. If **XML Profile** is selected as yes,

a) Specify the **XML Profile Name** in the corresponding field.

b) Select the option to **Check Signatures** (Y/N).

c) Select the Defence level which has to be set (High/Medium/Low).

iv. If the JSON profile is selected as yes,

a) Please Enter the **JSON Profile Name.**

b) Select the option to **Check Signatures** (Y/N).

c) Enter the **Maximum Total length of JSON data in Bytes.**

d) Enter the **Maximum Value length in bytes.**

e) Enter the **Maximum Structure depth.**

f) Enter the **Maximum Array length.**

g) Select the choice to **Tolerate JSON Parsing Warnings** (Enable/Disable).

v. If **GWT Profile name** is selected as yes,

a) Please Enter the **GWT profile Name.**

b) Select the option to **Check Signatures** (Y/N).

c) Enter the **Maximum Total length of GWT data in Bytes.**

d) Enter the **maximum Value length in bytes.**

e) Select the option to **Tolerate GWT Parsing Warnings** (Enable/Disable).

vi. If **Cookie** is selected as yes,

a) Select the **Category** of the cookie (Allowed/Enforced).

b) Please Enter the **Cookie Name.**

c) Select the type of cookie from the given list (Wildcard/Explicit).

vii. If **Allow Headers** is selected as yes,

a) Please Enter the **Name** of the Header.

b) Select the **Method** (Get/Post).

viii. If **File Type** is selected as yes,

a) Select the **Category** of the File type (Allowed/Disallowed).

b) Please Enter the **Name.**

c) Select the Type from the given list (Wildcard/Explicit).

ix. If **URL** is selected as yes,

a) Select the **Category** of the URL (Allowed/Disallowed).

b) Please Enter the **Name of the URL.**

c) Please select the protocol (HTTP/HTTPS).

d) Select the type from the given list (Wildcard/Explicit).

x. If **Web Scraping** is selected as yes,

a) Select the option to Enable/Disable **Bot detection alarm.**

b) Select the option to Enable/Disable **Bot detection alarm & Block.**

c) Select the option to Enable/Disable **Session opening Anomaly Alarm.**

d) Select the option to Enable/Disable **Session opening Anomaly Alarm & Block.**

e) Select the option to Enable/Disable **Fingerprints.**

xi. If **Signature Sets** is selected as yes,

a) Retrieve the Signature set name by clicking on 🔍 and select it from the list populated.

xii. The Following Remaining Features can be added by Selecting the yes option:

a) Signature Staging.

b) Data guard for credit card number.

c) Data guard for social security number.

d) Brute force attack prevention.

e) Cross Site Request Forgery (CSRF).

f) IP Address Intelligence.

g) Redirection Protection.

h) Login Enforcement.

i) Session Awareness.

22. Click on *Submit* to generate work order(s) for the provisioning request.