

# ASM Deployment

diagram\_05.png

## API Security

Manual Chapter v13.1.0: [Implementing Web Services Security](#)

Manual Chapter v13.1.0: [Creating Parent and Child Security Policies](#)

## Fundamental, Enhanced, Comprehensive

Fundamental = Grundlegend

Enhanced = Verbessert

Comprehensive = Umfassend

The following is from the v12 UI (Security - Application Security : Policy Building : Learning and Blocking Settings, Policy Type)

<b>Fundamental</b>	<b>Enhanced</b> <b>Fundamental plus:</b>	<b>Comprehensive</b> <b>Enhanced plus:</b>
--------------------	---	---

<ul style="list-style-type: none"> <li>• HTTP Protocol Compliance</li> <li>• Evasion Techniques</li> <li>• Learn New File Types + Lengths</li> <li>• Learn New Parameters in selective mode at Global level</li> <li>• Methods</li> <li>• Attack Signatures</li> <li>• Request length exceeds defined buffer size</li> <li>• Host Names</li> <li>• Failed to convert character</li> <li>• Learn New Redirection Domains</li> <li>• Bad WebSocket handshake request</li> <li>• Failure in WebSocket framing protocol</li> <li>• Mask not found in client frame</li> <li>• Null character found in WebSocket text message</li> <li>• Illegal websocket frame length</li> <li>• Illegal number of frames per message</li> <li>• Illegal binary message length</li> <li>• Illegal WebSocket extension</li> </ul>	<ul style="list-style-type: none"> <li>• Learn New URLs in selective mode + Meta Characters</li> <li>• Learn New Parameters in selective mode + Lengths, at Global level</li> <li>• Learn New Cookies</li> <li>• Content Profiles</li> <li>• Bad WebSocket handshake request</li> <li>• Failure in WebSocket framing protocol</li> <li>• Mask not found in client frame</li> <li>• Null character found in WebSocket text message</li> <li>• Illegal websocket frame length</li> <li>• Illegal number of frames per message</li> <li>• Illegal binary message length</li> <li>• Illegal WebSocket extension</li> <li>• Illegal cross-origin request</li> <li>• Plain text data does not comply with format settings</li> </ul>	<ul style="list-style-type: none"> <li>• Learn New URLs + Meta Characters, Classify Request Content</li> <li>• Learn New Parameters + Lengths, at URL level, Classify Value Content</li> <li>• Parameter Meta Characters</li> <li>• Dynamic Parameters: Using Statistics</li> <li>• CSRF URLs</li> <li>• Header Length</li> <li>• Cookie Length</li> <li>• Bad WebSocket handshake request</li> <li>• Failure in WebSocket framing protocol</li> <li>• Mask not found in client frame</li> <li>• Null character found in WebSocket text message</li> <li>• Illegal websocket frame length</li> <li>• Illegal number of frames per message</li> <li>• Illegal binary message length</li> <li>• Illegal WebSocket extension</li> <li>• Illegal cross-origin request</li> <li>• Plain text data does not comply with format settings</li> <li>• Binary content found in text only WebSocket</li> <li>• Text content found in binary only WebSocket</li> </ul>
--	--	--

<https://devcentral.f5.com/questions/asm-confusion-about-wildcard-selective-all-entities-49185>

-> “Add All Entities Creates a comprehensive whitelist policy that includes all web site entities”

## Learning Schemes to build a policy

- **Never (wildcard only)**, when false positive occur the system will suggest to relax the settings of the wildcard entity.
- **Selective** is that only entity (Parameter name/value, URL etc) that exceeds the Wildcard setting would generate learning suggestion and those learning suggestion are accepted by administrator entity will get included in security policy.
  - Selective mode offers intermediate protection between Never (Wildcard Only) and Add All Entities.

- Selective mode is suitable for applications containing entities which use similar or identical attributes.
- Ideally, when you know the policy is mature, you can remove the wildcard
- **Add All Entities**, you will see a suggestion to add an entity by name

# BIG-IP ASM Policy Builder updates

## BIG-IP 13.0

Updates to Policy Builder in BIG-IP 13.0 include the following enhancements:

- **Compact mode** is an entity learning mode designed to effectively manage high traffic loads and increase policy security.
  - Compact mode reduces the amount of learning suggestions, enabling a policy to converge more quickly, and automatically adds disallowed file types.
  - Compact mode will never removing the wildcard.
- **Server Technologies** is an option that customizes policies to an application. This option enables Policy Builder to identify the back-end technologies used by an application and add the relevant signatures to the policy.
- **Client Reputation** is a technique that improves learning suggestions by using behavioral analysis to assign a reputation score to a source IP or device ID. Policy Builder ignores sources classified as malicious and speeds learning on sources classified as benign.

## BIG-IP 12.0

There are several updates to Policy Builder in BIG-IP 12.0, including the following:

- Staging, enforcement, and learning suggestions can be configured manually or by the BIG-IP ASM system.
- Security checks Learn, Alarm, and Block are now system-wide settings integrated with Policy Builder.
- An improved learning suggestions mechanism handles requests, with or without violations, for manual and automated policy building.

## Links

- [Using Rapid Deployment](#)
- [BIG-IP Application Security Manager Operations Guide](#)
- [Use ASM for Block Page Example](#)
- [DevCentral: F5 ASM deployment for production traffic in transparent mode](#)
- [DevCentral: Lightboard Lessons: BIG-IP ASM Policy Buildin](#)
- [DevCentral: Different Blocking pages for different violation?](#)

---

Revision #2

Created 17 March 2021 05:26:54

Updated 20 September 2022 09:58:29