BIG-IP® Application Security Manager™: Getting Started

Version 12.0

Table of Contents

Legal Notices

Legal notices

Publication Date

This document was published on September 1, 2015.

Publication Number

MAN-0285-10

Copyright

Trademarks

Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Introduction to Application Security Manager

What is Application Security Manager?

Application Security Manager™ (ASM) is a web application firewall that secures web applications and protects them from vulnerabilities. ASM also helps to ensure compliance with key regulatory mandates. The browser-based user interface provides network device configuration, centralized security policy management, and easy-to-read audit reports.

You can use ASM™ to implement different levels of security to protect Layer 7 applications. You can let ASM automatically develop a security policy based on observed traffic patterns. Or you have the flexibility to manually develop a security policy that is customized for your needs based on the amount of protection and risk acceptable in your business environment.

ASM creates robust security policies that protect web applications from targeted application layer threats, such as buffer overflows, SQL injection, cross-site scripting, parameter tampering, cookie poisoning, web scraping, and many others, by allowing only valid application transactions. Using a positive security model, ASM secures applications based on a combination of validated user sessions and user input, as well as a valid application response. ASM also includes built-in security policies that can quickly secure common applications.

ASM also protects applications using negative security by means of attack signatures. Attack signatures can detect and thwart attacks such as the latest known worms, SQL injections, cross-site scripting, and attacks that target commonly used databases, applications, and operating systems.

All these features work together to identify threats and react to them according to your policy. Application traffic is analyzed by ASM and it can also be load balanced to the web application servers. You can configure ASM so that if malicious activity is detected, ASM can terminate the request, send a customized error page to the client, and prevent the traffic from reaching the back-end systems.

When to use application security

The decision about when to use Application Security Manager™ (ASM) to protect an application can be made on a case-by-case basis by each application and security team.

You can use ASM™ in many ways:

- For securing existing web applications against vulnerabilities and known attack patterns, protecting sensitive data, and proactively identifying (and possibly blocking) attackers performing unauthorized activities.
- To restrict access to a web application only from those locations identified on a whitelist or to prevent access from certain geolocations.
- To help address external traffic vulnerability issues that it might not be cost effective to address at the application level.
- As an interim solution while an application is being developed or modified to address vulnerability issues.
- As a means to quickly respond to new threats. You can tune ASM to block new threats within a few hours of detection if needed.

These are just a few of the ways that ASM can be used to secure your web applications.

Types of attacks ASM protects against

Application Security Manager™ (ASM) protects mission-critical enterprise Web infrastructure against application-layer attacks, and monitors the protected web applications. For example, ASM protects against web application attacks such as:

- Manipulation of cookies or hidden fields
- SQL injection attacks intended to expose confidential information or to corrupt content
- Malicious exploitations of the application memory buffer to stop services, to get shell access, and to propagate worms
- Unauthorized user access to authenticated accounts using cross-site request forgery (CSRF)
- Unauthorized changes to server content
- Attempts aimed at causing the web application to be unavailable or to respond slowly to legitimate users
- Layer 7 denial-of-service, brute force, and web scraping attacks
- Unknown threats, also known as zero-day threats
- Access from unauthorized IP addresses or geolocations

The system can automatically develop a security policy to protect against security threats, and you can configure additional protections and customize the system response to threats.

Performing Basic Configuration Tasks

About basic networking configuration terms

This list summarizes some basic networking configuration terms that you should know before you start configuring the BIG-IP® system and using Application Security Manager™ (ASM).

local traffic policy
The way to direct traffic using rules with conditions the traffic must meet, and specifying actions to take (such as where to route the traffic, what security policies or DoS profiles to assign to traffic, and many other actions). ASM™ automatically creates a local traffic policy when you create a security policy or attach a security policy to a virtual server (manually).

pool
The web server or application server resources that host the web application being protected with a security policy. You can create a local traffic pool, and then assign the pool to a virtual server. On Application Security Manager systems, you can create a pool as part of creating a security policy.

self IP address
An IP address that you associate with a VLAN, to access hosts in that VLAN. You create a self IP address and associate it with a VLAN.

virtual server
The virtual server processes incoming traffic for the web application you are securing. When you create a virtual server manually, you assign the local traffic policy and pool to it. On Application Security Manager systems, you can create a virtual server and pool as part of creating a security policy.

VLAN (virtual local area network)
A logical grouping of network devices. You create a VLAN and associate the physical interfaces on the BIG-IP system with the VLAN. The VLAN can logically group devices on different network segments.

Overview: Performing basic networking configuration tasks

For initial installation, the BIG-IP® hardware includes a hardware setup guide for your platform that you can refer to for details about how to install the hardware in a rack, connect the cables, and run the setup utility. Next, you must configure the BIG-IP system on your network before you can run the Application Security Manager™ (ASM) Deployment wizard to create a security policy. The specific tasks you need to perform depend on your company's networking configuration, and which of the other BIG-IP system features are in use.

For using ASM™, the minimum networking configuration tasks that you need to perform are creating a VLAN and a self-IP address for the system. During the process of creating a security policy, the system helps you complete other necessary configuration tasks, such as creating a virtual server and pool. The tasks are included here in case you want to create them first. For complex networking configurations that also use other BIG-IP features, you need to perform additional tasks described in the respective documentation.

Task summary

Creating a VLAN

VLANs represent a logical collection of hosts that can share network resources, regardless of their physical location on the network. You create a VLAN to associate physical interfaces with that VLAN.

1. On the Main tab, click **Network** > **VLANs**.
   The VLAN List screen opens.
2. Click **Create**.
   The New VLAN screen opens.
3. In the **Name** field, type a unique name for the VLAN.
4. In the **Tag** field, type a numeric tag, between 1-4094, for the VLAN, or leave the field blank if you want the BIG-IP system to automatically assign a VLAN tag.

   The VLAN tag identifies the traffic from hosts in the associated VLAN.
5. From the **Customer Tag** list:
   a) Retain the default value of **None** or select **Specify**.
   b) If you chose **Specify** in the previous step, type a numeric tag, between 1-4094, for the VLAN.

   The customer tag specifies the inner tag of any frame passing through the VLAN.
6. For the **Interfaces** setting,
   a) From the **Interface** list, select an interface number.
   b) From the **Tagging** list, select **Untagged**.
   c) Click **Add**.
7. Click **Finished**.
   The screen refreshes, and displays the new VLAN in the list.

Creating a self IP address for a VLAN

Ensure that you have at least one VLAN configured before you create a self IP address.

Self IP addresses enable the BIG-IP® system, and other devices on the network, to route application traffic through the associated VLAN.

1. On the Main tab, click **Network** > **Self IPs**.
2. Click **Create**.
   The New Self IP screen opens.
3. In the **Name** field, type a unique name for the self IP address.
4. In the **IP Address** field, type an IPv4 or IPv6 address.

   This IP address should represent the address space of the VLAN that you specify with the **VLAN/Tunnel** setting.
5. In the **Netmask** field, type the full network mask for the specified IP address.

For example, you can type `ffff:ffff:ffff:ffff:0000:0000:0000:0000` or `ffff:ffff:ffff:ffff::`.

6. From the **VLAN/Tunnel** list, select the VLAN to associate with this self IP address.
   - On the internal network, select the internal or high availability VLAN that is associated with an internal interface or trunk.
   - On the external network, select the external VLAN that is associated with an external interface or trunk.
7. Use the default values for all remaining settings.
8. Click **Finished**.
   The screen refreshes, and displays the new self IP address.

The BIG-IP system can now send and receive TCP/IP traffic through the specified VLAN.

Creating a local traffic pool for application security

You can use a local traffic pool with Application Security Manager™ system to forward traffic to the appropriate resources.

Note: *You can optionally create a pool as part of creating a security policy using the Deployment wizard.*

---

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. In the Resources area, for the **New Members** setting, add to the pool the application servers that host the web application:
   a) Type an IP address in the **Address** field.
   b) In the **Service Port** field, type a port number (for example, type `80` for the HTTP service), or select a service name from the list.
   c) Click **Add**.
5. Click **Finished**.

The BIG-IP® system configuration now includes a local traffic pool containing the resources that you want to protect using Application Security Manager™.

Creating a virtual server

You can create a virtual server on the BIG-IP® system, and this is where clients send application requests. The *virtual server* manages the network resources for the web application that you are securing with a security policy.

Note: *You can optionally create a virtual server as part of creating a security policy.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.

The New Virtual Server screen opens.

3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type an address, as appropriate for your network.

   The supported format is address/prefix, where the prefix length is in bits. For example, an IPv4 address/prefix is `10.0.0.1` or `10.0.0.0/24`, and an IPv6 address/prefix is `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`. When you use an IPv4 address without specifying a prefix, the BIG-IP® system automatically uses a `/32` prefix.
5. In the **Service Port** field, type `80`, or select **HTTP** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.

   Note that this step is required.
8. From the **Source Address Translation** list, select **Auto Map**.
9. From the **Default Pool** list, select the pool that is configured for application security.
10. Click **Finished**.

About additional networking configuration

Depending on your network environment, you may need to configure the following additional networking features on the BIG-IP® system before you start creating security policies.

- DNS
- SMTP
- NTP
- Routes
- Packet filters
- Spanning tree
- Trunks
- ARP
- Redundant systems

Several Application Security features require that the DNS server is on the DNS lookup server list (**System** > **Configuration** > **Device** > **DNS**). For example, integrating vulnerability assessment tools, web scraping mitigation, and external anti-virus protection usually require you to configure DNS servers on the BIG-IP system.

Creating a Security Policy Automatically

Deployment scenarios when creating security policies

The Deployment wizard provides several different scenarios for creating and deploying security policies. Before you start creating a security policy, review the descriptions of each deployment scenario to help you decide which one is most appropriate for your organization.

Deployment scenario	Description
Create a security policy automatically (recommended)	Develops a security policy for a web application by examining traffic. In this scenario, the Real Traffic Policy Builder® automatically creates the security policy based on statistical analysis of the traffic and the intended behavior of the application. The system stabilizes and enforces the security policy when it processes sufficient traffic over a period of time. You have the option of modifying the policy manually, as well, to speed up policy creation.
Create a security policy manually or use templates (advanced)	Uses rapid deployment or an application-ready security policy (pre-configured template) to develop a security policy, or lets you develop a policy manually. The system creates a basic security policy that you can review and fine-tune. When the security policy includes all the protections that you need, and does not produce any false positives, you can enforce the security policy.
Create a security policy for XML and web services manually	Develops a security policy to protect web services or XML applications, such as those that use a WSDL or XML schema document. The system creates the security policy based on your configurations, and provides additional learning suggestions that you can review and fine-tune. When the security policy includes all the protections that you need, and does not produce any false positives, you can enforce the security policy.
Create a security policy using third party vulnerability assessment tool output	Creates a security policy based on integrating the output from a vulnerability assessment tool, such as WhiteHat Sentinel, IBM® AppScan®, Cenzic® Hailstorm®, Qualys, Quotium Seeker, HP WebInspect, or a generic scanner if using another tool. Based on the results from an imported vulnerability report, Application Security Manager™ creates a policy that automatically mitigates the vulnerabilities on your web site. You can also review and fine-tune the policy. When the security policy includes all the protections that you need and does not produce any false positives, you can enforce the security policy.

Overview: Automatic policy building

You can use the Application Security Manager™ to help you build a security policy that is tailored to your environment. The automatic policy building tool is called the Real Traffic Policy Builder®. The Real Traffic Policy Builder (referred to simply as the Policy Builder) adds suggestions for creating a security policy based on settings that you configure using the Deployment wizard, and the characteristics of the traffic going to and from the web application that the system is protecting. If using automatic learning, the system implements the learning suggestions and automatically builds the policy when sufficient traffic and time

has passed. If using manual learning, you can review the suggestions and develop the policy adding the policy elements and features you want.

Task summary

Creating a security policy automatically
Reviewing learning suggestions
Reviewing outstanding security policy tasks

Creating a security policy automatically

Before you can create a security policy, you must perform the minimal system configuration tasks including defining a VLAN, a self IP address, and other tasks required according to the needs of your networking environment.

Application Security Manager™ can automatically create a security policy that is tailored to secure your web application.

1. On the Main tab, click **Security** > **Application Security** > **Security Policies**.
   The Active Policies screen opens.
2. Click the **Create** button.
   The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.
3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.
   - To secure an existing virtual server that has no security policy associated with it, select **Existing Virtual Server** and click **Next**.
   - To create a new virtual server and pool with basic configuration settings, select **New Virtual Server** and click **Next**.
   - To create an active but unused security policy, select **Do not associate with Virtual Server** and click **Next**. No traffic will go through this security policy until you associate it with a virtual server. The Policy Builder cannot begin automatically creating a policy until traffic is going to ASM through the virtual server.

   The virtual server represents the web application you want to protect.

   The Configure Local Traffic Settings screen opens if you are adding a virtual server. Otherwise, the Select Deployment Scenario screen opens.
4. If you are adding a virtual server, configure the new or existing virtual server, and click **Next**.
   - If creating a new virtual server, specify the protocol, virtual server name, virtual server destination address and port, pool member IP address and port, and the logging profile.
   - If using an existing virtual server, it must have an HTTP profile and cannot be associated with a local traffic policy. Specify the protocol and virtual server.
   - If you selected **Do not associate with Virtual Server**, you will have to manually associate the security policy with a virtual server at a later time. On the policy properties screen, you need to specify a name for the security policy.

   The Select Deployment Scenario screen opens.
5. For **Deployment Scenario**, select **Create a security policy automatically** and click **Next**.
   The Configure Security Policy Properties screen opens.
6. If not associating a virtual server, in the **Security Policy Name** field, type a name for the policy.
7. From the **Application Language** list, select the language encoding of the application, or use **Auto detect** and let the system detect the language.

Important: *You cannot change this setting after you have created the security policy.*

8. If the application is not case-sensitive, clear the **Security Policy is case sensitive** check box. Otherwise, leave it selected.

Important: *You cannot change this setting after you have created the security policy.*

9. If you do not want the security policy to distinguish between HTTP and HTTPS URLs, clear the **Differentiate between HTTP and HTTPS URLs** check box. Otherwise, leave it selected.
10. Click **Next**.
The Configure Attack Signatures screen opens.
11. To configure attack signatures, move the systems used by your web application from the **Available Systems** list into the **Assigned Systems** list.
The system adds the attack signatures needed to protect the selected systems.
12. For the **Signature Staging** setting, verify that the default option **Enabled** is selected.

Note: *Because the Real Traffic Policy Builder® begins building the security policy in Blocking mode, you can keep signature staging enabled so you can check whether legitimate traffic is being stopped to reduce the chance of false positives.*

New and updated attack signatures remain in staging for 7 days, and are recorded but not enforced (according to the learn, alarm, and block flags in the attack signatures configuration) during that time.

13. Click **Next**.
The Configure Automatic Policy Building screen opens.
14. For **Policy Type**, select an option to determine the security features to include in the policy.

Option	Description
Fundamental	Creates a security policy enforcing HTTP protocol compliance, evasion techniques, explicit file types (including length checks), explicit parameters in selective mode at the global level, attack signatures, the violation Request Length Exceeds Defined Buffer Size, host names, header lengths, cookie lengths, the violation Failed to Convert Character, and learn explicit redirection domains.
Enhanced	Creates a security policy with all the elements of the Fundamental policy type; also checks for explicit URLs in selective mode plus meta characters, explicit parameter length checks in selective mode at the global level, methods, explicit cookies, and content profiles. If tracking user login sessions or using brute force protection, this is the recommended policy type.
Comprehensive	Creates a security policy with all the elements of the Enhanced policy type; also checks for explicit URLs and meta characters, explicit parameters and lengths at the URL level, parameter meta characters, and dynamic parameters.

A bulleted list on the screen describes which security features are included in each type.

15. For the **Policy Builder Learning Speed** setting, select how fast to generate suggestions for the policy.

Option	Description
Fast	Use if your application supports a small number of requests from a small number of sessions; for example, useful for web sites with less traffic. Policy Builder requires fewer unique traffic samples to make decisions in Automatic Learning Mode, or to reach a high learning score. However, choosing this option may present a greater chance of adding false entities to the security policy.
Medium	Use if your application supports a medium number of requests, or if you are not sure about the amount of traffic on the application web site. This is the default setting.

Option	Description
Slow	Use if your application supports a large number of requests from many sessions; for example, useful for web sites with lots of traffic. Policy Builder requires a large amount of unique traffic samples to make decisions in Automatic Learning Mode, or to reach a high learning score. This option creates the most accurate security policy, but it takes Policy Builder longer to collect the statistics.

Based on the option you select, the system sets greater or lesser values for the number of different user sessions, different IP addresses, and length of time before it adds suggestions to the security policy and if you are using automatic learning, enforces the elements.

16. For **Trusted IP Addresses**, select which IP addresses to consider safe:

Option	Description
All	Specifies that the policy trusts all IP addresses. This option is recommended for traffic in a corporate lab or preproduction environment where all of the traffic is trusted. The policy is created faster when you select this option.
Address List	Specifies networks to consider safe. Fill in the **IP Address** and **Netmask** fields, then click **Add**. This option is typically used in a production environment where traffic could come from untrusted sources. The IP Address can be either an IPv4 or an IPv6 address.

If you leave the trusted IP address list empty, the system treats all traffic as untrusted. In general, it takes more untrusted traffic, from different IP addresses, over a longer period of time to build a security policy.

17. If you want to display a response page when an AJAX request does not adhere to the security policy, select the **AJAX blocking response behavior** check box.
18. Click **Next**.
    The Security Policy Configuration Summary opens where you can review the settings to be sure they are correct.
19. Click **Finish** to create the security policy.
    The Automatic Policy Building Status screen opens where you can view the current state of the security policy.

ASM™ creates the virtual server with an HTTP profile (or associates an existing one), and on the Security tab, **Application Security Policy** is enabled and associated with the security policy you created. A local traffic policy is also created and by default sends all traffic for the virtual server to ASM. The Policy Builder automatically begins examining the traffic to the web application and making suggestions for building the security policy (unless you did not associate a virtual server). The system sets the enforcement mode of the security policy to Blocking, but it does not block requests until the Policy Builder processes sufficient traffic, adds elements to the security policy, and enforces the elements.

Tip: *This is a good point at which to test that you can access the application being protected by the security policy and check that traffic is being processed by the BIG-IP® system.*

How the security policy is built

When you finish running the Deployment wizard, you have created a basic security policy to protect your web application. The Real Traffic Policy Builder® starts examining the application traffic, and fine-tunes the security policy using the guidelines you configured.

The Policy Builder builds the security policy as follows:

- Adds policy elements and updates their attributes when ASM sees enough traffic from various users

- Examines application content and creates XML or JSON profiles as needed (if the policy includes JSON/XML payload detection)
- Configures attack signatures in the security policy
- Stabilizes the security policy when sufficient sessions over a period of time include the same elements
- Includes new elements if the site changes

The Policy Builder automatically discovers and populates the security policy with the policy elements (such as file types, URLs, parameters, and cookies). On the Policy Building screens, you can monitor general policy building progress, review learning suggestions and deal with those you must handle manually, and see the number of elements that have been included in the policy.

Automatic policy building characteristics

If you create a security policy with the Learning Mode set to Automatic, the Real Traffic Policy Builder® does automatic policy building. This is how it works:

- The security policy starts out loose, allowing traffic, then the Policy Builder adds policy elements based on evaluating the traffic.
- By examining the traffic, the Policy Builder makes learning suggestions that you can review on the Traffic Learning screen to see the suggested additions to the security policy. You can select and examine each suggestion if you want to learn more about it. If using automatic policy building, you can still change the policy manually, or leave it up to the system to make the changes.
- The system sets the enforcement mode of the security policy to **Blocking**, but it does not block requests until the Policy Builder sees sufficient traffic, adds elements to the security policy, and enforces the elements.
- The system holds attack signatures in staging for 7 days (by default, you can adjust the length of staging): the system checks, but does not block traffic during the staging period. If a request causes an attack signature violation, the system disables the attack signature for the particular element (parameter, JSON or XML profile, or security policy). After the staging period is over, the Policy Builder can remove all attack signatures from staging if enough traffic from different sessions and different IP addresses was processed. The security policy enforces the enabled signatures and blocks traffic that causes a signature violation.
- The system enforces elements in the security policy when it has processed sufficient traffic and sessions over enough time, from different IP addresses, to determine the legitimacy of the file types, URLs, parameters, cookies, methods, and so on.
- The security policy stabilizes.
- If the web site for the application changes, the Policy Builder initially loosens the security policy then adds policy elements to the security policy, updates the attributes of policy elements, puts the added elements in staging, and enforces the new elements when traffic and time thresholds are met.

This is the process describing what happens during the automatic policy building process. You can always control the way the security policy works by making changes manually and configuring additional layers of security based on the unique needs of your environment.

Reviewing learning suggestions

After you create a security policy, the system provides learning suggestions concerning additions to the security policy based on the traffic that is accessing the application. For example, you can have users or testers browse the web application. By analyzing the traffic to and from the application, Application Security Manager™ generates learning suggestions or ways to fine-tune the security policy to better suit the traffic and secure the application.

Note: *This task is primarily for building a security policy manually. If you are using the automatic learning mode, this task applies to resolving suggestions that require manual intervention, or for speeding up the enforcement of policy elements.*

1. On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Traffic Learning**.
   The Traffic Learning screen opens, and lists suggestions based on traffic patterns and violations that the system has detected.
2. If you want to change the order in which the suggestions are listed, or refine what is included in the list, use the filters at the top of the column.

   You can also list the suggestions by average violation rating of all matching requests, first occurrence, last occurrence, matched entity name, or use the search filter to display specific types of suggestions that you are interested in.

   By default, the suggestions that have the highest learning score (those closest to being ready to be enforced) are listed first. Suggestions have higher learning scores if that traffic has met the conditions in the policy, if it originates from many sources, if it is unlikely to be a violation, or if the traffic comes from a trusted IP address. They may also be suggestions to add an entity the system learns, for example, a new file type, URL, or parameter.
3. On the Traffic Learning screen, review each learning suggestion.
   a) Select a learning suggestion.
   Information is displayed about the action the system will take if you accept the suggestion, and what caused the suggestion.
   b) You can learn more about the suggestion by looking at the action, the number of samples it is based on, the violations caused and their violation ratings, and if needed, by examining samples of the requests that caused the suggestion.
   c) With a request selected on the left, you can view data about the request on the right, including any violations it generated, the contents of the request itself, and the response (if any). Note that some requests may contain violations related to different suggestions.

      By examining the requests that caused a suggestion, you can determine whether it should be accepted.
   d) To add comments about the suggestion and the cause, click the Add Comment icon and type the comments.
4. Decide how to respond to the suggestion. You can start with the suggestions with the highest learning scores, or those which you know to be valid for the application. These are the options.

Option	What happens
Accept Suggestion	The system modifies the policy by taking the suggested action, such as adding an entity that is legitimate. If the entity that triggered the suggestion can be placed in staging (file types, URLs, parameters, cookies, or redirection domains), clicking **Accept Suggestion** displays a second option, **Accept suggestion** and enable staging on Matched <<entity>>. Click this option to accept the suggestion and place the matched entity in staging.
Delete Suggestion	The system removes the learning suggestion, but the suggestion reoccurs if new requests cause it. The learning score of the suggestion starts over from zero in that case.
Ignore Suggestion	The system does not change the policy and stops showing this suggestion on the Traffic Learning screen now and in the future. You can view ignored suggestions by filtering by status ignored.
Leave the suggestion	You can read the suggestions and wait to handle them until more traffic has passed through, or until you get more information. The suggestion remains in the list and no changes are made to the policy.

Note: *If you are working in automatic learning mode, when the learning score reaches 100%, the system accepts most of the suggestions, or you can accept suggestions manually at any time. If you are using manual learning, when the learning score reaches 100% (or before that if you know the suggestions are valid), you need to accept the suggestions manually.*

If you know that a suggestion is valid, you can accept it at any time even before the learning score reaches 100%. The ones that reach 100% have met all the conditions so that they are probably legitimate entities.

5. To put the security policy changes into effect immediately, click **Apply Policy**.

By default, a security policy is put into an enforcement readiness period for seven days. During that time, you can examine learning suggestions and adjust the security policy without blocking traffic. The security policy then includes elements unique to your web application.

It is a good idea to periodically review the learning suggestions on the Traffic Learning screen to determine whether the violations are legitimate and caused by an attack, or if they are false positives that indicate a need to update the security policy. Typically, a wide recurrence of violations at some place in the policy (with a low violation rating and a high learning score) indicates that they might be false positives, and hence the policy should be changed so that they will not be triggered anymore. If the violations seem to indicate true attacks (for example, they have a high violation rating), the policy should stay as is, and you can review the violations that it triggered.

Learning suggestions you must handle manually

Some learning suggestions must be resolved manually even if you are using the Automatic Learning Mode to create a security policy. Suggestions typically require manual intervention if they involve changing an attribute that was manually and deliberately set in the policy, such as a disallowed geolocation or a session ID in a URL. The system does not change the policy unless you accept the suggestion manually.

You can easily see the suggestions that you need to resolve manually because they are marked with an icon on the Traffic Learning screen as shown in the figure. You can also use the advanced filter to view the suggestions the have Learning Mode set to Manual, and this would list the suggestions you need to resolve.

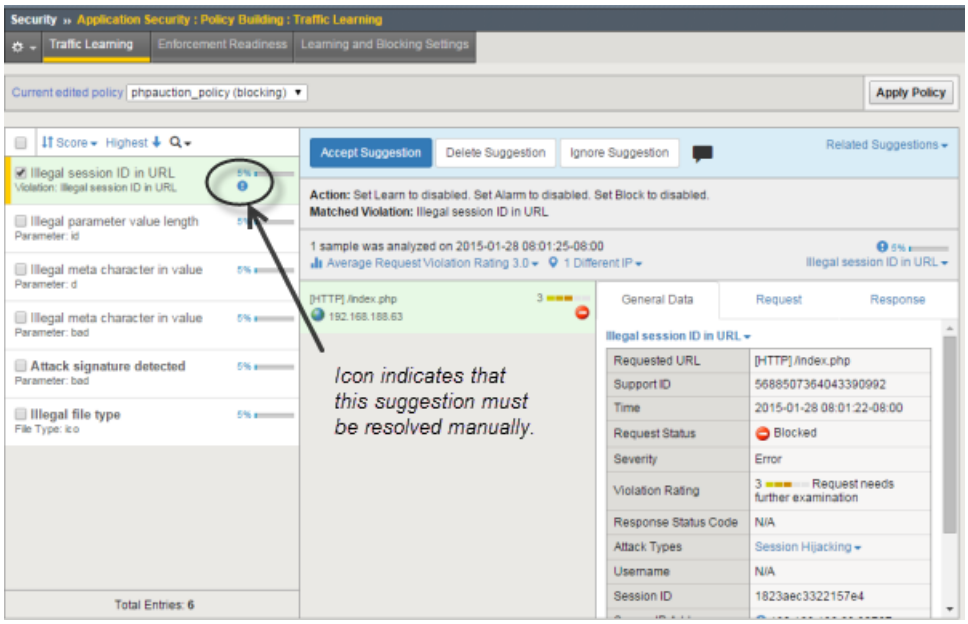

Figure 1: Suggestions that must be resolved manually

If you are using the Manual Learning Mode, you must resolve all of the suggestions manually.

Reviewing outstanding security policy tasks

You can display a security policy summary including a list of action items. To simplify your work, the system reminds you of required or recommended actions, such as, outstanding configuration and maintenance tasks, and provides links to setup and reporting screens.

1. On the Main tab, click **Security** > **Overview** > **Application** > **Action Items**.
   The Action Items screen opens.
2. Examine the Action Items screen for information about recommended tasks that you need to complete.
   - Review the Suggested Action Items area, which lists system tasks and security policy tasks that should be completed.
   - Click the links to go to the screen where you can perform the recommended action items.
   - Click any security policy task link to open the Summary screen, where you can view and resolve the tasks for that security policy.
3. In the Quick Links area, click **Policies Summary**.
   The Policies Summary opens and shows a summary of all the active security policies on the system.
4. In the Policy Details area, click the links to display details about a security policy.
   - Click the Policy Name to view or edit policy properties.
   - Click a security policy row (not on the policy name) to view Suggested Action Items, Quick Links, and how Policy Builder is operating for that security policy (whether automatically, manually, or disabled).
   - Click a number in the File Types, URLs, Parameters, or Cookies column of a security policy to see details about these policy elements.
   - Click the status in the Real Traffic Policy Builder® column to view the automatic security policy building status.

If you keep an eye on the summary screens, the system lists the tasks that you should complete to ensure that the security policy is configured completely.

About additional application security protections

The Application Security Manager™ provides additional security protections that you can manually configure for a security policy.

Feature	Description and Location
DoS attack prevention	Prevents Denial of Service (DoS) attacks based on latency and/or transaction rates (also using geolocation, CAPTCHA challenge, heavy URL detection, proactive web scraping detection, and blacklisting). Click **Security** > **DoS Protection**. You need to create a DoS profile with Application Security enabled to configure Layer 7 DoS protection.
IP Address Intelligence	Logs and blocks attacks from IP addresses that are in the IP Address Intelligence Database and are considered to have a bad reputation. Click **Security** > **Application Security** > **IP Addresses** > **IP Address Intelligence**.

Feature	Description and Location
Web scraping detection	Mitigates web scraping (web data extraction) on web sites by attempting to determine whether a web client source is human. Click **Security** > **Application Security** > **Anomaly Detection** > **Web Scraping**.
CSRF protection	Prevents cross-site request forgery (CSRF) where a user is forced to perform unwanted actions on a web application where the user is currently authenticated. Click **Security** > **Application Security** > **CSRF Protection**.
Sensitive data masking	Protects sensitive data in responses such as a credit card number, U.S. Social Security number, or custom pattern. Click **Security** > **Application Security** > **Data Guard**. Create sensitive parameters if needed (they are also masked); click **Security** > **Application Security** > **Parameters** > **Sensitive Parameters**. As an additional protection, set the **Mask Credit Card Numbers in Request Log** option in the policy properties.
Anti-virus protection through an ICAP server	Configures the system as an Internet Content Adaptation Protocol (ICAP) client so that an external ICAP server can inspect HTTP file uploads for viruses before releasing the content to the web server. To set up the ICAP server, click **Security** > **Options** > **Application Security** > **Integrated Services** > **Anti-Virus Protection**. To set the blocking settings (alarm and/or block) of the Virus Detected violation, click **Security** > **Application Security** > **Policy Building** > **Learning and Blocking Settings**. Also check that the values of the system variables `icap_uri` and `virus_header_name` correspond to the ICAP server (**Security** > **Options** > **Application Security** > **Advanced Configuration** > **System Variables**).

Using Vulnerability Assessment Tools for a Security Policy

Overview: Vulnerability assessment policy building

Application Security Manager™ (ASM) integrates with current version of services, such as IBM® AppScan®, Trustwave ® App Scanner, Qualys, Quotium Seeker®, HP WebInspect, and WhiteHat Sentinel, that perform vulnerability assessments of web applications. ASM™ also integrates with other vulnerability assessment tools by means of a generic scanner. Vulnerability assessment services identify, classify, and report potential security holes or weaknesses in the code of your web site.

You can use the vulnerability assessment deployment scenario to create a baseline security policy that is integrated with a vulnerability assessment tool. By using vulnerability assessment tool output, the system suggests updates to the security policy that can protect against the vulnerabilities that the tool found. You can choose which of the vulnerabilities you want the security policy to handle, retest to be sure that the security policy protects against the vulnerabilities, then enforce the security policy when you are ready.

If you have an existing security policy that was created using a different deployment scenario, you can also incorporate use of a vulnerability assessment tool with that policy.

Task summary

Creating a security policy using vulnerability assessment tool output
Associating a vulnerability assessment tool with an existing security policy
Importing vulnerability assessment tool output
Resolving vulnerabilities
Reviewing learning suggestions
Enforcing a security policy

About using Policy Builder with scanner policies

When you develop a security policy using third party vulnerability assessment tool or scanner output, you can set the Learning Mode to automatic or manual, which enables the Real Traffic Policy Builder®. In this case, the Policy Builder makes suggestions for what to add to the policy based on what it learns from your web application traffic, and uses logic to prevent false positives. The suggestions are either automatically learned by the system or they must be manually learned by an administrator depending on the learning mode you selected.

In addition, you select an external scanning tool such as WhiteHat Sentinel, Qualys Web Application Scanning, IBM AppScan, Trustwave App Scanner (Cenzic), Quotium Seeker, or others to build your policy to protect against the vulnerabilities they have found. You import the vulnerabilities detected by the scanner, and choose whether or not to update the security policy for each problem found.

It is possible that in some cases Policy Builder decisions might conflict with and override the scanner results. Here are some examples:

- The Policy Builder might remove a URL that the scanner added to the list of CSRF-protected URLs.
- The Policy Builder might allow file upload of executable files on a parameter after the scanner disallowed it.
- The Policy Builder might add an allowed method after the scanner disallowed it.

- The Policy Builder might disable attack signatures on parameters, cookies, and at the policy level after the scanner enabled them.

You can also select disabled for the Learning Mode, which disables the Policy Builder so that it does not make learning suggestions. In this case, you can manually build the security policy or just use scanner output to build it. You can adjust the Learning Mode after creating the policy on the Policy Building Learning and Blocking Settings screen.

About exporting results from scanners

Application Security Manager™ (ASM) integrates with the current version of many vulnerability assessment tools (also called *scanners*). ASM uses the exported results from the scanners to address potential vulnerabilities or security risks concerning your application web site. Using a scanner external to ASM, you perform a vulnerability assessment of the web site, then export the results in standard XML format. Then later, using ASM, you import the results into the security policy being developed to protect the application.

Here are brief instructions on how to export the scan results from several of the vulnerability assessment tools.

Tool	To export scan results from the tool
Trustwave App Scanner	Right click **Assessment Run** > **Export Assessment Run To** > **Standard XML**.
HP WebInspect	Click **File** > **Export** > **Scan Details**. Export the Full details in XML format.
IBM AppScan	Click **File** > **Export** > **Scan results as XML**.
Qualys	Click **Web Applications** > **View Report** > **Download** > **XML**.
Quotium Seeker	Click **Project** > **Export Results**, select **F5 BIG-IP ASM** format. In ASM, use **Generic Scanner** to configure.
WhiteHat Sentinel	Retrieves reports by connecting directly to ASM using a web service.

You can use additional vulnerability assessment tools as long as you have the results in standard XML output.

Creating a security policy using vulnerability assessment tool output

In order to integrate vulnerability assessment tool output with Application Security Manager™ (ASM), you need recent scanner output for the web application you want to protect in the form of an XML file (except if using WhiteHat or Trustwave tools which allow you to download output directly).

Before you can create a security policy using ASM™, you need to complete the basic BIG-IP® system configuration tasks including creating a VLAN, a self IP address, and other tasks, according to the needs of your networking environment.

You can create a baseline security policy to protect against the potential problems that a vulnerability assessment tool scan finds.

1. On the Main tab, click **Security** > **Application Security** > **Security Policies**.
   The Active Policies screen opens.
2. Click the **Create** button.
   The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.
3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.

- To secure an existing virtual server that has no security policy associated with it, select **Existing Virtual Server** and click **Next**.
- To create a new virtual server and pool with basic configuration settings, select **New Virtual Server** and click **Next**.
- To create an active but unused security policy, select **Do not associate with Virtual Server** and click **Next**. No traffic will go through this security policy until you associate it with a virtual server. The Policy Builder cannot begin automatically creating a policy until traffic is going to ASM through the virtual server.

The virtual server represents the web application you want to protect.

The Configure Local Traffic Settings screen opens if you are adding a virtual server. Otherwise, the Select Deployment Scenario screen opens.

4. If you are adding a virtual server, configure the new or existing virtual server, and click **Next**.
   - If creating a new virtual server, specify the protocol, virtual server name, virtual server destination address and port, pool member IP address and port, and the logging profile.
   - If using an existing virtual server, it must have an HTTP profile and cannot be associated with a local traffic policy. Specify the protocol and virtual server.
   - If you selected **Do not associate with Virtual Server**, you will have to manually associate the security policy with a virtual server at a later time. On the policy properties screen, you need to specify a name for the security policy.

   The Select Deployment Scenario screen opens.
5. For **Deployment Scenario**, select **Create a security policy using third party vulnerability assessment tool output** and click **Next**.
6. If not associating a virtual server, in the **Security Policy Name** field, type a name for the policy.
7. From the **Application Language** list, select the language encoding of the application, then click **Next**.

   Important: *You cannot change this setting after you have created the security policy.*

8. For **Enforcement Mode** specify whether or not the system blocks traffic that violates the security policy.
   - Leave the value set to **Transparent**, the default value, if you want to review and fine-tune the security policy before placing it in Blocking mode.
   - If you want the system to enforce the security policy immediately, select **Blocking**.
9. If the application is case-sensitive, select the **Security Policy is case sensitive** check box. Otherwise, leave it cleared.

   Important: *You cannot change this setting after you have created the security policy.*

10. If you do not want the security policy to distinguish between HTTP and HTTPS URLs, clear the **Differentiate between HTTP and HTTPS URLs** check box. Otherwise, leave it selected.
11. Click **Next**.
    The Vulnerability Assessments Settings screen opens.
12. From the **Vulnerability Assessment Tool** list, select the vulnerability assessment tool that you use to scan your web application for problems.

    Tip: *If your tool is not listed, select* ***Generic Scanner****.*

13. In the **Configure exceptions for the scanner IP Address** setting, specify any IP addresses that you want the security policy to allow (for example, the IP address of the vulnerability assessment tool), and how to deal with them.
    a) Type the IP address and netmask of the vulnerability assessment tool.

You can add `%n` after an IP address to specify a route domain, where `n` is the route domain identification number.

b) Select the appropriate check boxes for learning suggestions, logging, and blocking traffic from this IP address.

14. For **Learning Mode**, select how you want the Policy Builder to build the security policy.

- If you want the Policy Builder to automatically build the security policy, select **Automatic**.
- If you want the Policy Builder to make suggestions and manually decide what to include, select **Manual**.
- If you do not want the system to suggest policy changes, select **Disabled**.

Note: *In some cases, running the Policy Builder may overwrite some of the security policy changes suggested by the vulnerability assessment tool. For example, to prevent false positives, the Policy Builder might adjust some of the entities in the security policy based on examining the traffic.*

If you select **Automatic** or **Manual**, the system examines traffic and makes suggestions about how to tighten the security policy. If you are using automatic learning, the system enforces the suggestions when it is reasonable to do so. If you are using manual learning, you need to examine the changes and accept, delete, or ignore them on the Traffic Learning screen. If you disabled this option, the system does not do any learning for this policy, it makes no suggestions, and the **Learn** flag for all violations becomes inactive.

15. Click **Next**.
The Security Policy Configuration Summary screen opens.

16. Review the settings for the security policy. When you are satisfied with the security policy configuration, click **Finish**.
The system creates the security policy and opens the vulnerability assessment settings screen specific to the tool you are using. For most tools, you can import the results of a vulnerabilities scan in an XML file.

17. If using the WhiteHat Sentinel, you can connect with these tools on the Vulnerabilities Assessments Settings screen that opens. If you have an account, click **Connect**.

If you do not have an account, you can open a trial account and run a free scan to find and resolve vulnerabilities.

18. If using the Generic Scanner, click **Download Generic Schema** to download the `generic_scanner.xsd` file.

The system creates a baseline security policy for your web application, but it does not yet protect against the vulnerabilities or enforce the policy. The policy type is Vulnerability Assessment.

Next, you need to import, review, and resolve vulnerabilities on the Vulnerabilities screen so that the security policy protects against them.

Associating a vulnerability assessment tool with an existing security policy

In order to integrate vulnerability assessment tool output with Application Security Manager™ (ASM), you need recent scanner output for the web application you want to protect in the form of a standard XML file.

If you have already created a security policy that does not use vulnerability assessment, you can import vulnerability assessment tool output into that security policy.

1. On the Main tab, click **Security** > **Application Security** > **Vulnerability Assessments** > **Settings**.
The Vulnerabilities Assessments: Settings screen opens.

2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. From the **Vulnerability Assessment Tool** list, select the vulnerability assessment tool that you use to scan your web application for problems, or select **Generic Scanner** if your tool is not listed.

   Important: *After you import vulnerabilities, you cannot change the vulnerability assessment tool you are using for a security policy.*

   A popup screen informs you that the Policy Type will be changed to Vulnerability Assessment and asks if you want to continue.
4. To associate the selected vulnerability assessment tool with the security policy, click **OK**.
5. If using the Generic Scanner, click **Download Generic Schema** to download the `generic_scanner.xsd` file.
6. In the editing context area, click **Apply Policy** to immediately put the changes into effect.

The system associates the vulnerability assessment tool with the security policy.

Next, you need to import, review, and resolve vulnerabilities on the Vulnerabilities screen so that the security policy protects against them.

Importing vulnerability assessment tool output

In order to import vulnerability assessment tool output into a security policy, you need to have configured the policy to use a vulnerability assessment tool. You also need recent scanner output (in standard XML format) for the web application you want to protect.

You can import vulnerability assessment tool output into a security policy.

1. On the Main tab, click **Security** > **Application Security** > **Vulnerability Assessments**.
   The Vulnerabilities screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. To import the recent scanner output from the vulnerabilities tool, click **Import**.
4. In the import popup screen, for the **Import previously saved vulnerabilities file** field, specify the XML file output from the vulnerabilities assessment tool that you associated with the security policy, then click **Import**.

   Some vulnerability assessment tools (such as WhiteHat) provide additional settings allow you to connect to an existing account, create a trial account, and request a new scan. Refer to the online help for details about the settings.

   The system verifies the file and if vulnerabilities for more than one domain are discovered, on the popup screen you can select the domain names for which to include the vulnerabilities.

The system imports the vulnerabilities that the vulnerabilities assessment tool found on your web application.

Next, you need to review and resolve vulnerabilities on the Vulnerabilities screen so that the security policy protects against them.

Resolving vulnerabilities

Before you can resolve vulnerabilities for a security policy, the security policy must be associated with a vulnerability assessment tool, and have the vulnerabilities file imported to it.

When you resolve vulnerabilities discovered by a scanner, the security policy protects against them. Application Security Manager™ (ASM) can resolve some vulnerabilities automatically. Others require some manual intervention on your part, and ASM™ provides guidance on what to do.

1. On the Main tab, click **Security** > **Application Security** > **Vulnerability Assessments**.
   The Vulnerabilities screen opens and lists the vulnerabilities that the vulnerability assessment scan discovered.
2. In the Vulnerabilities Found and Verified area, you can filter the vulnerabilities that are displayed using the **View** and **Vulnerabilities with** lists.

View option	Description
All	Displays all vulnerabilities found by the scanner.
Resolvable	Displays all vulnerabilities that are resolvable either automatically or manually.
Resolvable (Automatically)	Displays vulnerabilities that ASM can resolve.
Resolvable (Manually)	Displays vulnerabilities that can be resolved with some manual intervention.
Not Resolvable	Displays vulnerabilities that are not resolvable in any straightforward way.

Vulnerabilities with option	Description
Any	Displays vulnerabilities in any state.
Ignored	Displays vulnerabilities that you decided to ignore by selecting and clicking **Ignore**.
Mitigated	Displays vulnerabilities that ASM has mitigated, or those which have been fixed and marked as mitigated..
Pending	Displays vulnerabilities that need to be dealt with.
Mitigated (In Staging)	Displays vulnerabilities that were resolved by adding a parameter or cookie (in staging) to the security policy.

3. Review the vulnerabilities that the assessment tool has detected and verified.
   a) Click a row in the table to display details about the vulnerability.
      Below the Vulnerabilities Found table, a list of the specific vulnerabilities is displayed.
   b) To add notes about the vulnerability, click the pencil icon in the ASM Status column.
      The Vulnerability Notes popup opens where you can add notes.
4. For the vulnerabilities that are shown as **Resolvable (Automatically)**, select the vulnerabilities you want the system to resolve (or ignore), and click the appropriate button.

Option	Description
Resolve and Stage	Updates the security policy to protect against the vulnerability, and puts parameters in staging. Entities in staging do not cause violations, and this allows you to fine-tune their settings without causing false positives.
Resolve	Updates the security policy to protect against the vulnerability.
Ignore	Changes the ASM Status of the selected vulnerability from **Pending** to **Ignore**. If later you decide to protect against this vulnerability, you can select it and click **Cancel Ignore**.

   ASM reviews the prerequisites and then displays a list of the changes it will make to fix the vulnerability.
5. If you agree with the changes, click **Resolve**.

ASM modifies the security policy to protect against the vulnerabilities for which you clicked **Resolve** and ignores the rest. In the Vulnerabilities list, the ASM Status column for the vulnerability changes to Mitigated or Mitigated (In Staging), if appropriate.

6. For the vulnerabilities that are shown as **Resolvable (Manually)**, select the vulnerability you want to work on, and click the appropriate button.

Option	Description
Show Resolution	Opens a popup that describes the vulnerability and its possible impact, shows the steps required to manually fix the vulnerability, and describes any risks that might result from making the changes..
Change ASM Status to Mitigated	Changes the status of the vulnerability to say **Mitigated**. Recommended after you manually fix vulnerabilities.
Ignore	Changes the ASM Status of the selected vulnerability from **Pending** to **Ignore**. If later you decide to protect against this vulnerability, you can select it and click **Cancel Ignore**.

7. Click **Apply Policy** to save the changes to the security policy.
   The system updates the security policy to prevent the handled vulnerabilities from reoccurring.
8. If using WhiteHat Sentinel, select all of the vulnerabilities you dealt with and click **Retest** to have the WhiteHat Sentinel service verify that the vulnerability has been dealt with.

The security policy for your web application protects against the vulnerabilities that the vulnerability assessment tool discovered and which you resolved manually or automatically. The ASM Status of vulnerabilities that have been dealt with is set to **Mitigated**.

You can periodically rescan your system to check for additional vulnerabilities that need to be resolved.

Reviewing learning suggestions

After you create a security policy, the system provides learning suggestions concerning additions to the security policy based on the traffic that is accessing the application. For example, you can have users or testers browse the web application. By analyzing the traffic to and from the application, Application Security Manager™ generates learning suggestions or ways to fine-tune the security policy to better suit the traffic and secure the application.

Note: *This task is primarily for building a security policy manually. If you are using the automatic learning mode, this task applies to resolving suggestions that require manual intervention, or for speeding up the enforcement of policy elements.*

---

1. On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Traffic Learning**.
   The Traffic Learning screen opens, and lists suggestions based on traffic patterns and violations that the system has detected.
2. If you want to change the order in which the suggestions are listed, or refine what is included in the list, use the filters at the top of the column.

   You can also list the suggestions by average violation rating of all matching requests, first occurrence, last occurrence, matched entity name, or use the search filter to display specific types of suggestions that you are interested in.

   By default, the suggestions that have the highest learning score (those closest to being ready to be enforced) are listed first. Suggestions have higher learning scores if that traffic has met the conditions in the policy, if it originates from many sources, if it is unlikely to be a violation, or if the traffic comes from a trusted IP address. They may also be suggestions to add an entity the system learns, for example, a new file type, URL, or parameter.

3. On the Traffic Learning screen, review each learning suggestion.
   a) Select a learning suggestion.
   Information is displayed about the action the system will take if you accept the suggestion, and what caused the suggestion.
   b) You can learn more about the suggestion by looking at the action, the number of samples it is based on, the violations caused and their violation ratings, and if needed, by examining samples of the requests that caused the suggestion.
   c) With a request selected on the left, you can view data about the request on the right, including any violations it generated, the contents of the request itself, and the response (if any). Note that some requests may contain violations related to different suggestions.

      By examining the requests that caused a suggestion, you can determine whether it should be accepted.
   d) To add comments about the suggestion and the cause, click the Add Comment icon and type the comments.

4. Decide how to respond to the suggestion. You can start with the suggestions with the highest learning scores, or those which you know to be valid for the application. These are the options.

Option	What happens
Accept Suggestion	The system modifies the policy by taking the suggested action, such as adding an entity that is legitimate. If the entity that triggered the suggestion can be placed in staging (file types, URLs, parameters, cookies, or redirection domains), clicking **Accept Suggestion** displays a second option, **Accept suggestion** and enable staging on Matched <<entity>>. Click this option to accept the suggestion and place the matched entity in staging.
Delete Suggestion	The system removes the learning suggestion, but the suggestion reoccurs if new requests cause it. The learning score of the suggestion starts over from zero in that case.
Ignore Suggestion	The system does not change the policy and stops showing this suggestion on the Traffic Learning screen now and in the future. You can view ignored suggestions by filtering by status ignored.
Leave the suggestion	You can read the suggestions and wait to handle them until more traffic has passed through, or until you get more information. The suggestion remains in the list and no changes are made to the policy.

Note: *If you are working in automatic learning mode, when the learning score reaches 100%, the system accepts most of the suggestions, or you can accept suggestions manually at any time. If you are using manual learning, when the learning score reaches 100% (or before that if you know the suggestions are valid), you need to accept the suggestions manually.*

If you know that a suggestion is valid, you can accept it at any time even before the learning score reaches 100%. The ones that reach 100% have met all the conditions so that they are probably legitimate entities.

---

5. To put the security policy changes into effect immediately, click **Apply Policy**.

By default, a security policy is put into an enforcement readiness period for seven days. During that time, you can examine learning suggestions and adjust the security policy without blocking traffic. The security policy then includes elements unique to your web application.

It is a good idea to periodically review the learning suggestions on the Traffic Learning screen to determine whether the violations are legitimate and caused by an attack, or if they are false positives that indicate a need to update the security policy. Typically, a wide recurrence of violations at some place in the policy (with a low violation rating and a high learning score) indicates that they might be false positives, and hence

the policy should be changed so that they will not be triggered anymore. If the violations seem to indicate true attacks (for example, they have a high violation rating), the policy should stay as is, and you can review the violations that it triggered.

Learning suggestions you must handle manually

Some learning suggestions must be resolved manually even if you are using the Automatic Learning Mode to create a security policy. Suggestions typically require manual intervention if they involve changing an attribute that was manually and deliberately set in the policy, such as a disallowed geolocation or a session ID in a URL. The system does not change the policy unless you accept the suggestion manually.

You can easily see the suggestions that you need to resolve manually because they are marked with an icon on the Traffic Learning screen as shown in the figure. You can also use the advanced filter to view the suggestions the have Learning Mode set to Manual, and this would list the suggestions you need to resolve.

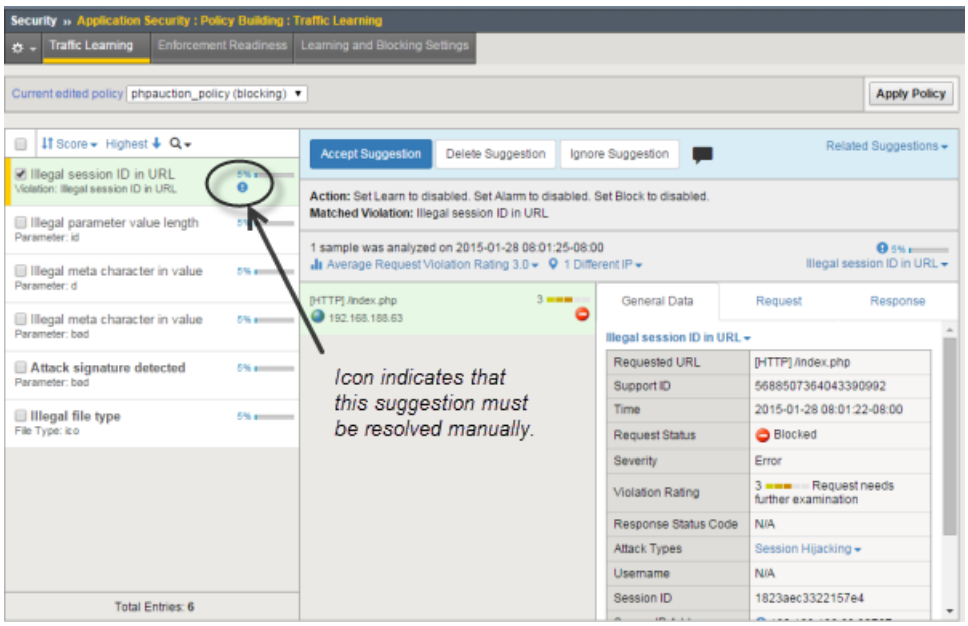

Figure 2: Suggestions that must be resolved manually

If you are using the Manual Learning Mode, you must resolve all of the suggestions manually.

Enforcing a security policy

You only need to enforce a security policy if it was created manually (not using automatic learning), and if it is operating in transparent mode. Traffic should be moving through Application Security Manager™, allowing users to access the web application for which you set up the security policy.

When you enforce a security policy, the system blocks requests that cause violations that are set to block.

1. On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Learning and Blocking Settings**.
   The Learning and Blocking Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For the **Enforcement Mode** setting, select **Blocking**.

4. Review each of the policy building settings so you understand how the security policy handles requests that cause the associated violations, and adjust if necessary. You need to expand most of the settings to see the violations.

   Tip: *To the right of Policy Building Settings, click* ***Blocking Settings*** *to see and adjust all of the violations at once.*

Option	What happens when selected
Learn	The system generates learning suggestions for requests that trigger the violation (except learning suggestions are not generated for requests that return HTTP responses with 400 or 404 status codes).
Alarm	When selected, the system marks requests that trigger the violation as illegal. The system also records illegal requests in the Charts screen, the system log (`/var/log/asm`), and possibly in local or remote logs (depending on the settings of the logging profile).
Block	The system blocks requests that trigger the violation when (1) the security policy is in the blocking enforcement mode, (2) a violation occurs, and (3) the entity is enforced. The system sends the blocking response page (containing a Support ID to identify the request) to the client.

5. Click **Save** to save your settings.
6. On the Main tab, click **Security** > **Application Security** > **Security Policies**.
   The Active Policies screen opens.
7. Click the name of the security policy you want to work on.
   The Policy Properties screen opens.
8. To change the number of days that the security policy entities and attack signatures remain in staging, change the value in the **Enforcement Readiness Period** field.

   The security policy does not block traffic during the Enforcement Readiness Period even if violations occur.

9. If you want to immediately block traffic that causes violations, you need to enforce entities that are ready to be enforced. This is one way to do this quickly:
   a) Set the **Enforcement Readiness Period** to `0`. (Not generally recommended. Use only if you want to speed up the process.)
   b) Click **Save**.
   c) On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Enforcement Readiness**.
   d) Click **Enforce Ready**.

   In most cases, it is better to use a longer **Enforcement Readiness Period**, such as the default of 7 days. The entities become ready to be enforced after that.

10. To put the security policy changes into effect immediately, click **Apply Policy**.
11. For a quick summary of system activity, look at the Overview screen (**Security** > **Overview** > **Application**).
    The Summary screen displays statistical information about Application Security traffic.

After the enforcement readiness period is over and the enforcement mode is set to blocking, the security policy no longer allows requests that cause violations set to block to reach the back-end resources. Instead, the security policy blocks the request, and sends the blocking response page to the client.

Using WhiteHat Sentinel for a Security Policy

Overview: Integrating WhiteHat Sentinel with ASM

Application Security Manager™ (ASM) integrates with WhiteHat Sentinel to perform vulnerability assessments of web applications. WhiteHat identifies, classifies, and reports potential security holes or weaknesses in the code of your web site.

You can use the vulnerability assessment deployment scenario to create a baseline security policy that is integrated with WhiteHat Sentinel. By using Sentinel scan output, the system suggests updates to the security policy that can protect against the vulnerabilities that WhiteHat Sentinel found. You can choose which of the vulnerabilities you want the security policy to handle, resolve them automatically or manually, retest to be sure that the security policy protects against the vulnerabilities, then enforce the security policy when you are ready.

Task summary

Creating a security policy integrated with WhiteHat Sentinel
Creating a vulnerability file
Resolving vulnerabilities when using WhiteHat Sentinel
Reviewing learning suggestions
Enforcing a security policy

Creating a security policy integrated with WhiteHat Sentinel

Before you can integrate WhiteHat Sentinel with Application Security Manager™ (ASM), you should have the following prerequisites:

- Up-to-date WhiteHat Sentinel subscription and valid login credentials (`sentinel.whitehatsec.com`)
- WhiteHat Sentinel Web API key for your account
- Site name (as defined in your WhiteHat account)
- Recent Sentinel scan of the web application you want to protect

If you do not have a WhiteHat account, you will have the opportunity to get a free assessment of your website from WhiteHat Sentinel.

The ASM™ system needs to be able to access the WhiteHat web site to download the results of the vulnerability scan and to perform retests after updating the security. If the BIG-IP® system does not have Internet access, you can run the vulnerability scan from a system that does have access, then save the results of the scan as an XML file on that system and import the vulnerabilities file manually onto the BIG-IP system.

You need to complete the basic BIG-IP system configuration tasks including creating a VLAN, a self IP address, and other tasks according to the needs of your networking environment. You also need to configure a DNS address (go to **System** > **Configuration** > **Device** > **DNS)**.

The WhiteHat Sentinel service assesses web applications for vulnerabilities. You can create a baseline security policy to protect against the potential problems that a Sentinel vulnerability assessment scan finds.

1. On the Main tab, click **Security** > **Application Security** > **Security Policies**.

The Active Policies screen opens.

2. Click the **Create** button.
   The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.
3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.
   - To secure an existing virtual server that has no security policy associated with it, select **Existing Virtual Server** and click **Next**.
   - To create a new virtual server and pool with basic configuration settings, select **New Virtual Server** and click **Next**.
   - To create an active but unused security policy, select **Do not associate with Virtual Server** and click **Next**. No traffic will go through this security policy until you associate it with a virtual server. The Policy Builder cannot begin automatically creating a policy until traffic is going to ASM through the virtual server.

   The virtual server represents the web application you want to protect.

   The Configure Local Traffic Settings screen opens if you are adding a virtual server. Otherwise, the Select Deployment Scenario screen opens.
4. If you are adding a virtual server, configure the new or existing virtual server, and click **Next**.
   - If creating a new virtual server, specify the protocol, virtual server name, virtual server destination address and port, pool member IP address and port, and the logging profile.
   - If using an existing virtual server, it must have an HTTP profile and cannot be associated with a local traffic policy. Specify the protocol and virtual server.
   - If you selected **Do not associate with Virtual Server**, you will have to manually associate the security policy with a virtual server at a later time. On the policy properties screen, you need to specify a name for the security policy.

   The Select Deployment Scenario screen opens.
5. For **Deployment Scenario**, select **Create a security policy using third party vulnerability assessment tool output** and click **Next**.
   The Configure Security Policy Properties screen opens.
6. In the **Security Policy Name** field, type a unique name for the policy.
7. From the **Application Language** list, select the language encoding of the application, then click **Next**.

   Important: *You cannot change this setting after you have created the security policy.*

8. For **Enforcement Mode** specify whether or not the system blocks traffic that violates the security policy.
   - Leave the value set to **Transparent**, the default value, if you want to review and fine-tune the security policy before placing it in Blocking mode.
   - If you want the system to enforce the security policy immediately, select **Blocking**.
9. If the application is case-sensitive, select the **Security Policy is case sensitive** check box. Otherwise, leave it cleared.

   Important: *You cannot change this setting after you have created the security policy.*

10. If you do not want the security policy to distinguish between HTTP and HTTPS URLs, clear the **Differentiate between HTTP and HTTPS URLs** check box. Otherwise, leave it selected.
11. Click **Next**.
    The Vulnerability Assessments Settings screen opens.
12. From the **Vulnerability Assessment Tool** list, select **WhiteHat Sentinel**.

13. In the **Configure exceptions for the scanner IP Address** setting, specify any IP addresses that you want the security policy to allow (for example, the IP address of the vulnerability assessment tool), and how to deal with them.
    a) Type the IP address and netmask of the vulnerability assessment tool.
    You can add `%n` after an IP address to specify a route domain, where `n` is the route domain identification number.
    b) Select the appropriate check boxes for learning suggestions, logging, and blocking traffic from this IP address.

14. For **Learning Mode**, select how you want the Policy Builder to build the security policy.
    - If you want the Policy Builder to automatically build the security policy, select **Automatic**.
    - If you want the Policy Builder to make suggestions and manually decide what to include, select **Manual**.
    - If you do not want the system to suggest policy changes, select **Disabled**.

    Note: *In some cases, running the Policy Builder may overwrite some of the security policy changes suggested by the vulnerability assessment tool. For example, to prevent false positives, the Policy Builder might adjust some of the entities in the security policy based on examining the traffic.*

    If you select **Automatic** or **Manual**, the system examines traffic and makes suggestions about how to tighten the security policy. If you are using automatic learning, the system enforces the suggestions when it is reasonable to do so. If you are using manual learning, you need to examine the changes and accept, delete, or ignore them on the Traffic Learning screen. If you disabled this option, the system does not do any learning for this policy, it makes no suggestions, and the **Learn** flag for all violations becomes inactive.

15. Click **Next**.
    The Security Policy Configuration Summary screen opens.

16. Review the settings for the security policy. When you are satisfied with the security policy configuration, click **Finish**.
    The system creates the security policy and opens the vulnerability assessment settings screen specific to the tool you are using. For most tools, you can import the results of a vulnerabilities scan in an XML file.

17. Verify that the **Vulnerability Assessment Tool** is set to **WhiteHat Sentinel**.

18. To share information about the web site structure with WhiteHat Sentinel, select the **Share Site Map with Vulnerability Assessment Tool** check box, and from the **Scheduled Synchronization** list, select how often to send the information.

19. For **WhiteHat Web API Key**, type the key generated and supplied by WhiteHat Sentinel for your web application.

    Note: *If you do not have a web API key, click the* ***Get a free website security assessment from WhiteHat*** *link. A popup screen opens where you can fill in a form to request a free website security assessment. A WhiteHat representative verifies eligibility, then initiates the scan. ASM automatically downloads the results into the security policy, where you can mitigate the vulnerabilities. In this case, you do not have to complete the rest of the steps in this procedure.*

    ---

20. Click **Refresh WhiteHat Site Names List** to populate the **WhiteHat Site Name** list with the names of web applications configured under the WhiteHat Web API key. If this BIG-IP system cannot communicate with the WhiteHat service, type the application site name (defined in your WhiteHat account) in the **Custom** box.

21. On the menu bar, click **Vulnerabilities**.

22. Next, import the vulnerabilities from the WhiteHat Sentinel server. Click **Import**.
    The Import WhiteHat Sentinel Verified Vulnerabilities popup screen opens.

23. For **Import Method**, select how to import the vulnerability report:

Option	Description
Download verified vulnerabilities directly from WhiteHat Sentinel service	Download the vulnerability file from the Sentinel server directly to the Application Security Manager.
Import previously saved vulnerabilities file	Upload a previously downloaded vulnerabilities file to the Application Security Manager. Type the name of the file, or click **Browse** to search for it.

24. Click **Import**.
    The system imports the vulnerabilities the WhiteHat Sentinel service discovered during the last scan of the application.

The system creates a baseline security policy for your web application but does not yet protect against the vulnerabilities discovered by WhiteHat Sentinel. The policy type is Vulnerability Assessment.

Note: *When integrating with WhiteHat Sentinel, Application Security Manager has to recognize whether a request is coming from the WhiteHat server. This enables ASM to communicate with WhiteHat Sentinel so the WhiteHat portal can mark fixed vulnerabilities as* `Mitigated by WAF`.

ASM identifies requests sent by WhiteHat Sentinel using the published source IP of the WhiteHat Sentinel service. However, ASM does not see the original source IP address of requests if the BIG-IP system is behind a NAT (or NAT firewall), or if you are using a WhiteHat Satellite box. In these configurations, vulnerabilities that ASM protects against are not shown as mitigated in WhiteHat Sentinel.

To resolve this issue, set one or more of the `WhiteHatIP#` system variables to the redirected source IP addresses or subnets (**Security** > **Options** > **Application Security** > **Advanced Configuration** > **System Variables**). ASM then treats the address as one of the WhiteHat addresses, and sends WhiteHat information on vulnerabilities that ASM has mitigated.

Next, you need to review and resolve vulnerabilities on the Vulnerabilities screen so that the security policy protects against them.

Creating a vulnerability file

Before you can upload a vulnerability scan file from WhiteHat Sentinel, you need the following:

- Up-to-date WhiteHat Sentinel subscription and valid login credentials (`sentinel.whitehatsec.com`)
- WhiteHat Sentinel Web API key for your account
- Site name (as defined in your WhiteHat account)
- Computer with Internet access

If the BIG-IP® system does not have Internet access, you can use WhiteHat Sentinel to run a vulnerability scan on a system that does have access, then save the results of the scan as an XML file. You can then upload the vulnerability file onto Application Security Manager™. If the BIG-IP system does have Internet access, you do not need to follow this procedure.

1. On a computer with Internet access, open a browser and run the WhiteHat Sentinel vulnerability scan by typing the following command:

   `https://sentinel.whitehatsec.com/api/vuln/?display_attack_vectors=1&key=<WhiteHat_web_API_key>&display_param=1&query_site=<website_name>`

   Note: *Replace* `<WhiteHat_web_API_key>` *with the WhiteHat Web API Key, and replace* `<website_name>` *with the name of the web site you want WhiteHat Sentinel to scan for vulnerabilities.*

The results of the vulnerability scan appear in the web browser in XML format.

2. Save the results as an XML file.

You have created the vulnerability scan file that you need to create a security policy using vulnerability assessment. Place it in a location where you can access it from Application Security Manager, and upload it when creating a security policy integrated with WhiteHat Sentinel.

Resolving vulnerabilities when using WhiteHat Sentinel

Before you can resolve vulnerabilities for a security policy, the security policy must be associated with a vulnerability assessment tool (WhiteHat Sentinel, in this case), and have the vulnerabilities file imported to it.

When you resolve vulnerabilities discovered by WhiteHat Sentinel, the security policy protects against them. Application Security Manager™ (ASM) can resolve some vulnerabilities automatically. Others require some manual intervention on your part, and ASM™ provides guidance on what to do.

1. On the Main tab, click **Security** > **Application Security** > **Vulnerability Assessments**.
   The Vulnerabilities screen opens and lists the vulnerabilities that the vulnerability assessment scan discovered.
2. In the Vulnerabilities Found and Verified area, you can filter the vulnerabilities that are displayed using the **View** and **Vulnerabilities with** lists.

View option	Description
All	Displays all vulnerabilities found by the scanner.
Resolvable	Displays all vulnerabilities that are resolvable either automatically or manually.
Resolvable (Automatically)	Displays vulnerabilities that ASM can resolve.
Resolvable (Manually)	Displays vulnerabilities that can be resolved with some manual intervention.
Not Resolvable	Displays vulnerabilities that are not resolvable

Vulnerabilities with option	Description
Any	Displays vulnerabilities in any state.
Closed	Displays vulnerabilities that no longer exist and were resolved by the application (not by ASM).
Mitigated	Displays vulnerabilities that ASM has mitigated, or those which have been fixed and marked as mitigated..
Open	Displays vulnerabilities that need to be dealt with.

3. Review the vulnerabilities that the assessment tool has detected and verified.
   a) Click a row in the table to display details about the vulnerability.
      Below the Vulnerabilities Found table, a list of the specific vulnerabilities is displayed.
   b) To add notes about the vulnerability, click the pencil icon in the ASM Status column.
      The Vulnerability Notes popup opens where you can add notes.
4. For the vulnerabilities that are shown as **Resolvable (Automatically)**, select the vulnerabilities you want the system to resolve (or ignore), and click the appropriate button.

Option	Description
Resolve and Stage	Updates the security policy to protect against the vulnerability, and puts parameters in staging. Entities in staging do not cause violations, and this allows you to fine-tune their settings without causing false positives.
Resolve	Updates the security policy to protect against the vulnerability.
Ignore	Changes the ASM Status of the selected vulnerability from **Pending** to **Ignore**. If later you decide to protect against this vulnerability, you can select it and click **Cancel Ignore**.

ASM reviews the prerequisites and then displays a list of the changes it will make to fix the vulnerability.

5. If you agree with the changes, click **Resolve**.
   ASM modifies the security policy to protect against the vulnerabilities for which you clicked **Resolve** and ignores the rest. In the Vulnerabilities list, the ASM Status column for the vulnerability changes to Mitigated or Mitigated (In Staging), if appropriate.
6. For the vulnerabilities that are shown as **Resolvable (Manually)**, select the vulnerability you want to work on, and click the appropriate button.

Option	Description
Show Resolution	Opens a popup that describes the vulnerability and its possible impact, shows the steps required to manually fix the vulnerability, and describes any risks that might result from making the changes..
Change ASM Status to Mitigated	Changes the status of the vulnerability to say **Mitigated**. Recommended after you manually fix vulnerabilities.
Ignore	Changes the ASM Status of the selected vulnerability from **Pending** to **Ignore**. If later you decide to protect against this vulnerability, you can select it and click **Cancel Ignore**.

7. Click **Apply Policy** to save the changes to the security policy.
   The system updates the security policy to prevent the handled vulnerabilities from reoccurring.
8. If using WhiteHat Sentinel, select all of the vulnerabilities you dealt with and click **Retest** to have the WhiteHat Sentinel service verify that the vulnerability has been dealt with.

The security policy for your web application protects against the vulnerabilities that the vulnerability assessment tool discovered and which you resolved manually or automatically. The ASM Status of vulnerabilities that have been dealt with is set to Mitigated.

You can periodically rescan your system to check for additional vulnerabilities that need to be resolved.

Reviewing learning suggestions

After you create a security policy, the system provides learning suggestions concerning additions to the security policy based on the traffic that is accessing the application. For example, you can have users or testers browse the web application. By analyzing the traffic to and from the application, Application Security Manager™ generates learning suggestions or ways to fine-tune the security policy to better suit the traffic and secure the application.

Note: *This task is primarily for building a security policy manually. If you are using the automatic learning mode, this task applies to resolving suggestions that require manual intervention, or for speeding up the enforcement of policy elements.*

---

1. On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Traffic Learning**.
   The Traffic Learning screen opens, and lists suggestions based on traffic patterns and violations that the system has detected.
2. If you want to change the order in which the suggestions are listed, or refine what is included in the list, use the filters at the top of the column.

   You can also list the suggestions by average violation rating of all matching requests, first occurrence, last occurrence, matched entity name, or use the search filter to display specific types of suggestions that you are interested in.

   By default, the suggestions that have the highest learning score (those closest to being ready to be enforced) are listed first. Suggestions have higher learning scores if that traffic has met the conditions in the policy, if it originates from many sources, if it is unlikely to be a violation, or if the traffic comes from a trusted IP address. They may also be suggestions to add an entity the system learns, for example, a new file type, URL, or parameter.
3. On the Traffic Learning screen, review each learning suggestion.
   a) Select a learning suggestion.
   Information is displayed about the action the system will take if you accept the suggestion, and what caused the suggestion.
   b) You can learn more about the suggestion by looking at the action, the number of samples it is based on, the violations caused and their violation ratings, and if needed, by examining samples of the requests that caused the suggestion.
   c) With a request selected on the left, you can view data about the request on the right, including any violations it generated, the contents of the request itself, and the response (if any). Note that some requests may contain violations related to different suggestions.

      By examining the requests that caused a suggestion, you can determine whether it should be accepted.
   d) To add comments about the suggestion and the cause, click the Add Comment icon and type the comments.
4. Decide how to respond to the suggestion. You can start with the suggestions with the highest learning scores, or those which you know to be valid for the application. These are the options.

Option	What happens
Accept Suggestion	The system modifies the policy by taking the suggested action, such as adding an entity that is legitimate. If the entity that triggered the suggestion can be placed in staging (file types, URLs, parameters, cookies, or redirection domains), clicking **Accept Suggestion** displays a second option, **Accept suggestion** and enable staging on Matched <<entity>>. Click this option to accept the suggestion and place the matched entity in staging.
Delete Suggestion	The system removes the learning suggestion, but the suggestion reoccurs if new requests cause it. The learning score of the suggestion starts over from zero in that case.
Ignore Suggestion	The system does not change the policy and stops showing this suggestion on the Traffic Learning screen now and in the future. You can view ignored suggestions by filtering by status ignored.
Leave the suggestion	You can read the suggestions and wait to handle them until more traffic has passed through, or until you get more information. The suggestion remains in the list and no changes are made to the policy.

Note: *If you are working in automatic learning mode, when the learning score reaches 100%, the system accepts most of the suggestions, or you can accept suggestions manually at any time. If you are using manual learning, when the learning score reaches 100% (or before that if you know the suggestions are valid), you need to accept the suggestions manually.*

If you know that a suggestion is valid, you can accept it at any time even before the learning score reaches 100%. The ones that reach 100% have met all the conditions so that they are probably legitimate entities.

5. To put the security policy changes into effect immediately, click **Apply Policy**.

By default, a security policy is put into an enforcement readiness period for seven days. During that time, you can examine learning suggestions and adjust the security policy without blocking traffic. The security policy then includes elements unique to your web application.

It is a good idea to periodically review the learning suggestions on the Traffic Learning screen to determine whether the violations are legitimate and caused by an attack, or if they are false positives that indicate a need to update the security policy. Typically, a wide recurrence of violations at some place in the policy (with a low violation rating and a high learning score) indicates that they might be false positives, and hence the policy should be changed so that they will not be triggered anymore. If the violations seem to indicate true attacks (for example, they have a high violation rating), the policy should stay as is, and you can review the violations that it triggered.

Learning suggestions you must handle manually

Some learning suggestions must be resolved manually even if you are using the Automatic Learning Mode to create a security policy. Suggestions typically require manual intervention if they involve changing an attribute that was manually and deliberately set in the policy, such as a disallowed geolocation or a session ID in a URL. The system does not change the policy unless you accept the suggestion manually.

You can easily see the suggestions that you need to resolve manually because they are marked with an icon on the Traffic Learning screen as shown in the figure. You can also use the advanced filter to view the suggestions the have Learning Mode set to Manual, and this would list the suggestions you need to resolve.

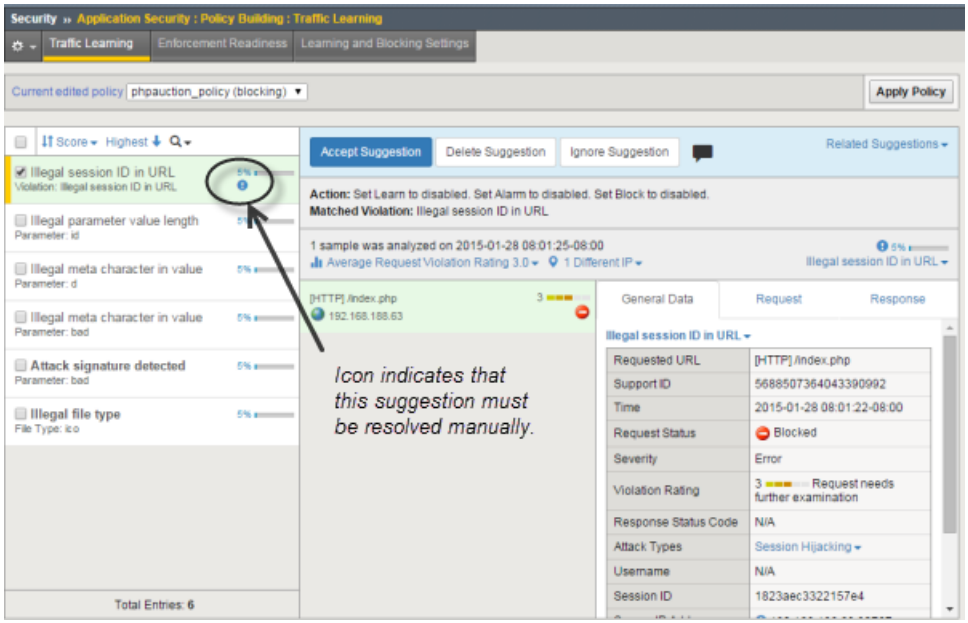

Figure 3: Suggestions that must be resolved manually

If you are using the Manual Learning Mode, you must resolve all of the suggestions manually.

Enforcing a security policy

You only need to enforce a security policy if it was created manually (not using automatic learning), and if it is operating in transparent mode. Traffic should be moving through Application Security Manager™, allowing users to access the web application for which you set up the security policy.

When you enforce a security policy, the system blocks requests that cause violations that are set to block.

1. On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Learning and Blocking Settings**.
   The Learning and Blocking Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For the **Enforcement Mode** setting, select **Blocking**.
4. Review each of the policy building settings so you understand how the security policy handles requests that cause the associated violations, and adjust if necessary. You need to expand most of the settings to see the violations.

   Tip: *To the right of Policy Building Settings, click* ***Blocking Settings*** *to see and adjust all of the violations at once.*

Option	What happens when selected
Learn	The system generates learning suggestions for requests that trigger the violation (except learning suggestions are not generated for requests that return HTTP responses with 400 or 404 status codes).
Alarm	When selected, the system marks requests that trigger the violation as illegal. The system also records illegal requests in the Charts screen, the system log (`/var/log/asm`), and possibly in local or remote logs (depending on the settings of the logging profile).
Block	The system blocks requests that trigger the violation when (1) the security policy is in the blocking enforcement mode, (2) a violation occurs, and (3) the entity is enforced. The system sends the blocking response page (containing a Support ID to identify the request) to the client.

5. Click **Save** to save your settings.
6. On the Main tab, click **Security** > **Application Security** > **Security Policies**.
   The Active Policies screen opens.
7. Click the name of the security policy you want to work on.
   The Policy Properties screen opens.
8. To change the number of days that the security policy entities and attack signatures remain in staging, change the value in the **Enforcement Readiness Period** field.

   The security policy does not block traffic during the Enforcement Readiness Period even if violations occur.
9. If you want to immediately block traffic that causes violations, you need to enforce entities that are ready to be enforced. This is one way to do this quickly:
   a) Set the **Enforcement Readiness Period** to `0`. (Not generally recommended. Use only if you want to speed up the process.)
   b) Click **Save**.
   c) On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Enforcement Readiness**.
   d) Click **Enforce Ready**.

In most cases, it is better to use a longer **Enforcement Readiness Period**, such as the default of 7 days. The entities become ready to be enforced after that.

10. To put the security policy changes into effect immediately, click **Apply Policy**.
11. For a quick summary of system activity, look at the Overview screen (**Security** > **Overview** > **Application**).
    The Summary screen displays statistical information about Application Security traffic.

After the enforcement readiness period is over and the enforcement mode is set to blocking, the security policy no longer allows requests that cause violations set to block to reach the back-end resources. Instead, the security policy blocks the request, and sends the blocking response page to the client.

Creating a Security Policy for Web Services

Overview: Creating a security policy for web services

Use the Application Security Manager™ to create a security policy for a web application that uses XML formatting or web services. The security policy can verify XML format, and validate XML document integrity against a WSDL or XSD file. The security policy can also handle encryption and decryption for web services.

The Deployment wizard guides you through the steps required to create a security policy to protect web services or XML transactions.

Considerations for developing XML security

Before you get started, you need to understand a bit about the application you are developing a security policy for. For example, you need to know the answers to the following questions:

- Does the web application use a WSDL or XML schema (XSD) file to validate the XML documents? Some web services use a WSDL or XML schema document to validate whether or not the incoming traffic complies with XML language rules. If the application uses a WSDL or XSD file, you need a copy of the file.
- Does the application use a URL or parameter to point to the server that you want to protect? You need to know the URLs or parameters that the application uses.

Task summary

Creating a security policy for web services
Creating a basic XML profile
Creating an XML profile with WSDL validation
Creating an XML profile with XML schema validation
Reviewing the status of an XML security policy
Reviewing learning suggestions
Enforcing a security policy

About XML security

Because XML is used as a data exchange mechanism, it is important to inspect, validate, and protect XML transactions. With XML security, you can protect the following applications:

- Web services that use HTTP as a transport layer for XML data
- Web services that use encryption and decryption in HTTP requests
- Web services that require verification and signing using digital signatures
- Web applications that use XML for client-server data communications, for example, Microsoft Outlook Web Access

You implement XML security by creating an XML profile for a security policy. The XML profile can protect XML applications in the following ways:

- Validates XML format

- Enforces compliance against XML schema files or WSDL documents
- Implements defense rules for XML documents
- Masks sensitive XML data
- Encrypts and decrypts parts of SOAP (Simple Object Access Protocol) web services
- Signs and verifies parts of SOAP messages using digital signatures

Flowchart for configuring XML security policy

How you proceed with configuring XML security depends on the type of application you want to protect. If the application consists simply of XML content, creating the security policy is straightforward. If your application is a SOAP web service, you have additional options for setting up the security policy.

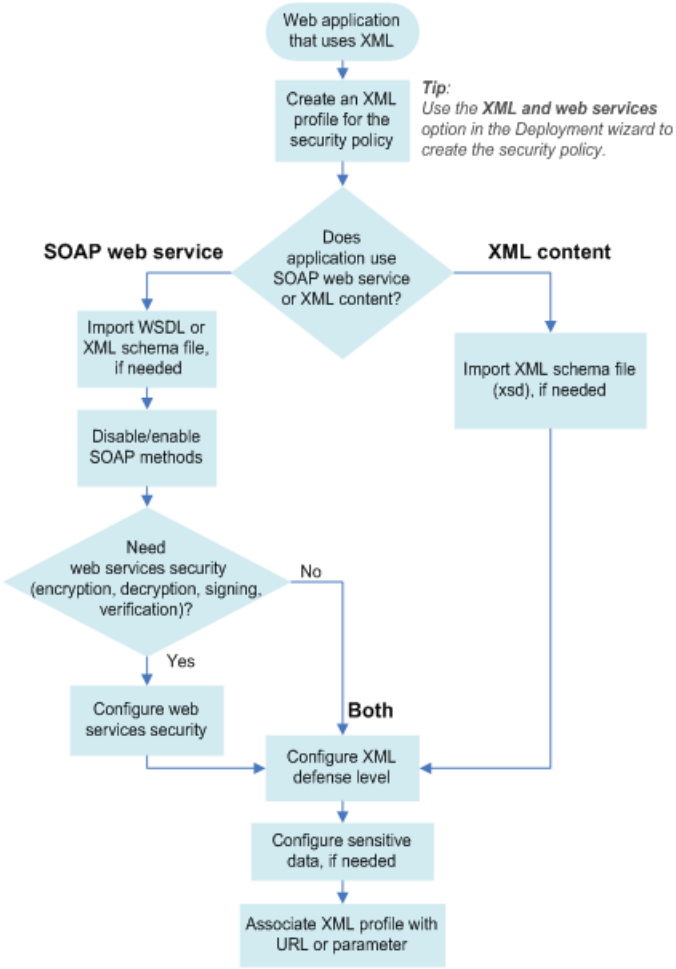

Figure 4: Securing XML applications

Creating a security policy for web services

Before you can create a security policy using ASM™, you need to complete the basic BIG-IP® system configuration tasks including creating a VLAN, a self IP address, and other tasks according to the needs of your networking environment.

Application Security Manager™ can help you create a security policy that is tailored to protect a web service application. The Deployment wizard guides you through the tasks required.

1. On the Main tab, click **Security** > **Application Security** > **Security Policies**.
   The Active Policies screen opens.
2. Click the **Create** button.
   The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.
3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.
   - To secure an existing virtual server that has no security policy associated with it, select **Existing Virtual Server** and click **Next**.
   - To create a new virtual server and pool with basic configuration settings, select **New Virtual Server** and click **Next**.
   - To create an active but unused security policy, select **Do not associate with Virtual Server** and click **Next**. No traffic will go through this security policy until you associate it with a virtual server. The Policy Builder cannot begin automatically creating a policy until traffic is going to ASM through the virtual server.

   The virtual server represents the web application you want to protect.

   The Configure Local Traffic Settings screen opens if you are adding a virtual server. Otherwise, the Select Deployment Scenario screen opens.
4. If you are adding a virtual server, configure the new or existing virtual server, and click **Next**.
   - If creating a new virtual server, specify the protocol, virtual server name, virtual server destination address and port, pool member IP address and port, and the logging profile.
   - If using an existing virtual server, it must have an HTTP profile and cannot be associated with a local traffic policy. Specify the protocol and virtual server.
   - If you selected **Do not associate with Virtual Server**, you will have to manually associate the security policy with a virtual server at a later time. On the policy properties screen, you need to specify a name for the security policy.

   The Select Deployment Scenario screen opens.
5. For **Deployment Scenario**, click **Create a security policy for XML and web services manually** and click **Next**.
   The Configure Security Policy Properties screen opens.
6. In the **Security Policy Name** field, type a unique name for the policy.
7. From the **Application Language** list, select the language encoding of the application, then click **Next**.

   Important: *You cannot change this setting after you have created the security policy.*

8. If the application is not case-sensitive, clear the **Security Policy is case sensitive** check box. Otherwise, leave it selected.

   Important: *You cannot change this setting after you have created the security policy.*

9. If you do not want the security policy to distinguish between HTTP and HTTPS URLs, clear the **Differentiate between HTTP and HTTPS URLs** check box. Otherwise, leave it selected.
10. Click **Next**.
    The Configure Attack Signatures screen opens.
11. To configure attack signatures, move the systems used by your web application from the **Available Systems** list into the **Assigned Systems** list.
    The system adds the attack signatures needed to protect the selected systems.
12. Retain the default value of **Enabled** for the **Signature Staging** setting.
    New and updated attack signatures remain in staging for seven days.
13. Click **Next**.
    The Security Policy Configuration Summary screen opens.

14. Review the settings for the security policy. When you are satisfied with the security policy configuration, click **Finish**.
    The system creates the security policy, and the Create New XML Profile screen opens and displays the message: `The initial configuration of the <<policy>> is complete. You can now create a new XML profile.`

The Deployment wizard creates the security policy. You can now configure the security policy for XML validation.

If your application has no WSDL or XML schema validation, create a basic XML profile. If the application uses a WSDL file, create an XML profile with WSDL validation. If the application uses an XML schema file, create an XML profile with XML schema validation.

Creating a basic XML profile

Before you can complete this task, you must have created a security policy using the option **Create a policy for XML and web services manually**.

If your web service includes XML data (without WSDL or schema validation), follow these steps to create a basic XML profile that defines the formatting and attack pattern checks for the security policy. You associate the XML profile with a URL or parameter.

1. If you are on the Create New XML Profile screen, skip to step 2. If not, at the top of the screen, click the **Create new XML profile** link.

   You can also navigate to **Security** > **Application Security** > **Content Profiles** > **XML Profiles** and click **Create**.

   The Create New XML Profile screen opens.
2. For **Profile Name**, type a unique name.
3. Select the **Use XML Blocking Response Page** check box to send an XML response page when the security policy blocks a request that contains XML content that does not comply with this XML profile.
4. To allow SOAP messages to have attachments, select the **Allow Attachments in SOAP Messages** check box.
5. In the Defense Configuration area, for **Defense Level**, select **High** (the default value), **Medium**, or **Low** to specify the level of protection you want the security policy to provide for XML applications and services.
   The system adjusts the defense configuration settings according to your choice. You can review the settings by selecting **Advanced** next to Defense Configuration.
6. Click **Create**.
   The Associate XML Profile screen opens.
7. For the **Associate XML Profile** setting, specify whether to associate the XML profile with a URL or a parameter:

Option	Description
URL	Validates XML data found in requests to this URL.
Parameter	Validates XML data in a parameter. You also select the **Parameter Level**: **Global** specifies that this is a global parameter that has no association with URLs. **URL** specifies that this parameter is associated with a specific URL, a protocol (HTTP or HTTPS), and a target URL path.

8. Click **Next**.

The New Allowed URL or Add Parameter screen opens, depending on which entity you choose to associate with the XML profile.

9. Create the URL or parameter to associate with the XML profile. Your steps depend on which option you selected.

Option	Description
URL	Type the explicit URL or wildcard URL that represents the web application, and click **Next**.
Global Parameter	Type the name of the parameter, and click **Create**.
URL Parameter	Type the explicit URL or wildcard URL that represents the web application, and click **Next**. Type the name of the parameter, and click **Create**.

The system creates the URL or parameter and displays the list of entities.

The system automatically associates the XML profile with the URL, global parameter, or URL parameter.

Next, you can review the status of the security policy you created.

Creating an XML profile with WSDL validation

Before you can complete this task, you must have created a security policy using the option **Create a policy for XML and web services manually**. You need to have the WSDL file you want to use for validation, and it must comply with W3C XML schema specifications and use UTF-8 character encoding.

Follow these steps to include the WSDL document in the XML profile. The resulting security policy can then enforce the allowed (or disallowed) methods and URLs.

1. If you are on the Create New XML Profile screen, skip to step 2. If not, at the top of the screen, click the **Create new XML profile** link.
   You can also navigate to **Security** > **Application Security** > **Content Profiles** > **XML Profiles** and click **Create**.
   The Create New XML Profile screen opens.
2. For **Profile Name**, type a unique name.
3. Select the **Use XML Blocking Response Page** check box to send an XML response page when the security policy blocks a request that contains XML content that does not comply with this XML profile.
4. In the Validation Configuration area, for the **File** option of the **Configuration Files** setting, navigate to the WSDL document.
5. Click **Upload**.
   The screen lists the uploaded file.
6. If the imported file references another URL (and the setting is available), for **Import URL**, type the URL.
7. To allow SOAP messages to have attachments, select the **Allow Attachments in SOAP Messages** check box.
8. In the Defense Configuration area, for **Defense Level**, select **High** (the default value), **Medium**, or **Low** to specify the level of protection you want the security policy to provide for XML applications and services.
   The system adjusts the defense configuration settings according to your choice. You can review the settings by selecting **Advanced** next to Defense Configuration.
9. Click **Create**.

In most cases, the system automatically associates a URL or parameter with the application based on the WSDL file.

If the XML Profiles screen is displayed, you are done creating the profile. Otherwise, the Associate XML Profile screen opens, and you can continue with the next step.

10. For the **Associate XML Profile** setting, specify whether to associate the XML profile with a URL or a parameter:

Option	Description
URL	Validates XML data found in requests to this URL.
Parameter	Validates XML data in a parameter. You also select the **Parameter Level**: **Global** specifies that this is a global parameter that has no association with URLs. **URL** specifies that this parameter is associated with a specific URL, a protocol (HTTP or HTTPS), and a target URL path.

11. Click **Next**.
    The New Allowed URL or Add Parameter screen opens, depending on which entity you choose to associate with the XML profile.
12. Create the URL or parameter to associate with the XML profile. Your steps depend on which option you selected.

Option	Description
URL	Type the explicit URL or wildcard URL that represents the web application, and click **Next**.
Global Parameter	Type the name of the parameter, and click **Create**.
URL Parameter	Type the explicit URL or wildcard URL that represents the web application, and click **Next**. Type the name of the parameter, and click **Create**.

    The system creates the URL or parameter and displays the list of entities.

The security policy now includes the XML profile with WSDL validation.

When you upload a WSDL document, the system automatically populates a list of SOAP methods in the validation configuration of the XML profile. Additionally, the system adds the SOAP methods as URLs in the security policy, and automatically associates the XML profile with the URLs. The system configures into the policy all relevant URLs that it finds in the WSDL and designates them as valid SOAP methods. By default, all methods are enabled, which means that the security policy allows those methods.

Next, you can review the status of the security policy you created.

Creating an XML profile with XML schema validation

Before you can complete this task, you must have created a security policy using the option **Create a policy for XML and web services manually**. You need to have the XML schema file you want to use for validation, and it must comply with W3C XML schema specifications and use UTF-8 character encoding.

You incorporate the schema file into the XML profile to complete this security policy.

1. If you are on the Create New XML Profile screen, skip to step 2. If not, at the top of the screen, click the **Create new XML profile** link.

You can also navigate to **Security** > **Application Security** > **Content Profiles** > **XML Profiles** and click **Create**.

The Create New XML Profile screen opens.

2. For **Profile Name**, type a unique name.
3. Select the **Use XML Blocking Response Page** check box to send an XML response page when the security policy blocks a request that contains XML content that does not comply with this XML profile.
4. In the Validation Configuration area, for the **Configuration Files** setting **File** option, navigate to the XML schema file (`.xsd`), then click **Upload**.
5. If the imported file references another URL (and the setting is available), for **Import URL**, type the URL.
6. To allow SOAP messages to have attachments, select the **Allow Attachments in SOAP Messages** check box.
7. In the Defense Configuration area, for **Defense Level**, select **High** (the default value), **Medium**, or **Low** to specify the level of protection you want the security policy to provide for XML applications and services.
   The system adjusts the defense configuration settings according to your choice. You can review the settings by selecting **Advanced** next to Defense Configuration.
8. Click **Create**.
   The Associate XML Profile screen opens.
9. For the **Associate XML Profile** setting, specify whether to associate the XML profile with a URL or a parameter:

Option	Description
URL	Validates XML data found in requests to this URL.
Parameter	Validates XML data in a parameter. You also select the **Parameter Level**: **Global** specifies that this is a global parameter that has no association with URLs. **URL** specifies that this parameter is associated with a specific URL, a protocol (HTTP or HTTPS), and a target URL path.

10. Click **Next**.
    The New Allowed URL or Add Parameter screen opens, depending on which entity you choose to associate with the XML profile.
11. Create the URL or parameter to associate with the XML profile. Your steps depend on which option you selected.

Option	Description
URL	Type the explicit URL or wildcard URL that represents the web application, and click **Next**.
Global Parameter	Type the name of the parameter, and click **Create**.
URL Parameter	Type the explicit URL or wildcard URL that represents the web application, and click **Next**. Type the name of the parameter, and click **Create**.

    The system creates the URL or parameter and displays the list of entities.

The security policy includes the XML profile with XML schema validation.

Next, you can review the status of the security policy you created.

Reviewing the status of an XML security policy

Before you can complete this task, you must have created a security policy using the option **Create a policy for XML and web services manually**, and traffic must be flowing to the application through the BIG-IP® system.

You can monitor the general progress of the XML security policy created using the Deployment wizard. The system processes the traffic to gather information needed to create the security policy, and displays messages about its progress.

1. On the Main tab, click **Security** > **Application Security** > **Security Policies**.
   The Active Policies screen opens.
2. Click the name of the security policy you want to work on.
   The Policy Properties screen opens.
3. Review the messages in the identification and messages area to learn about the security policy status.

Status Message	Description
The initial configuration of the security policy is complete. Checking to see if ASM is detecting traffic.	The Application Security Manager™ is parsing and analyzing received requests. Allow the system several minutes to analyze requests.
The ASM did not detect any traffic for the <<policy>> security policy.	Verify the networking configuration (check the VLAN, self IP address, pool, and virtual server).
ASM detected traffic successfully. Waiting for a minimum of 10000 requests and at least one hour from running the wizard for the *name* security policy. The ASM detected n requests during x hours and y minutes.	Application Security Manager detected traffic and will sample requests until it processes at least 10,000 requests, and at least one hour has passed since you started the Deployment wizard.
Processing XML violations for at least one hour for the *name* security policy. The ASM found *n* new XML violations during *xx* minutes and *yy* seconds.	After successfully detecting traffic and sampling requests, the Application Security Manager processes XML violations. Based on what it finds in the traffic sample and the violations, Application Security Manager automatically adjusts security policy settings to match the traffic and eliminate false positives. The system samples requests for at least one hour.
The system did not detect any new XML violations over the last hour for the *name* security policy. You can now go to the Traffic Learning page to fine-tune the security policy.	For at least an hour, none of the traffic going to or from the application has caused XML violations. When you see this message, you can fine-tune the security policy.
Timed out while waiting for sufficient number of requests for the security policy. Checking XML violations status.	The system processed insufficient traffic to finish building the security policy. Check to be sure that traffic can access the web application.

Reviewing learning suggestions

After you create a security policy, the system provides learning suggestions concerning additions to the security policy based on the traffic that is accessing the application. For example, you can have users or testers browse the web application. By analyzing the traffic to and from the application, Application Security Manager™ generates learning suggestions or ways to fine-tune the security policy to better suit the traffic and secure the application.

Note: *This task is primarily for building a security policy manually. If you are using the automatic learning mode, this task applies to resolving suggestions that require manual intervention, or for speeding up the enforcement of policy elements.*

1. On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Traffic Learning**.
   The Traffic Learning screen opens, and lists suggestions based on traffic patterns and violations that the system has detected.
2. If you want to change the order in which the suggestions are listed, or refine what is included in the list, use the filters at the top of the column.

   You can also list the suggestions by average violation rating of all matching requests, first occurrence, last occurrence, matched entity name, or use the search filter to display specific types of suggestions that you are interested in.

   By default, the suggestions that have the highest learning score (those closest to being ready to be enforced) are listed first. Suggestions have higher learning scores if that traffic has met the conditions in the policy, if it originates from many sources, if it is unlikely to be a violation, or if the traffic comes from a trusted IP address. They may also be suggestions to add an entity the system learns, for example, a new file type, URL, or parameter.
3. On the Traffic Learning screen, review each learning suggestion.
   a) Select a learning suggestion.
   Information is displayed about the action the system will take if you accept the suggestion, and what caused the suggestion.
   b) You can learn more about the suggestion by looking at the action, the number of samples it is based on, the violations caused and their violation ratings, and if needed, by examining samples of the requests that caused the suggestion.
   c) With a request selected on the left, you can view data about the request on the right, including any violations it generated, the contents of the request itself, and the response (if any). Note that some requests may contain violations related to different suggestions.

      By examining the requests that caused a suggestion, you can determine whether it should be accepted.
   d) To add comments about the suggestion and the cause, click the Add Comment icon and type the comments.
4. Decide how to respond to the suggestion. You can start with the suggestions with the highest learning scores, or those which you know to be valid for the application. These are the options.

Option	What happens
Accept Suggestion	The system modifies the policy by taking the suggested action, such as adding an entity that is legitimate. If the entity that triggered the suggestion can be placed in staging (file types, URLs, parameters, cookies, or redirection domains), clicking **Accept Suggestion** displays a second option, **Accept suggestion** and enable staging on Matched <<entity>>. Click this option to accept the suggestion and place the matched entity in staging.
Delete Suggestion	The system removes the learning suggestion, but the suggestion reoccurs if new requests cause it. The learning score of the suggestion starts over from zero in that case.
Ignore Suggestion	The system does not change the policy and stops showing this suggestion on the Traffic Learning screen now and in the future. You can view ignored suggestions by filtering by status ignored.
Leave the suggestion	You can read the suggestions and wait to handle them until more traffic has passed through, or until you get more information. The suggestion remains in the list and no changes are made to the policy.

Note: *If you are working in automatic learning mode, when the learning score reaches 100%, the system accepts most of the suggestions, or you can accept suggestions manually at any time. If you are using manual learning, when the learning score reaches 100% (or before that if you know the suggestions are valid), you need to accept the suggestions manually.*

If you know that a suggestion is valid, you can accept it at any time even before the learning score reaches 100%. The ones that reach 100% have met all the conditions so that they are probably legitimate entities.

---

5. To put the security policy changes into effect immediately, click **Apply Policy**.

By default, a security policy is put into an enforcement readiness period for seven days. During that time, you can examine learning suggestions and adjust the security policy without blocking traffic. The security policy then includes elements unique to your web application.

It is a good idea to periodically review the learning suggestions on the Traffic Learning screen to determine whether the violations are legitimate and caused by an attack, or if they are false positives that indicate a need to update the security policy. Typically, a wide recurrence of violations at some place in the policy (with a low violation rating and a high learning score) indicates that they might be false positives, and hence the policy should be changed so that they will not be triggered anymore. If the violations seem to indicate true attacks (for example, they have a high violation rating), the policy should stay as is, and you can review the violations that it triggered.

Enforcing a security policy

You only need to enforce a security policy if it was created manually (not using automatic learning), and if it is operating in transparent mode. Traffic should be moving through Application Security Manager™, allowing users to access the web application for which you set up the security policy.

When you enforce a security policy, the system blocks requests that cause violations that are set to block.

1. On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Learning and Blocking Settings**.
   The Learning and Blocking Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For the **Enforcement Mode** setting, select **Blocking**.
4. Review each of the policy building settings so you understand how the security policy handles requests that cause the associated violations, and adjust if necessary. You need to expand most of the settings to see the violations.

Tip: *To the right of Policy Building Settings, click* ***Blocking Settings*** *to see and adjust all of the violations at once.*

Option	What happens when selected
Learn	The system generates learning suggestions for requests that trigger the violation (except learning suggestions are not generated for requests that return HTTP responses with 400 or 404 status codes).
Alarm	When selected, the system marks requests that trigger the violation as illegal. The system also records illegal requests in the Charts screen, the system log (`/var/log/asm`), and possibly in local or remote logs (depending on the settings of the logging profile).

Option	What happens when selected
Block	The system blocks requests that trigger the violation when (1) the security policy is in the blocking enforcement mode, (2) a violation occurs, and (3) the entity is enforced. The system sends the blocking response page (containing a Support ID to identify the request) to the client.

5. Click **Save** to save your settings.
6. On the Main tab, click **Security** > **Application Security** > **Security Policies**.
   The Active Policies screen opens.
7. Click the name of the security policy you want to work on.
   The Policy Properties screen opens.
8. To change the number of days that the security policy entities and attack signatures remain in staging, change the value in the **Enforcement Readiness Period** field.

   The security policy does not block traffic during the Enforcement Readiness Period even if violations occur.
9. If you want to immediately block traffic that causes violations, you need to enforce entities that are ready to be enforced. This is one way to do this quickly:
   a) Set the **Enforcement Readiness Period** to `0`. (Not generally recommended. Use only if you want to speed up the process.)
   b) Click **Save**.
   c) On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Enforcement Readiness**.
   d) Click **Enforce Ready**.

   In most cases, it is better to use a longer **Enforcement Readiness Period**, such as the default of 7 days. The entities become ready to be enforced after that.
10. To put the security policy changes into effect immediately, click **Apply Policy**.
11. For a quick summary of system activity, look at the Overview screen (**Security** > **Overview** > **Application**).
    The Summary screen displays statistical information about Application Security traffic.

After the enforcement readiness period is over and the enforcement mode is set to blocking, the security policy no longer allows requests that cause violations set to block to reach the back-end resources. Instead, the security policy blocks the request, and sends the blocking response page to the client.

Using Rapid Deployment

Overview: Rapid deployment

The Rapid Deployment security policy provides security features that minimize the number of false positive alarms and reduce the complexity and length of the deployment period. By default, the Rapid Deployment security policy includes the following security checks:

- Performs HTTP compliance checks
- Checks for mandatory HTTP headers
- Stops information leakage
- Prevents illegal HTTP methods from being used in a request
- Checks response codes
- Enforces cookie RFC compliance
- Applies attack signatures to requests (and responses, if applying signatures to responses)
- Detects evasion technique
- Prevents access from disallowed geolocations
- Prevents access from disallowed users, sessions, and IP addresses
- Checks whether request length exceeds defined buffer size
- Detects disallowed file upload content
- Checks for characters that failed to convert
- Looks for requests with modified ASM™ cookies

With the Rapid Deployment security policy, your organization can quickly create a security policy that meets the majority of web application security requirements.

Task summary

Creating a security policy using rapid deployment
Reviewing learning suggestions
Enforcing a security policy

Creating a security policy using rapid deployment

Before you can create a security policy using ASM™, you need to complete the basic BIG-IP® system configuration tasks including creating a VLAN, a self IP address, and other tasks, according to the needs of your networking environment.

You can use rapid deployment to create a security policy quickly. The Deployment wizard takes you through the steps required for rapid deployment.

1. On the Main tab, click **Security** > **Application Security** > **Security Policies**.
   The Active Policies screen opens.
2. Click the **Create** button.
   The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.
3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.

- To secure an existing virtual server that has no security policy associated with it, select **Existing Virtual Server** and click **Next**.
- To create a new virtual server and pool with basic configuration settings, select **New Virtual Server** and click **Next**.
- To create an active but unused security policy, select **Do not associate with Virtual Server** and click **Next**. No traffic will go through this security policy until you associate it with a virtual server. The Policy Builder cannot begin automatically creating a policy until traffic is going to ASM through the virtual server.

The virtual server represents the web application you want to protect.

The Configure Local Traffic Settings screen opens if you are adding a virtual server. Otherwise, the Select Deployment Scenario screen opens.

4. If you are adding a virtual server, configure the new or existing virtual server, and click **Next**.
   - If creating a new virtual server, specify the protocol, virtual server name, virtual server destination address and port, pool member IP address and port, and the logging profile.
   - If using an existing virtual server, it must have an HTTP profile and cannot be associated with a local traffic policy. Specify the protocol and virtual server.
   - If you selected **Do not associate with Virtual Server**, you will have to manually associate the security policy with a virtual server at a later time. On the policy properties screen, you need to specify a name for the security policy.

   The Select Deployment Scenario screen opens.
5. For **Deployment Scenario**, select **Create a security policy manually or use templates** and click **Next**.
   The Configure Security Policy Properties screen opens.
6. In the **Security Policy Name** field, type a unique name for the policy.
7. From the **Application Language** list, select the language encoding of the application.

   Important: *You cannot change this setting after you have created the security policy.*

8. From the **Application-Ready Security Policy** list, select **Rapid Deployment security policy**.
9. For the **Enforcement Readiness Period**, retain the default setting of 7 days.

   During this period, you can test the security policy entities for false positives before enforcing them.

   During the enforcement readiness period, the security policy provides learning suggestions when it processes requests that do not meet the security policy; but the security policy does not alert or block that traffic, even if those requests trigger violations. You can review new entities and decide which are legitimate and include them in the security policy.
10. Click **Next**.
    The Configure Attack Signatures screen opens.
11. To configure attack signatures, move the systems used by your web application from the **Available Systems** list into the **Assigned Systems** list.
    The system adds the attack signatures needed to protect the selected systems.
12. Retain the default value of **Enabled** for the **Signature Staging** setting.
    New and updated attack signatures remain in staging for seven days, and during that time, they are not enforced (according to the learn, alarm, and block flags selected for each of the signature sets), and only generate alerts for traffic that matches the signature. At the end of the staging period, the system automatically enforces the signatures that did not receive any hits.
13. To have the system inspect responses for attacks, for the **Apply Signatures to Responses** setting, select **Enabled**.
14. Click **Next**.
    The Security Policy Configuration Summary screen opens.
15. Review the settings for the security policy. When you are satisfied with the security policy configuration, click **Finish**.

The system creates the security policy and opens the Policy Properties screen.

The system creates a simple security policy that protects against known vulnerabilities, such as evasion attacks, data leakage, and buffer overflow attacks. The rapid deployment security policy operates in transparent mode (meaning that it does not block traffic unless you changed the enforcement mode). If the system receives a request that violates the security policy, the system logs the violation event, but does not block the request. Suggestions for changes to the policy are added to the Traffic Learning screen.

Reviewing learning suggestions

After you create a security policy, the system provides learning suggestions concerning additions to the security policy based on the traffic that is accessing the application. For example, you can have users or testers browse the web application. By analyzing the traffic to and from the application, Application Security Manager™ generates learning suggestions or ways to fine-tune the security policy to better suit the traffic and secure the application.

Note: *This task is primarily for building a security policy manually. If you are using the automatic learning mode, this task applies to resolving suggestions that require manual intervention, or for speeding up the enforcement of policy elements.*

---

1. On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Traffic Learning**.
   The Traffic Learning screen opens, and lists suggestions based on traffic patterns and violations that the system has detected.
2. If you want to change the order in which the suggestions are listed, or refine what is included in the list, use the filters at the top of the column.

   You can also list the suggestions by average violation rating of all matching requests, first occurrence, last occurrence, matched entity name, or use the search filter to display specific types of suggestions that you are interested in.

   By default, the suggestions that have the highest learning score (those closest to being ready to be enforced) are listed first. Suggestions have higher learning scores if that traffic has met the conditions in the policy, if it originates from many sources, if it is unlikely to be a violation, or if the traffic comes from a trusted IP address. They may also be suggestions to add an entity the system learns, for example, a new file type, URL, or parameter.
3. On the Traffic Learning screen, review each learning suggestion.
   a) Select a learning suggestion.
   Information is displayed about the action the system will take if you accept the suggestion, and what caused the suggestion.
   b) You can learn more about the suggestion by looking at the action, the number of samples it is based on, the violations caused and their violation ratings, and if needed, by examining samples of the requests that caused the suggestion.
   c) With a request selected on the left, you can view data about the request on the right, including any violations it generated, the contents of the request itself, and the response (if any). Note that some requests may contain violations related to different suggestions.

      By examining the requests that caused a suggestion, you can determine whether it should be accepted.
   d) To add comments about the suggestion and the cause, click the Add Comment icon and type the comments.
4. Decide how to respond to the suggestion. You can start with the suggestions with the highest learning scores, or those which you know to be valid for the application. These are the options.

Option	What happens
Accept Suggestion	The system modifies the policy by taking the suggested action, such as adding an entity that is legitimate. If the entity that triggered the suggestion can be placed in staging (file types, URLs, parameters, cookies, or redirection domains), clicking **Accept Suggestion** displays a second option, **Accept suggestion** and enable staging on Matched <<entity>>. Click this option to accept the suggestion and place the matched entity in staging.
Delete Suggestion	The system removes the learning suggestion, but the suggestion reoccurs if new requests cause it. The learning score of the suggestion starts over from zero in that case.
Ignore Suggestion	The system does not change the policy and stops showing this suggestion on the Traffic Learning screen now and in the future. You can view ignored suggestions by filtering by status ignored.
Leave the suggestion	You can read the suggestions and wait to handle them until more traffic has passed through, or until you get more information. The suggestion remains in the list and no changes are made to the policy.

Note: *If you are working in automatic learning mode, when the learning score reaches 100%, the system accepts most of the suggestions, or you can accept suggestions manually at any time. If you are using manual learning, when the learning score reaches 100% (or before that if you know the suggestions are valid), you need to accept the suggestions manually.*

If you know that a suggestion is valid, you can accept it at any time even before the learning score reaches 100%. The ones that reach 100% have met all the conditions so that they are probably legitimate entities.

---

5. To put the security policy changes into effect immediately, click **Apply Policy**.

By default, a security policy is put into an enforcement readiness period for seven days. During that time, you can examine learning suggestions and adjust the security policy without blocking traffic. The security policy then includes elements unique to your web application.

It is a good idea to periodically review the learning suggestions on the Traffic Learning screen to determine whether the violations are legitimate and caused by an attack, or if they are false positives that indicate a need to update the security policy. Typically, a wide recurrence of violations at some place in the policy (with a low violation rating and a high learning score) indicates that they might be false positives, and hence the policy should be changed so that they will not be triggered anymore. If the violations seem to indicate true attacks (for example, they have a high violation rating), the policy should stay as is, and you can review the violations that it triggered.

Enforcing a security policy

You only need to enforce a security policy if it was created manually (not using automatic learning), and if it is operating in transparent mode. Traffic should be moving through Application Security Manager™, allowing users to access the web application for which you set up the security policy.

When you enforce a security policy, the system blocks requests that cause violations that are set to block.

1. On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Learning and Blocking Settings**.
   The Learning and Blocking Settings screen opens.

2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For the **Enforcement Mode** setting, select **Blocking**.
4. Review each of the policy building settings so you understand how the security policy handles requests that cause the associated violations, and adjust if necessary. You need to expand most of the settings to see the violations.

   Tip: *To the right of Policy Building Settings, click* ***Blocking Settings*** *to see and adjust all of the violations at once.*

Option	What happens when selected
Learn	The system generates learning suggestions for requests that trigger the violation (except learning suggestions are not generated for requests that return HTTP responses with 400 or 404 status codes).
Alarm	When selected, the system marks requests that trigger the violation as illegal. The system also records illegal requests in the Charts screen, the system log (`/var/log/asm`), and possibly in local or remote logs (depending on the settings of the logging profile).
Block	The system blocks requests that trigger the violation when (1) the security policy is in the blocking enforcement mode, (2) a violation occurs, and (3) the entity is enforced. The system sends the blocking response page (containing a Support ID to identify the request) to the client.

5. Click **Save** to save your settings.
6. On the Main tab, click **Security** > **Application Security** > **Security Policies**.
   The Active Policies screen opens.
7. Click the name of the security policy you want to work on.
   The Policy Properties screen opens.
8. To change the number of days that the security policy entities and attack signatures remain in staging, change the value in the **Enforcement Readiness Period** field.

   The security policy does not block traffic during the Enforcement Readiness Period even if violations occur.
9. If you want to immediately block traffic that causes violations, you need to enforce entities that are ready to be enforced. This is one way to do this quickly:
   a) Set the **Enforcement Readiness Period** to `0`. (Not generally recommended. Use only if you want to speed up the process.)
   b) Click **Save**.
   c) On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Enforcement Readiness**.
   d) Click **Enforce Ready**.

   In most cases, it is better to use a longer **Enforcement Readiness Period**, such as the default of 7 days. The entities become ready to be enforced after that.
10. To put the security policy changes into effect immediately, click **Apply Policy**.
11. For a quick summary of system activity, look at the Overview screen (**Security** > **Overview** > **Application**).
    The Summary screen displays statistical information about Application Security traffic.

After the enforcement readiness period is over and the enforcement mode is set to blocking, the security policy no longer allows requests that cause violations set to block to reach the back-end resources. Instead, the security policy blocks the request, and sends the blocking response page to the client.

Using Application-Ready Security Templates

Overview: Using application-ready security templates

The Application Security Manager™ provides application-ready security policies, which are baseline templates, for the following enterprise applications:

- Microsoft ActiveSync® 1.0, 2.0
- Microsoft Outlook Web Access Exchange® 2003, 2007, 2010
- Microsoft Outlook Web Access Exchange® with Microsoft ActiveSync® 2003, 2007
- Oracle® Applications 11i
- Oracle® Portal 10g
- Lotus Domino® 6.5
- SAP NetWeaver® 7
- PeopleSoft® Portal Solutions 9

By using an application-ready template, your organization can quickly create a security policy designed to secure that specific web application. It is a fixed policy that only changes if you decide to adjust it manually or configure additional security features.

Task summary

Creating a security policy from an application template
Reviewing learning suggestions
Enforcing a security policy

Creating a security policy from an application template

Before you can create a security policy, you must perform the minimal system configuration tasks including defining a VLAN, a self IP address, and other tasks required according to the needs of your networking environment.

If you want to create a security policy for one of the commonly used enterprise applications, you can use application-ready templates to create the policy quickly. The Deployment wizard takes you through the steps required.

1. On the Main tab, click **Security** > **Application Security** > **Security Policies**.
   The Active Policies screen opens.
2. Click the **Create** button.
   The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.
3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.
   - To secure an existing virtual server that has no security policy associated with it, select **Existing Virtual Server** and click **Next**.
   - To create a new virtual server and pool with basic configuration settings, select **New Virtual Server** and click **Next**.

- To create an active but unused security policy, select **Do not associate with Virtual Server** and click **Next**. No traffic will go through this security policy until you associate it with a virtual server. The Policy Builder cannot begin automatically creating a policy until traffic is going to ASM through the virtual server.

The virtual server represents the web application you want to protect.

The Configure Local Traffic Settings screen opens if you are adding a virtual server. Otherwise, the Select Deployment Scenario screen opens.

4. If you are adding a virtual server, configure the new or existing virtual server, and click **Next**.
   - If creating a new virtual server, specify the protocol, virtual server name, virtual server destination address and port, pool member IP address and port, and the logging profile.
   - If using an existing virtual server, it must have an HTTP profile and cannot be associated with a local traffic policy. Specify the protocol and virtual server.
   - If you selected **Do not associate with Virtual Server**, you will have to manually associate the security policy with a virtual server at a later time. On the policy properties screen, you need to specify a name for the security policy.

   The Select Deployment Scenario screen opens.
5. For **Deployment Scenario**, select **Create a security policy manually or use templates** and click **Next**. The Configure Security Policy Properties screen opens.
6. In the **Security Policy Name** field, type a unique name for the policy.
7. From the **Application Language** list, select the language encoding of the application.

   Important: *You cannot change this setting after you have created the security policy.*

8. From the **Application-Ready Security Policy** list, select the security policy template to use for your enterprise application.
9. For the **Enforcement Readiness Period**, retain the default setting of 7 days.

   During this period, you can test the security policy entities for false positives before enforcing them.

   During the enforcement readiness period, the security policy provides learning suggestions when it processes requests that do not meet the security policy; but the security policy does not alert or block that traffic, even if those requests trigger violations. You can review new entities and decide which are legitimate and include them in the security policy.
10. Click **Next**.
    The Security Policy Configuration Summary screen opens.
11. Review the settings for the security policy. When you are satisfied with the security policy configuration, click **Finish**.
    The system creates the security policy and opens the Policy Properties screen.

When you first create the security policy, it operates in transparent mode (meaning that it does not block traffic). When the system receives a request that violates the security policy, the system logs the violation event and makes suggestions for additions to the security policy, but does not block the request. After a period of time (called the enforcement readiness period), the system suggests that you enforce the policy changes. Next, you can review the learning suggestions, decide which are reasonable to make for the web application, and add them to the security policy.

Reviewing learning suggestions

After you create a security policy, the system provides learning suggestions concerning additions to the security policy based on the traffic that is accessing the application. For example, you can have users or testers browse the web application. By analyzing the traffic to and from the application, Application Security

Manager™ generates learning suggestions or ways to fine-tune the security policy to better suit the traffic and secure the application.

Note: *This task is primarily for building a security policy manually. If you are using the automatic learning mode, this task applies to resolving suggestions that require manual intervention, or for speeding up the enforcement of policy elements.*

---

1. On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Traffic Learning**.
   The Traffic Learning screen opens, and lists suggestions based on traffic patterns and violations that the system has detected.
2. If you want to change the order in which the suggestions are listed, or refine what is included in the list, use the filters at the top of the column.

   You can also list the suggestions by average violation rating of all matching requests, first occurrence, last occurrence, matched entity name, or use the search filter to display specific types of suggestions that you are interested in.

   By default, the suggestions that have the highest learning score (those closest to being ready to be enforced) are listed first. Suggestions have higher learning scores if that traffic has met the conditions in the policy, if it originates from many sources, if it is unlikely to be a violation, or if the traffic comes from a trusted IP address. They may also be suggestions to add an entity the system learns, for example, a new file type, URL, or parameter.
3. On the Traffic Learning screen, review each learning suggestion.
   a) Select a learning suggestion.
   Information is displayed about the action the system will take if you accept the suggestion, and what caused the suggestion.
   b) You can learn more about the suggestion by looking at the action, the number of samples it is based on, the violations caused and their violation ratings, and if needed, by examining samples of the requests that caused the suggestion.
   c) With a request selected on the left, you can view data about the request on the right, including any violations it generated, the contents of the request itself, and the response (if any). Note that some requests may contain violations related to different suggestions.

      By examining the requests that caused a suggestion, you can determine whether it should be accepted.
   d) To add comments about the suggestion and the cause, click the Add Comment icon and type the comments.
4. Decide how to respond to the suggestion. You can start with the suggestions with the highest learning scores, or those which you know to be valid for the application. These are the options.

Option	What happens
Accept Suggestion	The system modifies the policy by taking the suggested action, such as adding an entity that is legitimate. If the entity that triggered the suggestion can be placed in staging (file types, URLs, parameters, cookies, or redirection domains), clicking **Accept Suggestion** displays a second option, **Accept suggestion** and enable staging on Matched <<entity>>. Click this option to accept the suggestion and place the matched entity in staging.
Delete Suggestion	The system removes the learning suggestion, but the suggestion reoccurs if new requests cause it. The learning score of the suggestion starts over from zero in that case.
Ignore Suggestion	The system does not change the policy and stops showing this suggestion on the Traffic Learning screen now and in the future. You can view ignored suggestions by filtering by status ignored.

Option	What happens
Leave the suggestion	You can read the suggestions and wait to handle them until more traffic has passed through, or until you get more information. The suggestion remains in the list and no changes are made to the policy.

Note: *If you are working in automatic learning mode, when the learning score reaches 100%, the system accepts most of the suggestions, or you can accept suggestions manually at any time. If you are using manual learning, when the learning score reaches 100% (or before that if you know the suggestions are valid), you need to accept the suggestions manually.*

If you know that a suggestion is valid, you can accept it at any time even before the learning score reaches 100%. The ones that reach 100% have met all the conditions so that they are probably legitimate entities.

5. To put the security policy changes into effect immediately, click **Apply Policy**.

By default, a security policy is put into an enforcement readiness period for seven days. During that time, you can examine learning suggestions and adjust the security policy without blocking traffic. The security policy then includes elements unique to your web application.

It is a good idea to periodically review the learning suggestions on the Traffic Learning screen to determine whether the violations are legitimate and caused by an attack, or if they are false positives that indicate a need to update the security policy. Typically, a wide recurrence of violations at some place in the policy (with a low violation rating and a high learning score) indicates that they might be false positives, and hence the policy should be changed so that they will not be triggered anymore. If the violations seem to indicate true attacks (for example, they have a high violation rating), the policy should stay as is, and you can review the violations that it triggered.

Enforcing a security policy

You only need to enforce a security policy if it was created manually (not using automatic learning), and if it is operating in transparent mode. Traffic should be moving through Application Security Manager™, allowing users to access the web application for which you set up the security policy.

When you enforce a security policy, the system blocks requests that cause violations that are set to block.

1. On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Learning and Blocking Settings**.
   The Learning and Blocking Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For the **Enforcement Mode** setting, select **Blocking**.
4. Review each of the policy building settings so you understand how the security policy handles requests that cause the associated violations, and adjust if necessary. You need to expand most of the settings to see the violations.

Tip: *To the right of Policy Building Settings, click* ***Blocking Settings*** *to see and adjust all of the violations at once.*

Option	What happens when selected
Learn	The system generates learning suggestions for requests that trigger the violation (except learning suggestions are not generated for requests that return HTTP responses with 400 or 404 status codes).

Option	What happens when selected
Alarm	When selected, the system marks requests that trigger the violation as illegal. The system also records illegal requests in the Charts screen, the system log (`/var/log/asm`), and possibly in local or remote logs (depending on the settings of the logging profile).
Block	The system blocks requests that trigger the violation when (1) the security policy is in the blocking enforcement mode, (2) a violation occurs, and (3) the entity is enforced. The system sends the blocking response page (containing a Support ID to identify the request) to the client.

5. Click **Save** to save your settings.
6. On the Main tab, click **Security** > **Application Security** > **Security Policies**.
   The Active Policies screen opens.
7. Click the name of the security policy you want to work on.
   The Policy Properties screen opens.
8. To change the number of days that the security policy entities and attack signatures remain in staging, change the value in the **Enforcement Readiness Period** field.

   The security policy does not block traffic during the Enforcement Readiness Period even if violations occur.
9. If you want to immediately block traffic that causes violations, you need to enforce entities that are ready to be enforced. This is one way to do this quickly:
   a) Set the **Enforcement Readiness Period** to `0`. (Not generally recommended. Use only if you want to speed up the process.)
   b) Click **Save**.
   c) On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Enforcement Readiness**.
   d) Click **Enforce Ready**.

   In most cases, it is better to use a longer **Enforcement Readiness Period**, such as the default of 7 days. The entities become ready to be enforced after that.
10. To put the security policy changes into effect immediately, click **Apply Policy**.
11. For a quick summary of system activity, look at the Overview screen (**Security** > **Overview** > **Application**).
    The Summary screen displays statistical information about Application Security traffic.

After the enforcement readiness period is over and the enforcement mode is set to blocking, the security policy no longer allows requests that cause violations set to block to reach the back-end resources. Instead, the security policy blocks the request, and sends the blocking response page to the client.

Index

T

V

W

X