BIG-IP® Application Security Manager®: Getting Started

Version 13.1

Table of Contents

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, such as HIPAA and PCI DSS. 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, brute force attacks, 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 policy templates 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.

ASM provides multi-faceted DoS attack protection for web applications including proactive bot defense, bot signatures, CAPTCHA challenge, stress-based protection, and behavioral DoS.

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.

What is a security policy?

The core of Application Security Manager™ functionality centers around the security policy, which secures a web application server from malicious traffic, using both positive and negative security features. Positive security features indicate which traffic has a known degree of trust, such as which file types, URLs, parameters, or IP address ranges can access the web server. Negative security features provide the ability to detect and thwart known attack patterns, such as those defined in attack signatures. Security polices can also include protection against DoS attacks, brute force attacks, web scraping, cross-site request forgery, and multiple attacks from an IP address.

When a user sends a request to the web application server, the system examines the request to see if it meets the requirements of the security policy protecting the application. If the request complies with the security policy, the system forwards the request to the web application. If the request does not comply with the security policy, the system generates a violation (or violations), and then either forwards or blocks the request, depending on the enforcement mode of the security policy and the blocking settings on the violation.

The system can similarly check responses from the web server. Responses that comply with the security policy are sent to the client, but those that do not comply cause violations and may also be blocked.

Types of attacks ASM protects against

Application Security Manager™ (ASM) is a web application firewall that 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:

- Layer 7 DoS/DDoS, brute force, and web scraping attacks
- Malicious bot traffic
- SQL injection attacks intended to expose confidential information or to corrupt content
- Exploitations of the application memory buffer to stop services, get shell access, and propagate worms
- Fraudulent transactions 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
- Manipulation of cookies or hidden fields
- 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 customizing the system response to threats.

Creating a Simple Security Policy

Types of security policies

You can create several types of security policies. It is a good idea to understand your options before you begin.

Security policy type	Description
Automatic security policy	Create a security policy for a web application by having the system examine traffic and create the 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.
Manual security policy	Use rapid deployment or an application-ready security policy (pre-configured template) to develop a security policy so you can 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.
Security policy integrated with vulnerability assessment tool	Create a security policy based on integrating the output from a vulnerability assessment tool, such as WhiteHat Sentinel, IBM® AppScan®, Trustwave® App Scanner (Cenzic), 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.
Parent security policy	Create a security policy that can form the basis of other related security policies. This is useful if you have several similar applications for which you want to create security policies. Selected settings in the parent policy are inherited by child policies that you create. By adjusting the parent policy, the child policies are changed as well.
Child security policy	Create a security policy that is based on a parent security policy. When you create a child policy, the values for the settings are inherited from the parent. You can edit some of the settings and others can only be changed in the parent policy.
Template security policy	Use a template to populate the attributes of a new policy. The template is only used when creating the policy - a security policy is always created based on a user-defined or system-supplied template. Unlike parent policies, the templates do not affect the policy after it is created. If you modify a template, policies created from them in the past are not affected.

Preparing to create a security policy

Before you create and deploy a security policy, you should have an understanding of the application you are trying to protect and why you are trying to protect it. By defining your security problem, you will have an easier time creating and enforcing your security policy.

Some of the questions you might consider before you start are:

- How strict a policy do you want to create? Fundamental or comprehensive?
- How many applications do you want ASM to protect? If protecting multiple applications, how similar are they?
- Do you want to develop one policy for multiple applications, or are the applications different enough that you want to create separate policies for them?
- Are there a basic set of features that you want to control from a parent policy? Multiple policies can inherit settings from a parent policy.
- How much traffic and what types of traffic do the applications handle? HTTP, HTTPS, or both?
- Do the applications have lots of parameters and URLs associated with them? Or are they simple?

A strict, application-specific security policy can potentially take more time and effort to maintain, especially in light of application changes. A generic policy requires less maintenance, even when applied to multiple applications. Some situations will require more extensive tuning of the security policy while in other cases a simple policy will provide effective protection from attacks.

Overview: Creating a simple security policy

You can use the Application Security Manager™ (ASM) to help you build a security policy that is tailored to your environment. ASM can build a policy automatically, or you can do it manually. The policy building tool is called the Real Traffic Policy Builder® (referred to simply as the Policy Builder). The Policy Builder adds suggestions for strengthening a security policy based on settings that you configure, 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.

Here we take you through the steps of creating a simple security policy to introduce you to ASM.

Task summary

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

Creating a simple security policy

Before you can create a security policy, you must perform the minimal system configuration tasks required according to the needs of your networking environment.

You can use Application Security Manager™ to create a robust, yet simple, security policy that is tailored to protect your web application. This is the easiest way to create a security policy.

1. On the Main tab, click **Security** > **Application Security** > **Security Policies** > **Policies List**. The Policies List screen opens.
2. Click **Create New Policy**.

You only see this button when no policy is selected.

3. In the **Policy Name** field, type a name for the policy.
4. Leave **Policy Type**, set to **Security**.
5. For **Policy Template**, select **Fundamental**.
6. For **Virtual Server**, click **Configure new virtual server** to specify where to direct application requests.
   a) For **What type of protocol does your application use?**, select **HTTP**, **HTTPS**, or both.
   b) In the **Virtual Server Name** field, type a unique name.
   c) In the **HTTP Virtual Server Destination** field, type the address in IPv4 (`10.0.0.1`) or IPv6 (`2001:ed8:77b5:2:10:10:100:42/64`) format, and specify the service port.

   Tip: *If you want multiple IP addresses to be directed here, use the* ***Network*** *setting.*

   d) In the HTTP Pool Member setting, specify the addresses of the back-end application servers.
   e) From the **Logging Profile** list, select a profile such as **Log illegal requests** to determine which events are logged on the system.
7. In the upper right corner, click **Advanced**.

   You can use default values for the Advanced settings but it's a good idea to take a look at them.

   - If you selected **Fundamental** or **Comprehensive** for the **Policy Template**, **Learning Mode** is set to **Automatic** and **Enforcement Mode** is set to **Blocking**.

     Tip: *If you need to change these values, set application language to a value other than* ***Auto detect****.*

   - If you know the **Application Language**, select it or use **Unicode (utf-8)**.
   - To add specific protections (enforcing additional attack signatures) to the policy, for **Server Technologies**, select the technologies that apply to the back-end application servers.
   - You can configure trusted IP addresses that you want the security policy to consider safe.
8. Click **Create Policy** to create the security policy.

ASM™ creates a security policy that immediately starts protecting your application. The enforcement mode of the security policy is set to Blocking. Traffic that is considered to be an attack such as traffic that is not compliant with HTTP protocol, has malformed payloads, uses evasion techniques, performs web scraping, contains sensitive information or illegal values is blocked. Other potential violations are reported but not blocked.

The system examines the traffic to the web application making suggestions for more specifically building the security policy. The Policy Builder selectively learns new entities like file types, parameters, and cookies used in requests to the application. When ASM processes sufficient traffic, it automatically adds the entities to the security policy, and enforces them.

The system applies a basic set of attack signatures to the security policy and puts them in staging (by default, for 7 days). If you specified server technologies, additional attack signatures are included. ASM reports common attacks discovered by comparison to the signatures but does not block these attacks until the staging period is over and they are enforced. That gives you a chance to be sure that these are actual attacks and not legitimate requests.

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

How the security policy is built

When you create a security policy, you have a basic security policy that immediately starts 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 Traffic Learning screen, 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 most 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**. Traffic with obvious violations is blocked right away.
- 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 removes 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.
- After a while, 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 generally how the system automatically builds security policies. 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. Also, you have the option of changing the learning mode to **Manual**.

Reviewing learning suggestions

Before you can see learning suggestions on the system, it needs to have had some traffic sent to it.

After you create a security policy and begin sending traffic to the application, the system provides learning suggestions concerning additions to the security policy based on the traffic it sees. 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. Take a look at the Traffic Learning screen to get familiar with it.

   With no suggestions selected, the right pane displays sections that facilitate the reviewer decision-making process. These include graphical charts that summarize policy activity, a summary of top violations in **Reduce Potential False-positive Alerts**, an enforcement readiness summary and a summary of suggestions to add new entity or delete an obsolete entity.
3. 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. Click the search icon to see basic and advanced filters.
4. Review the learning suggestions as follows.
   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) Select a suggestion to learn more about what caused it by looking at the action, the number of samples it is based on, the violations caused and their violation ratings, and if available, by examining samples of the requests that caused the suggestion.
   c) Select a request to view data about the request on the right, including any violations it generated, the contents of the request itself, and the response (if any).

      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  to the right of the suggestion commands, and type the comments.
5. Decide how to respond to the suggestion. You can start with the suggestions that have 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.

Note: *If you are working in automatic learning mode, when the learning score reaches 100%, the system can accept most of the suggestions if you selected the Learning Mode Auto-apply Policy, 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.

6. 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 making sure that users can access the application. 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 may have a large impact on the policy or 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. In these cases, 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.

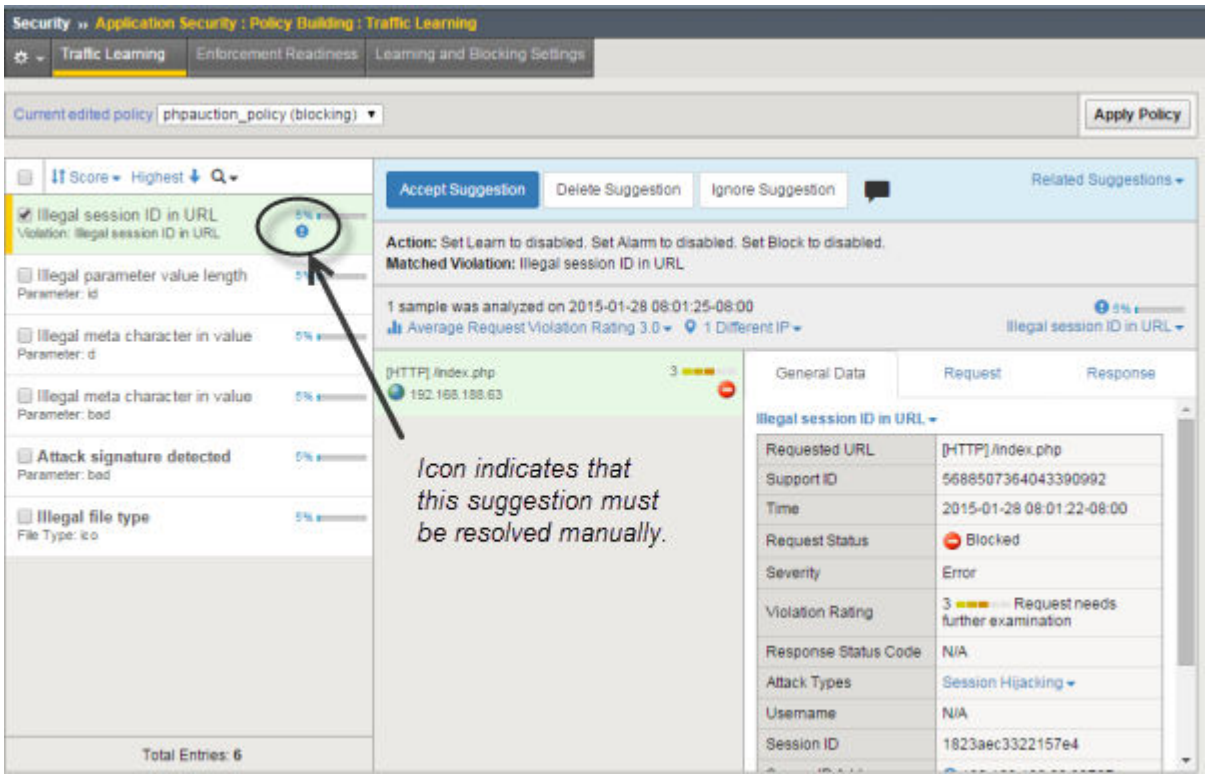

Figure 1: Suggestions that must be resolved manually

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. For example, you can update attack signatures if new ones are available.
   - 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, Cookies, or Redirection Domains column of a security policy to see details about these policy elements.

- Click the Real Traffic Policy Builder® column to view the learning suggestions for the policy.

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 for a security policy. Some of these protections are automatically enabled depending on the type of security policy you create.

Feature	Description and Location
DoS attack prevention	Prevents Denial of Service (DoS) attacks based on latency and/or transaction rates (also using behavioral analysis, geolocation, CAPTCHA challenge, heavy URL detection, proactive web scraping detection, and blacklisting). Click **Security** > **DoS Protection**. You create a DoS profile with Application Security enabled to configure Layer 7 DoS protection.
Brute force prevention	Stops attempts to break in to secured areas of a web application by trying exhaustive, systematic, login combinations. Click **Security** > **Application Security** > **Anomaly Detection** > **Brute Force Attack Prevention**.
IP Intelligence	Logs and blocks attacks from IP addresses that are in the IP Intelligence Database and are considered to have a bad reputation. Click **Security** > **Application Security** > **IP Addresses** > **IP Intelligence**.
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**.
Geolocation enforcement	Lets you specify countries from which users can and cannot access the web application. To set geolocation restrictions, click **Security** > **Application Security** > **Geolocation Enforcement**.
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	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**.

Creating Parent and Child Security Policies

Overview: Creating parent and child security policies

You can use Application Security Manager™ (ASM) to create two layers of security policies: parent policies and child policies. Parent policies include mandatory policy elements, and child policies inherit those attributes from the parent. When the parent policy is updated, its child policies are automatically updated.

Parent policies let you

- Create and maintain common elements and settings
- Impose mandatory elements on child policies
- Push a change to multiple child policies

You can specify which parts of the security policy must be inherited, which are optional, and which are not inherited. This way, you can keep child policies in sync with the changes in the global mandatory policies and still allow the child policies to address their own unique requirements. The inheritance follows the sections of the policy in the Learning and Blocking Settings: each part can be inherited or not inherited from the parent.

Creating a parent security policy

Parent security policies include features that you want to apply to multiple child security policies that can inherit those features.

1. On the Main tab, click **Security** > **Application Security** > **Security Policies** > **Policies List**.
   The Policies List screen opens.
2. Click **Create New Policy**.

   You only see this button when no policy is selected.
3. In the **Policy Name** field, type a name for the policy.
4. For **Policy Type**, select **Parent**.
5. For **Policy Template**, select the template that you want to use for the parent policy, for example, select **Fundamental** to create a robust yet compact security policy that is appropriate for most applications.

   To create a stricter policy that enforces many violations, select **Comprehensive** instead.
6. In the upper right corner, click **Advanced**.
7. To use automatic policy building for this policy and child policies, leave the **Learning Mode** set to **Automatic**.
8. For **Application Language**, leave the default of **Unicode (utf-8)** unless all child policies will use a specific language that you can select.

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

   ---
9. To enable specific protections that will apply to this policy and its child policies, for **Server Technologies**, select as many of the technologies as are relevant to the back-end servers.
   The system adds attack signatures specific to the selected technologies.
10. For **Trusted IP Addresses**, select which IP addresses to consider safe by all child policies.

Option	Description
All	Specifies that the policy trusts all IP addresses. This option is recommended only 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.

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

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.
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.
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.

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.

12. For the **Signature Staging** setting, verify that the default option **Enabled** is selected.
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. For the **Enforcement Readiness Period**, retain the default setting of 7 days.

This is how long entities remain in staging. 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.

14. If the application is not case-sensitive, disable the **Policy is Case Sensitive** check box. Otherwise, leave it selected.

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

---

15. If you do not want the security policy to distinguish between HTTP/WebSocket and HTTPS/WebSocket Secure URLs, for **Differentiate between HTTP/WS and HTTPS/WSS URLs**select **Disabled**.
16. Click **Create Policy** to create the security policy.

The system creates the parent security policy and displays the inheritance settings for each section of the policy (as on the Learning and Blocking Settings screen).

17. For each of the **Inheritance Settings**, decide whether you want inheritance to child policies to be **Mandatory** (child inherits the settings), **Optional** (the child can decide), or **None** (no inheritance for this feature). When done, click **Save Changes**.

You have created a security policy that you can use as a parent policy for multiple child policies. The child policies inherit the settings from this parent policy, and you can change only a subset of the settings in the child policy. Future changes made to the parent policy are passed down to the child policies.

Configuring parent policy settings

After you create a parent security policy, you can review and adjust the policy settings to be sure they include the correct details that you want to use for child policies. Although this task is not required and the default values may suit your needs, it gets you familiar with the settings in the policy. This is the same process to follow if later you need to make changes to the parent policy and how it works.

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 security policy** list near the top of the screen, verify that the policy shown is the parent security policy you want to work on.
3. On the right side of the Learning and Blocking Settings screen, select **Advanced**.
   The screen displays the advanced configuration details for the parent security policy.
4. For each of the settings, on the right you can see whether the setting has **Mandatory Inheritance**, **Optional Inheritance**, or **No Inheritance**.
5. Expand each of the settings and review the default values for each of the areas. Adjust the values, if necessary. If you change any of the values, click **Save**, then **Apply Policy**.

   Tip: *Descriptions of the settings are included in the online Help on the Help tab.*

6. On the Main tab, click **Security** > **Application Security** > **Security Policies** > **Policies List**.
   The Policies List screen opens.
7. In the Policies List, select the parent policy you previously created.
   The policy summary is displayed on the right.
8. Click **Inheritance Settings**.
9. Review the **Inheritance Settings**, and make sure that inheritance is set properly for child policies to be **Mandatory** (child inherits the settings), **Optional** (the child can decide), or **None** (no inheritance for this feature). When done, click **Save Changes**.

You have configured the security policy settings of the parent policy that you can use when creating child security policies. If you already have created child policies, when you save the changes to the parent policy, the changes are automatically made to the child policies.

Creating a child security policy

Child security policies inherit settings from a parent security policy.

1. On the Main tab, click **Security** > **Application Security** > **Security Policies** > **Policies List**.
   The Policies List screen opens.
2. Click **Create New Policy**.

   You only see this button when no policy is selected.
3. In the **Policy Name** field, type a name for the policy.
4. For **Policy Type**, select **Security**.

5. For **Policy Template**, select the template to use for the child policy, for example, select **Fundamental** to create a robust security policy that is appropriate for most applications.

   To create a strict security policy that enforces many violations, select **Comprehensive** instead.
6. From the **Parent Policy** list, select the parent security policy to use for this policy.
7. For **Virtual Server**, select an existing virtual server, click **Configure new virtual server** to to specify where to direct application requests, or leave it set to **None** for now.
   - Existing virtual servers are only listed if they have an HTTP profile, and are not associated with a local traffic policy.
   - To create a new virtual server, specify the protocol, virtual server name, virtual server destination IP address/network and port (IPv4 or IPv6), pool member address and port (address of the back-end application server), and logging profile.
   - If you select **None**, you will have to manually associate the security policy with a virtual server with an HTTP profile at a later time to activate the policy. (On the Security tab of the virtual server, set **Application Security Policy** to **Enabled**, then select the policy.)
8. In the upper right corner, click **Advanced**.

   You can use default values for the Advanced settings but it's a good idea to take a look at them.
   - If you selected **Fundamental** or **Comprehensive** for the **Policy Template**, **Learning Mode** is set to **Automatic** and **Enforcement Mode** is set to **Blocking**.

     Tip: *If you need to change these values, set application language to a value other than **Auto detect**.*
   - If you know the **Application Language**, select it or use **Unicode (utf-8)**.
   - To add specific protections (enforcing additional attack signatures) to the policy, for **Server Technologies**, select the technologies that apply to the back-end application servers.
   - You can configure trusted IP addresses that you want the security policy to consider safe.
9. Click **Create Policy** to create the security policy.
10. Click **Inheritance Settings** to see which parts of the policy are inherited from the parent and which can be declined or accepted.

    By default, all settings with optional inheritance are accepted.
11. You can adjust option settings from **Accepted** to **Decline**. When done, click **Save Changes**.

ASM™ creates a child security policy that uses the mandatory settings specified in the parent policy. As a result, some of the Learning and Blocking Settings are unavailable in the child policy, and you can only change them in the parent policy.

The security policy immediately starts protecting your application. The enforcement mode of the security policy is set to Blocking. Traffic that is considered to be an attack such as traffic that is not compliant with HTTP protocol, has malformed payloads, uses evasion techniques, performs web scraping, contains sensitive information or illegal values is blocked. Other potential violations are reported but not blocked.

Tip: *This is a good point at which send some traffic to test that you can access the application being protected by the child security policy and check that traffic is being processed correctly by the BIG-IP® system. Send the traffic to the virtual server destination address.*

If the parent is changed, the child policy is automatically updated with the latest inherited (or accepted) settings.

Reviewing learning suggestions for parent and child policies

Before you can see learning suggestions on the system, the application protected by a child policy needs to have had some traffic sent to it.

After you create parent and child policies and begin sending traffic to the application protected by the child policy, the system provides learning suggestions concerning additions to the policies based on the traffic it sees. 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 parent and child policies to better suit the traffic and secure the application.

Suggestions related to settings that are inherited appear locked in the child policy and can only be accepted in the parent policy.

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. Take a look at the Traffic Learning screen to get familiar with it.

   With no suggestions selected, graphical charts summarize policy activity and you see an enforcement readiness summary on the bottom right.

   Learning suggestions in the parent policy include a number on the right that shows how many of the child policies included that suggestion. A link lets you review the suggestion in the child policy.
3. Review the learning suggestions as follows.
   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 available, 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  to the right of the suggestion commands, and type the comments.
4. Decide how to respond to the suggestions. You can start with the suggestions that have 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. ***Note:*** *For suggestions concerning inherited settings, this option only appears in the parent policy.* Suggestions about adding file types, URLs, parameters, cookies, or redirection domains can only be accepted in child policies.
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.

Option	What happens
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**.

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**.

Using Rapid Deployment to Create a Security Policy

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** > **Policies List**.
   The Policies List screen opens.
2. Click **Create New Policy**.
   You only see this button when no policy is selected.
3. In the **Policy Name** field, type a name for the policy.
4. Leave **Policy Type**, set to **Security**.
5. For **Policy Template**, select **Rapid Deployment Policy**.
6. For **Virtual Server**, click **Configure new virtual server** to specify where to direct application requests.

a) For **What type of protocol does your application use?**, select **HTTP**, **HTTPS**, or both.
b) In the **Virtual Server Name** field, type a unique name.
c) In the **HTTP Virtual Server Destination** field, type the address in IPv4 (`10.0.0.1`) or IPv6 (`2001:ed8:77b5:2:10:10:100:42/64`) format, and specify the service port.

Tip: *If you want multiple IP addresses to be directed here, use the* ***Network*** *setting.*

---

d) In the HTTP Pool Member setting, specify the addresses of the back-end application servers.
e) From the **Logging Profile** list, select a profile such as **Log illegal requests** to determine which events are logged on the system.

7. In the upper right corner, click **Advanced**.

   You can use default values for the Advanced settings but it's a good idea to take a look at them.

   - Leave **Learning Mode** set to **Manual** and **Enforcement Mode** set to **Transparent**
   - If you know the **Application Language**, select it or use **Unicode (utf-8)**.
   - To add specific protections (enforcing additional attack signatures) to the policy, select the server technologies that apply to the backend application servers.

8. Click **Create Policy** to create the security policy.

The system creates a simple security policy that protects against known security problems, 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 and enforce the policy). 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

Before you can see learning suggestions on the system, it needs to have had some traffic sent to it.

After you create a security policy and begin sending traffic to the application, the system provides learning suggestions concerning additions to the security policy based on the traffic it sees. 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. Take a look at the Traffic Learning screen to get familiar with it.

   With no suggestions selected, the right pane displays sections that facilitate the reviewer decision-making process. These include graphical charts that summarize policy activity, a summary of top violations in **Reduce Potential False-positive Alerts**, an enforcement readiness summary and a summary of suggestions to add new entity or delete an obsolete entity.
3. 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. Click the search icon to see basic and advanced filters.
4. Review the learning suggestions as follows.
   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) Select a suggestion to learn more about what caused it by looking at the action, the number of samples it is based on, the violations caused and their violation ratings, and if available, by examining samples of the requests that caused the suggestion.

c) Select a request to view data about the request on the right, including any violations it generated, the contents of the request itself, and the response (if any).

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  to the right of the suggestion commands, and type the comments.

5. Decide how to respond to the suggestion. You can start with the suggestions that have 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.

Note: *If you are working in automatic learning mode, when the learning score reaches 100%, the system can accept most of the suggestions if you selected the Learning Mode Auto-apply Policy, 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.

---

6. 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 making sure that users can access the application. 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 security policy** list near the top of the screen, verify that the security policy shown is the one you want to work on.
3. For the **Enforcement Mode** setting, select **Blocking**.
4. To see the Policy Building Settings, in the upper right corner, click **Advanced**.
5. 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.

6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

When 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 Vulnerability Assessment Tools with a Security Policy

Overview: Vulnerability assessment policy building

Application Security Manager™ (ASM) integrates with current versions of services that perform vulnerability assessments of web applications, such as:

- HP WebInspect
- IBM® AppScan®
- Qualys®
- Quotium Seeker®
- Trustwave ® App Scanner
- WhiteHat Sentinel

ASM™ also provides a generic scanner so you can use other vulnerability assessment tools not explicitly supported. 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 policy template to create a baseline security policy and integrate it 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 previously created, you can also incorporate use of a vulnerability assessment tool with that policy.

Task summary

Creating a security policy using the vulnerability assessment template
Associating a vulnerability assessment tool with an existing security policy
Creating a WhiteHat vulnerability file
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 the vulnerability assessment template

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 according to the needs of your networking environment.

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

1. On the Main tab, click **Security** > **Application Security** > **Security Policies** > **Policies List**.
   The Policies List screen opens.
2. Click **Create New Policy**.

   You only see this button when no policy is selected.

3. In the **Policy Name** field, type a name for the policy.
4. Leave **Policy Type**, set to **Security**.
5. For **Policy Template**, select **Vulnerability Assessment Baseline**.
6. For **Virtual Server**, click **Configure new virtual server** to specify where to direct application requests.
   a) For **What type of protocol does your application use?**, select **HTTP**, **HTTPS**, or both.
   b) In the **Virtual Server Name** field, type a unique name.
   c) In the **HTTP Virtual Server Destination** field, type the address in IPv4 (`10.0.0.1`) or IPv6 (`2001:ed8:77b5:2:10:10:100:42/64`) format, and specify the service port.

   Tip: *If you want multiple IP addresses to be directed here, use the* ***Network*** *setting.*

   d) In the HTTP Pool Member setting, specify the addresses of the back-end application servers.
   e) From the **Logging Profile** list, select a profile such as **Log illegal requests** to determine which events are logged on the system.
7. Click **Create Policy** to create the security policy.

The system creates a baseline security policy for your web application with the enforcement mode set to blocking, and the learning mode set to manual. The policy already protects against malformed HTTP protocol, evasion techniques, and CSRF attacks. But it does not yet protect against the vulnerabilities found by the scanner.

Next, you need to associate the scanner, then import, review, and resolve vulnerabilities so that the security policy protects against them.

Associating a vulnerability assessment tool with an existing security policy

After creating a security policy using the vulnerability assessment template, you can associate a vulnerability assessment tool with 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 security policy** list near the top of the screen, verify that the security policy shown 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. For WhiteHat Sentinel only, complete these options:
   a) 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.
   b) 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.

c) 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.

d) Click **Site Mapping Settings** to indicate what traffic information to send to the scanner based on response codes, trusted IP addresses, and rules defining what traffic should be considered legitimate.

5. If using the Generic Scanner, click **Download Generic Schema** to download the `generic_scanner.xsd` file.
6. To associate the selected vulnerability assessment tool with the security policy, click **Save**.
7. 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.

Creating a WhiteHat vulnerability file

Before you can develop a vulnerability scan file using 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

This procedure explains how to create a WhiteHat vulnerability file 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 a WhiteHat vulnerability scan file that you can import into a security policy. 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.

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 for the web application you want to protect in the form of a standard XML file.

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

1. On the Main tab, click **Security** > **Application Security** > **Vulnerability Assessments** > **Vulnerabilities**.
   The Vulnerabilities screen opens.
2. In the **Current edited security policy** list near the top of the screen, verify that the security policy shown 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 details on the screen.

   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** > **Vulnerabilities**.
   The Vulnerabilities screen opens.
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	What it displays
All	All vulnerabilities found by the scanner.
Resolvable	All vulnerabilities that are resolvable either automatically or manually.
Resolvable (Automatically)	Vulnerabilities that ASM can resolve.
Resolvable (Manually)	Vulnerabilities that can be resolved with some manual intervention.

View option	What it displays
Not Resolvable	Vulnerabilities that are not resolvable in any straightforward way.

Vulnerabilities with option	What it displays
Any	Vulnerabilities in any state.
Ignored	Vulnerabilities that you decided to ignore by selecting and clicking **Ignore**.
Mitigated	Vulnerabilities that ASM has mitigated, or those which have been fixed and marked as mitigated.
Pending	Vulnerabilities that need to be dealt with.
Mitigated (In Staging)	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	What it does
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	What it does
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.

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

Before you can see learning suggestions on the system, it needs to have had some traffic sent to it.

After you create a security policy and begin sending traffic to the application, the system provides learning suggestions concerning additions to the security policy based on the traffic it sees. 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. Take a look at the Traffic Learning screen to get familiar with it.

   With no suggestions selected, the right pane displays sections that facilitate the reviewer decision-making process. These include graphical charts that summarize policy activity, a summary of top violations in **Reduce Potential False-positive Alerts**, an enforcement readiness summary and a summary of suggestions to add new entity or delete an obsolete entity.
3. 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. Click the search icon to see basic and advanced filters.
4. Review the learning suggestions as follows.
   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) Select a suggestion to learn more about what caused it by looking at the action, the number of samples it is based on, the violations caused and their violation ratings, and if available, by examining samples of the requests that caused the suggestion.
   c) Select a request to view data about the request on the right, including any violations it generated, the contents of the request itself, and the response (if any).

   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  to the right of the suggestion commands, and type the comments.
5. Decide how to respond to the suggestion. You can start with the suggestions that have 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**

Option	What happens
	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.

Note: *If you are working in automatic learning mode, when the learning score reaches 100%, the system can accept most of the suggestions if you selected the Learning Mode Auto-apply Policy, 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.

---

6. 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 making sure that users can access the application. 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 may have a large impact on the policy or 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. In these cases, 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.

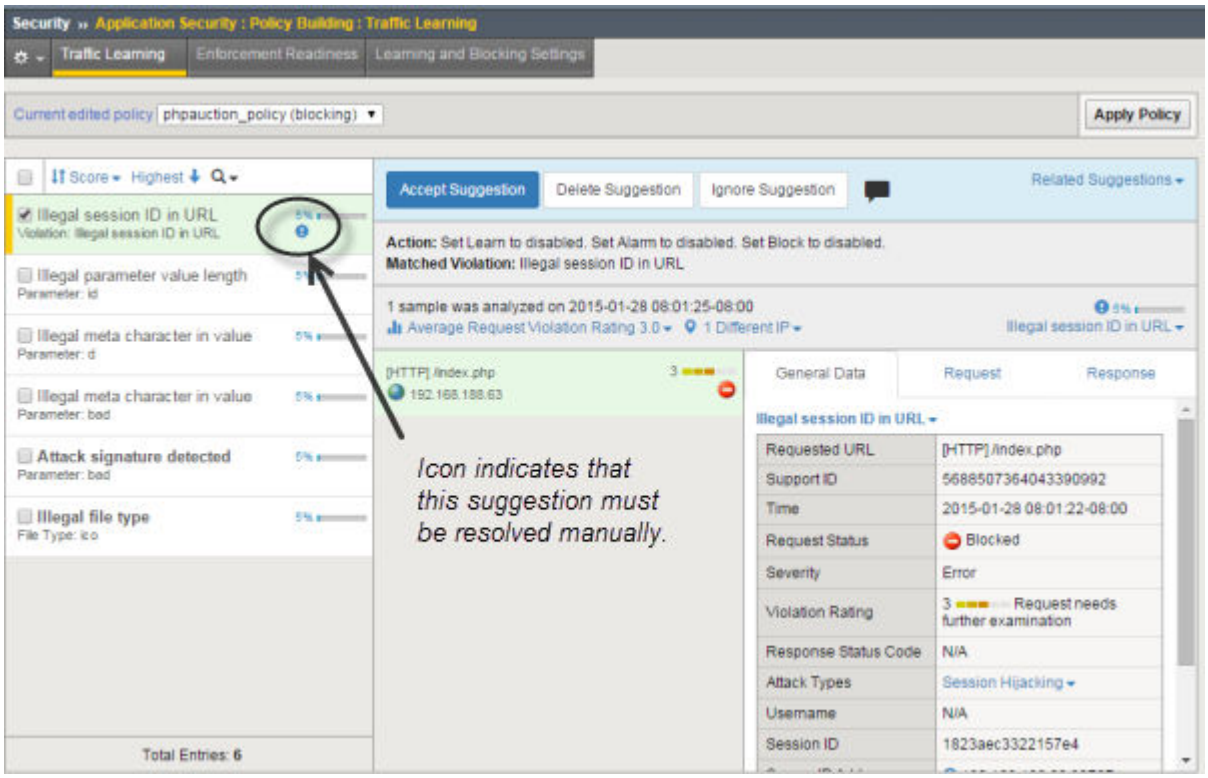

Figure 2: Suggestions that must be resolved manually

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 security policy** list near the top of the screen, verify that the security policy shown is the one you want to work on.
3. For the **Enforcement Mode** setting, select **Blocking**.
4. To see the Policy Building Settings, in the upper right corner, click **Advanced**.
5. 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.

6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

When 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
- Microsoft SharePoint® 2003, 2007, 2010

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.

Creating a security policy from an application template

Before you can create a security policy, you must perform the minimal system configuration tasks required according to the needs of your networking environment.

To quickly create a security policy for one of the commonly used enterprise applications (such as OWA Exchange, Oracle, PeopleSoft, SAP, SharePoint, ActiveSync, or LotusDomino), you can use an application-ready template to create a policy tailored to that application.

1. On the Main tab, click **Security** > **Application Security** > **Security Policies** > **Policies List**.
   The Policies List screen opens.
2. Click **Create New Policy**.

   You only see this button when no policy is selected.
3. In the **Policy Name** field, type a name for the policy.
4. Leave **Policy Type**, set to **Security**.
5. For **Policy Template**, select the application ready template for your application.
6. For **Virtual Server**, select an existing virtual server, click **Configure new virtual server** to to specify where to direct application requests, or leave it set to **None** for now.
   - Existing virtual servers are only listed if they have an HTTP profile, and are not associated with a local traffic policy.
   - To create a new virtual server, specify the protocol, virtual server name, virtual server destination IP address/network and port (IPv4 or IPv6), pool member address and port (address of the back-end application server), and logging profile.
   - If you select **None**, you will have to manually associate the security policy with a virtual server with an HTTP profile at a later time to activate the policy. (On the Security tab of the virtual server, set **Application Security Policy** to **Enabled**, then select the policy.)
7. In the upper right corner, click **Advanced**.

   You can use default values for the Advanced settings but it's a good idea to take a look at them.

- Leave **Learning Mode** set to **Disabled** and **Enforcement Mode** set to **Transparent**
- If you know the **Application Language**, select it or use **Unicode (utf-8)**.

8. Click **Create Policy** to create the security policy.

The system creates a security policy that is tailored to your enterprise application. When first created, the security policy operates in transparent mode (meaning that it does not block traffic). If 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

Before you can see learning suggestions on the system, it needs to have had some traffic sent to it.

After you create a security policy and begin sending traffic to the application, the system provides learning suggestions concerning additions to the security policy based on the traffic it sees. 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. Take a look at the Traffic Learning screen to get familiar with it.

   With no suggestions selected, the right pane displays sections that facilitate the reviewer decision-making process. These include graphical charts that summarize policy activity, a summary of top violations in **Reduce Potential False-positive Alerts**, an enforcement readiness summary and a summary of suggestions to add new entity or delete an obsolete entity.
3. 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. Click the search icon to see basic and advanced filters.
4. Review the learning suggestions as follows.
   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) Select a suggestion to learn more about what caused it by looking at the action, the number of samples it is based on, the violations caused and their violation ratings, and if available, by examining samples of the requests that caused the suggestion.
   c) Select a request to view data about the request on the right, including any violations it generated, the contents of the request itself, and the response (if any).

      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  to the right of the suggestion commands, and type the comments.
5. Decide how to respond to the suggestion. You can start with the suggestions that have 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.

Note: *If you are working in automatic learning mode, when the learning score reaches 100%, the system can accept most of the suggestions if you selected the Learning Mode Auto-apply Policy, 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.

---

6. 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 making sure that users can access the application. 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 security policy** list near the top of the screen, verify that the security policy shown is the one you want to work on.
3. For the **Enforcement Mode** setting, select **Blocking**.
4. To see the Policy Building Settings, in the upper right corner, click **Advanced**.

5. 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.

6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

When 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.

Performing Basic ASM 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 add HTTP pool members to the virtual server 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 ASM systems, you can create a virtual server 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 use Application Security Manager™ (ASM) 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
Creating a self IP address for a VLAN

Creating a local traffic pool for application security
Creating a virtual server

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. If you want to use Q-in-Q (double) tagging, use the **Customer Tag** setting to perform the following two steps. If you do not see the **Customer Tag** setting, your hardware platform does not support Q-in-Q tagging and you can skip this step.
   a) From the **Customer Tag** list, select **Specify**.
   b) Type a numeric tag, from 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. For the **Hardware SYN Cookie** setting, select or clear the check box.

   When you enable this setting, the BIG-IP system triggers hardware SYN cookie protection for this VLAN.

   Enabling this setting causes additional settings to appear. These settings appear on specific BIG-IP platforms only.
8. For the **Syncache Threshold** setting, retain the default value or change it to suit your needs.

   The **Syncache Threshold** value represents the number of outstanding SYN flood packets on the VLAN that will trigger the hardware SYN cookie protection feature.

   When the **Hardware SYN Cookie** setting is enabled, the BIG-IP system triggers SYN cookie protection in either of these cases, whichever occurs first:

   - The number of TCP half-open connections defined in the LTM® setting **Global SYN Check Threshold** is reached.
   - The number of SYN flood packets defined in this **Syncache Threshold** setting is reached.
9. For the **SYN Flood Rate Limit** setting, retain the default value or change it to suit your needs.

   The **SYN Flood Rate Limit** value represents the maximum number of SYN flood packets per second received on this VLAN before the BIG-IP system triggers hardware SYN cookie protection for the VLAN.
10. 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 network mask for the specified IP address.

   For example, you can type `255.255.255.0`.
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: *Instead of doing it now, you can optionally create a pool if creating a virtual server during security policy creation.*

---

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 also create a virtual server as part of creating a security policy. However, creating it this way allows you to see additional options available. This procedure describes the minimum settings required.*

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/Mask** 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**.

   Important: *If your networking configuration uses a proxy server, the specified* ***http*** *profile must have the* ***Accept XFF*** *setting enabled for the system to inspect XFF headers. You can locate the profile in* ***Local Traffic*** > ***Profiles*** > ***Services*** > ***HTTP****.*
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.

Legal Notices

Legal notices

Legal notices

Publication Date

This document was published on November 13, 2017.

Publication Number

MAN-0285-13

Copyright

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks*.

All other product and company names herein may be trademarks of their respective owners.

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.

Legal Notices

Index

T

V

W