BIG-IP® Application Security Manager™: Getting Started Guide

Version 11.2

IT agility. Your way.

Table of Contents

Legal Notices

Publication Date

This document was published on May 7, 2012.

Publication Number

MAN-0285-05

Copyright

Trademarks

Patents

This product may be protected by U.S. Patent 6,311,278. This list is believed to be current as of May 7, 2012.

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.

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, http://www.and.com.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

This product includes software developed by Balazs Scheidler (bazsi@balabit.hu), which is protected under the GNU Public License.

This product includes software developed by Niels Mueller (nisse@lysator.liu.se), which is protected under the GNU Public License.

In the following statement, *This software* refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with 386BSD and similar operating systems. *Similar operating systems* includes mainly non-profit oriented systems for research and education, including but not restricted to NetBSD, FreeBSD, Mach (by CMU).

This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at http://www.perl.com.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes RRDtool software developed by Tobi Oetiker (http://www.rrdtool.com/index.html) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License (GPL).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (http://www.nominum.com).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

This product contains software developed by MaxMind LLC, and is protected under the GNU Lesser General Public License, as published by the Free Software Foundation.

This product includes the Zend Engine, freely available at http://www.zend.com.

This product contains software developed by NuSphere Corporation, which is protected under the GNU Lesser General Public License.

This product contains software developed by Erik Arvidsson and Emil A Eklund.

This product contains software developed by Aditus Consulting.

This product contains software developed by Dynarch.com, which is protected under the GNU Lesser General Public License, version 2.1 or above.

This product contains software developed by InfoSoft Global (P) Limited.

This product includes software written by Steffen Beyer and licensed under the Perl Artistic License and the GPL.

Acknowledgments

Chapter 1

Performing Basic Configuration Tasks

Topics:

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™.

HTTP class profile	An HTTP class profile with application security enabled on it. The class determines which traffic the Application Security Manager inspects. When you create a security policy, the system automatically creates an HTTP class.
pool	A pool contains the web server or application server resources which host the web application that you want to protect with a security policy. You can create a local traffic pool, and then assign the pool to a virtual server. On Application Security Manager systems, you can create a pool as part of creating a security policy.
self IP address	An IP address that you associate with a VLAN, to access hosts in that VLAN. You create a self IP address and associate it with a VLAN.
virtual server	The virtual server processes incoming traffic for the web application you are securing. When you create a virtual server, you assign the HTTP class and pool to it. On Application Security Manager systems, you can create a virtual server, pool, and HTTP class 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. You can use a VLAN to logically group devices that are on different network segments.

About basic networking configuration tasks

For initial installation, the BIG-IP® hardware includes a hardware setup guide for your platform that you can refer to for details about how to install the hardware in a rack, connect the cables, and run the setup utility.

Next, you must configure the BIG-IP system on your network before you can run the Application Security Manager™ (ASM™) Deployment wizard to create a security policy. Which 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 for the system. During the process of creating a security policy, the system can help you complete other necessary configuration tasks, such as automatically creating an HTTP class with Application Security enabled, and creating a new virtual server and pool. 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 VLAN

VLANs represent a collection of hosts that can share network resources, regardless of their physical location on the network.

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. For the **Interfaces** setting, click an interface number from the **Available** list, and use the Move button to add the selected interface to the **Untagged** list. Repeat this step as necessary.
5. 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**.
   The Self IPs screen opens.
2. Click **Create**.
   The New Self IP screen opens.
3. In the **Name** field, type a unique name for the self IP.
4. In the **IP Address** field, type an IP address.

   This IP address should represent the address space of the VLAN that you specify with the **VLAN/Tunnel** setting.

   The system accepts IP addresses in both the IPv4 and IPv6 formats.
5. In the **Netmask** field, type the network mask for the specified IP address.
6. From the **VLAN/Tunnel** list, select the VLAN to associate with this self IP address. If creating a self IP address for an address space:
   - On the internal network, select the VLAN that is associated with an internal interface or trunk.
   - On the external network, select the 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 in the list.

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

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.

Chapter 2

Creating a Security Policy Automatically

Topics:

Overview: Automatic policy building

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

Deployment scenarios when creating security policies

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

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

Deployment scenario	Description
	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.

Creating a security policy automatically

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

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

1. On the Main tab, click **Application Security** > **Security Policies**.
   The Active Policies screen opens.
2. Click the **Create** button.
   The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.
3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.
   - Select **Existing Virtual Server** and click **Next** to use an existing virtual server (as long as it does not have an HTTP Class profile associated with it).
   - Select **New Virtual Server** and click **Next** to create a new virtual server and pool with basic configuration settings.

   The virtual server represents the web application you want to protect. The system automatically creates an HTTP Class with the same name as the virtual server.

   The Configure Local Traffic Settings screen opens.
4. Configure the new or existing virtual server, and click **Next**.
   The Select Deployment Scenario screen opens.
5. For **Deployment Scenario**, select **Create a policy automatically** and click **Next**.
   The Configure Security Policy Properties screen opens.
6. From the **Application Language** list, select the language encoding of the application, or select **Auto detect** and let the system detect the language.

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

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

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

8. Click **Next**.
   The Configure Attack Signatures screen opens.
9. To configure attack signatures, move the systems used by your web application from the **Available Systems** list into the **Assigned Systems** list.
   The system adds the attack signatures needed to protect the selected systems.

10. For the **Signature Staging** setting, verify that the default option **Enabled** is selected.

    Note: *Because the Real Traffic Policy Builder® begins building the security policy in Blocking mode, it is a good idea to keep signature staging enabled to make sure that false positives do not occur.*

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

11. Click **Next**.
    The Configure Automatic Policy Building screen opens.

12. For **Policy Type**, select an option to determine the security features to include in the policy.

Options	Description
Fundamental	Creates a security policy enforcing HTTP request protocol compliance, evasion techniques, allowed file types (including length checks), attack signatures, the violation Request Length Exceeds Defined Buffer Size, and host names.
Enhanced	Creates a security policy with all the elements of the **Fundamental** policy type; also checks for global parameters (including length checks), cookies, and allowed methods to the security policy.
Comprehensive	Creates a security policy with all the elements of the **Enhanced** policy type; also checks for allowed URLs, meta characters on URLs, meta characters on parameters, URL parameters (instead of global parameters), and dynamic parameters.

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

13. For **Rules**, move the slider to set the Policy Builder learning speed.

Option	Description
Fast	Use for a small number of requests from a small number of sessions; for example, useful for web sites with less traffic. However, there is a greater chance of adding false entities to the security policy.
Medium	Use for 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.
Slow	Use for a large number of requests from many sessions; for example, useful for web sites with lots of traffic. This option creates the most accurate security policy, but takes Policy Builder longer to collect the statistics.

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

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

Options	Description
All	Specifies that the policy trusts all IP addresses. For example, if the traffic is in a corporate lab or preproduction environment where all of the traffic is trusted; the policy is created faster.
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.

15. If you want the security policy to automatically detect JSON and XML protocols, select the **JSON/XML payload detection** check box.

    This option is available only for the **Enhanced** and **Fundamental** policy types.

    If requests contain legitimate XML or JSON data, the Policy Builder creates content profiles in the security policy according to the data it detects.
16. If you want to display a response page when an AJAX request does not meet the security policy, select the **AJAX blocking response behavior** check box.
17. Click **Next**.
    The Security Policy Configuration Summary opens where you can review the settings to be sure they are correct.
18. Click **Finish** to create the security policy.
    The Automatic Policy Building Status screen opens where you can view the current state of the security policy.

The Policy Builder starts and automatically begins building the security policy by examining the traffic to the web application. The system sets the enforcement mode of the security policy to Blocking, but it does not block requests until the Policy Builder processes sufficient traffic, adds elements to the security policy, and enforces the elements.

Tip: *This is a good point at which to test that you can access the application being protected by the security policy.*

How the security policy is built

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

The Policy Builder builds the security policy as follows:

- Adds policy elements and updates their attributes when ASM sees enough traffic from various users
- Examines application content and creates XML or JSON profiles as needed (if the policy includes JSON/XML payload detection)
- Configures attack signatures in the security policy
- Stabilizes the security policy when sufficient sessions over a period of time include the same elements
- Includes new elements if the site changes

The Policy Builder automatically discovers and populates the security policy with the policy elements (such as file types, URLs, parameters, and cookies). As the Policy Builder runs, you see status messages in the identification and messages area at the top of the screen. You can monitor general policy building progress, and see the number of elements that are included in the policy.

Automatic policy building characteristics

When you create a security policy using automatic policy building, it has the following characteristics:

- The security policy starts out loose, allowing traffic, then the Policy Builder adds policy elements based on evaluating the traffic.
- The system sets the enforcement mode of the security policy to **Blocking**, but does not block requests until the Policy Builder sees sufficient traffic, adds elements to the security policy, and enforces the elements.
- The system holds attack signatures in staging for 7 days (by default): the system checks, but does not block traffic during the staging period. If a request causes an attack signature violation, the system disables the attack signature for the particular element (parameter, JSON or XML profile, or security policy). After the staging period is over, the Policy Builder can remove all attack signatures from staging if enough traffic from different sessions and different IP addresses was processed. The security policy enforces the enabled signatures and blocks traffic that causes a signature violation.
- The system enforces elements in the security policy when it has processed sufficient traffic and sessions over enough time, from different IP addresses, to determine the legitimacy of the file types, URLs, parameters, cookies, methods, and so on.
- The security policy stabilizes.
- If the web site for the application changes, the Policy Builder initially loosens the security policy then adds policy elements to the security policy, updates the attributes of policy elements, puts the added elements in staging, and enforces the new elements when traffic and time thresholds are met.

Reviewing security policy status

You can monitor the general progress of the Real Traffic Policy Builder®, see what policy elements the system has learned, and view additional details on the Automatic Policy Building Status screen.

1. On the Main tab, click **Application Security** > **Policy Building** > **Automatic** > **Status**.
   The Automatic Policy Building Status screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Review any messages in the identification and messages area to learn what is currently happening on the system.

   For example, messages say when the Policy Builder is enabled, when the security policy was last updated, and the number of elements that were learned.
4. Review the status of the Real Traffic Policy Builder.

Options	Description
Enabled	The system is configured to automatically build a security policy, and the Policy Builder is processing traffic.
Disabled	The system is not processing traffic. Check the automatic policy building configuration.
Detecting Language	The system is still configuring the language after analyzing responses to identify the language of the web application. The Policy Builder is enabled, but it cannot add elements to the security policy until the language is set.

5. Examine the **General Progress** of the security policy.

   A progress bar indicates the stability level of the security policy. The progress bar reaches 100% when the policy is stable, no new policy elements need to be added, and time and traffic thresholds have been reached.

6. In the Policy Elements Learned table, review the number of elements that the Policy Builder has analyzed and added to the security policy, and the attributes that need to be updated.

   Tip: *Click the number in the Elements column to see the specific elements that were added.*

7. Optionally, in the Details tree view, click the expand button for any item to learn more about that security policy element, what the system has seen so far, and what it will take to stabilize the element.

When enough traffic from unique sessions occurs over a period of time, the system starts to enforce the file types and other elements in the security policy. When enforced as part of a stable policy, the files types and other elements are removed from the staging list.

Reviewing outstanding security policy tasks

You can display an overview of all security policies, and review any outstanding tasks that need to be completed. 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 **Application Security** > **Overview**.
   The Overview Summary screen opens.
2. Examine the summary screen for information about recommended tasks that you need to complete.
   - Review the Tasks to do area, which lists system tasks and security policy tasks that should be completed.
   - Click the links to go to the screen where you can perform the recommended action.
   - Review the progress of the Policy Builder for each security policy on which it is enabled.
   - 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 to view Tasks to do, Quick Links, and Policy Builder Progress for that security policy (if Policy Builder is running).
   - Click a number in the File Types, URLs, Parameters, or Cookies column of a security policy to see details about these policy elements.
   - Click the status in the Real Traffic Policy Builder® column to view the automatic security policy building status.

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

About stabilized security policies

This figure shows a security policy that has stabilized, and the Real Traffic Policy Builder® is disabled. The security policy is stable, and the system is enforcing it. To display the status screen shown in the figure: on the Main tab, click **Application Security** > **Policy Building** > **Automatic** > **Status**.

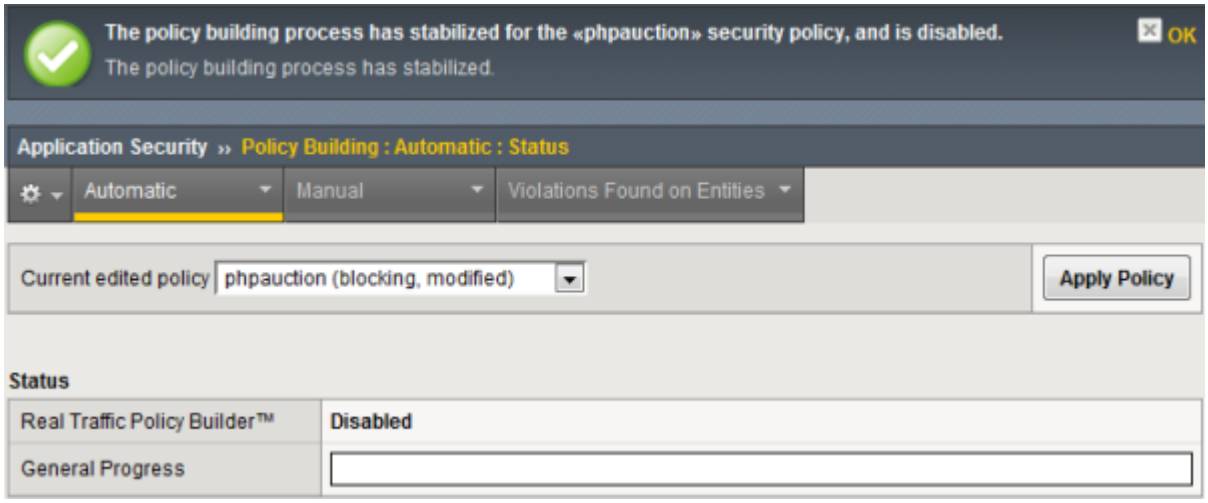

Figure 1: Stabilized security policy screen

About additional application security protections

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

Feature	Description and Location
DoS attack prevention	Prevents Denial of Service (DoS) attacks based on latency and transaction rates. Click **Application Security** > **Anomaly Detection** > **DoS Attack Prevention**.
Brute force attack prevention	Protects the system against illegal login attempts where a hacker tries to log in to a URL numerous times, running many combinations of user names and passwords, until the intruder successfully logs in. Click **Application Security** > **Anomaly Detection** > **Brute Force Attack Prevention**.
IP Enforcement	Prevents attacks performed by specific IP addresses using a violation threshold. Click **Application Security** > **Anomaly Detection** > **IP Enforcer**.
Web scraping detection	Mitigates web scraping (web data extraction) on web sites by attempting to determine whether a web client

Feature	Description and Location
	source is human. Click **Application Security** > **Anomaly Detection** > **Web Scraping**.
CSRF protection	Prevents cross-site request forgery (CSRF) where a user is forced to perform unwanted actions on a web application where the user is currently authenticated. Click **Application Security** > **CSRF Protection**.
Sensitive data masking (Data Guard)	Protects sensitive data in responses such as a credit card number, U.S. Social Security number, or custom pattern. Click **Application Security** > **Data Guard**.
Anti-virus protection through an ICAP server	Configures the system as an Internet Content Adaptation Protocol (ICAP) client so that an external ICAP server can inspect HTTP file uploads for viruses before releasing the content to the web server. To set up the ICAP server, click **Application Security** > **Options** > **Anti-Virus Protection**. To configure anti-virus protection on the security policy, click **Application Security** > **Policy** > **Anti-Virus Protection**.

Chapter 3

Using WhiteHat Sentinel for a Security Policy

Topics:

Overview: Vulnerability assessment policy building

Application Security Manager™ (ASM) integrates with services, such as IBM® Rational® AppScan®, Cenzic® Hailstorm®, and QualysGuard®, as well as WhiteHat Sentinel, that perform vulnerability assessments of web applications. Vulnerability assessment services identify, classify, and report potential security holes or weaknesses in the code of your web site.

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

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

Creating a security policy integrated with WhiteHat Sentinel

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

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

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

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

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

1. On the Main tab, click **Application Security** > **Security Policies**.
   The Active Policies screen opens.
2. Click the **Create** button.
   The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.
3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.
   - Select **Existing Virtual Server** and click **Next** to use an existing virtual server (as long as it does not have an HTTP Class profile associated with it).
   - Select **New Virtual Server** and click **Next** to create a new virtual server and pool with basic configuration settings.

The virtual server represents the web application you want to protect. The system automatically creates an HTTP Class with the same name as the virtual server.

The Configure Local Traffic Settings screen opens.

4. Configure the new or existing virtual server, and click **Next**.
   The Select Deployment Scenario screen opens.
5. For **Deployment Scenario**, select **Create a policy using third party vulnerability assessment tool output** and click **Next**.
6. From the **Application Language** list, select the language encoding of the application and click **Next**.

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

   The Vulnerability Assessments Settings screen opens.
7. From the **Vulnerability Assessment Tool** list, select **WhiteHat Sentinel**.
8. For **WhiteHat Web API Key**, type the key generated and supplied by WhiteHat Sentinel for your web applications.
9. 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.
10. In the **Configure exceptions for the scanner IP Address** setting, specify any IP addresses that you want the security policy to allow, and how to deal with them.
    - Type the IP address and netmask of the scanner.
    - Select the appropriate check boxes for learning suggestions, logging, and blocking traffic from this IP address.
11. Click **Next**.
    The Security Policy Configuration Summary screen opens.
12. Review the settings for the security policy. When you are satisfied with the security policy configuration, click **Finish**.
    The system creates the security policy and opens the Import Vulnerabilities screen specific to the vulnerability assessment tool you are using.
13. Next, import the vulnerabilities from the WhiteHat Sentinel server. For **Import Method**, select how to import a vulnerability report:

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

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

The system creates a baseline security policy for your web application but does not yet protect against the vulnerabilities or enforce the policy.

Note:

When integrating with WhiteHat Sentinel, Application Security Manager has to recognize whether a request is coming from the WhiteHat server. This enables ASM™ to communicate with WhiteHat Sentinel so the WhiteHat portal can mark fixed vulnerabilities as `Mitigated by WAF`*. ASM identifies requests sent by WhiteHat Sentinel using the published source IP of the WhiteHat Sentinel service. However, ASM does not see the original source IP address of requests if ASM is behind a NAT (or NAT firewall), or if you are using a WhiteHat Satellite box. In these configurations, vulnerabilities that ASM protects against are not shown as mitigated in WhiteHat Sentinel.*

To resolve this issue, set one or more of the `WhiteHatIP` *internal parameters to the redirected source IP addresses or subnets. ASM then treats the address as one of the WhiteHat addresses, and sends WhiteHat information on vulnerabilities that ASM has mitigated.*

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

Creating a vulnerability file

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

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

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

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

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

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

   The results of the vulnerability scan appear in the web browser in XML format.
2. Save the results as an XML file.

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

Resolving vulnerabilities

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, Application Security Manager™ (ASM™) configures the security policy to protect against them.

1. On the Main tab, click **Application Security** > **Security Policies**.
   The Active Security Policies list opens.
2. Click the name of the security policy integrated with your vulnerability assessment tool.
   The security policy Properties screen opens.
3. From the Vulnerability Assessments menu, click Vulnerabilities.
   The Vulnerabilities screen opens and lists the vulnerabilities that the vulnerability assessment scan discovered.
4. In the Vulnerabilities Found and Verified area, review the vulnerabilities that the assessment tool has detected and verified.

   Tip: *Click a row in this table to display details about the vulnerability.*

5. For the vulnerabilities that are shown as **Resolvable**, select the vulnerabilities you want the system to resolve (or ignore), and click the appropriate button.

Option	Description
Resolve and Stage	Updates the security policy to protect again 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 again 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**.

   BIG-IP® ASM reviews the prerequisites and then displays a list of the changes it will make to fix the vulnerability.
6. 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, if appropriate.
7. Click **Apply Policy** to save the changes to the security policy.
   The system updates the security policy to prevent the handled vulnerabilities from reoccurring.
8. If using WhiteHat Sentinel, select all of the vulnerabilities you dealt with and click **Retest** to have the WhiteHat Sentinel service verify whether the vulnerability still exists.

The security policy for your web application protects against the vulnerabilities that the vulnerability assessment tool discovered and which you resolved.

You can also review vulnerabilities that ASM cannot resolve automatically, and update the security policy manually to protect against them.

Fine-tuning a security policy

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

Note: *If you are using the Policy Builder to add elements to the security policy, you can skip this task.*

1. On the Main tab, click **Application Security** > **Policy Building** > **Manual**.
   The Traffic Learning screen opens, and lists violations and learning suggestions that the system has found based on real traffic.
2. In the Traffic Learning area, click each violation hyperlink, then review and handle learning suggestions:

Option	Description
Accept	Select a learning suggestion, click **Accept**, and then click **Apply Policy**. The system updates the security policy to allow the file type, URL, parameter, or other element.
Clear	Select a learning suggestion, and click **Clear**. The system removes the learning suggestion and continues to generate suggestions for that violation.
Cancel	Click **Cancel** to return to the Traffic Learning screen.

   By default, a security policy is put into a staging-tightening period for seven days. During this time, you can examine learning suggestions and adjust the security policy without blocking traffic.
3. On the Traffic Learning screen, review the violations and consider whether you want to permit any of them (for example, if a violation is causing false positives). Select any violations you do not want the system to trigger, and click **Disable Violation**.
   A popup screen opens, and you can verify that you want to disable the violations or cancel the action.
4. To activate the updated security policy, on the top right of the screen, click **Apply Policy**, then click **OK** to confirm.
5. To view outstanding tasks for the security policy, on the Main tab, click **Application Security** > **Overview**.
   The Overview Summary screen opens.
6. Examine the summary screen for information about recommended tasks that you need to complete.
   a) Review the Tasks to do area, which lists system tasks and security policy tasks that should be completed.
   b) Click the links in the Tasks to do area to go to the screen where you can perform the recommended action.
   c) In the Quick Links area, click any of the links to gain access to common configuration and reporting screens.

The security policy now 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, or if they are false positives that indicate a need to update the security policy.

Enforcing a security policy

To perform enforcement tasks, the security policy must be operating in transparent mode, and have been created manually. 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 **Application Security** > **Policy** > **Blocking**.
   The Settings screen shows the violations that can be detected, and how the security policy responds to requests that cause those violations (whether the system learns information from the illegal request, generates an alarm, or blocks the request).
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For each violation, review the settings so you understand how the security policy handles requests that cause the violation.

Option	Description
Learn	If selected, the system generates learning suggestions for requests that trigger the violation.
Alarm	If selected, the system records requests that trigger the violation in the Charts screen, the Syslog (`/var/log/asm`), and possibly in local or remote logs (depending on the settings of the logging profile).
Block	If selected (and the enforcement mode is set to **Blocking**), the system blocks requests that trigger the violation.

4. For the **Enforcement Mode** setting, select **Blocking**.
5. Click **Save**.
6. On the Main tab, click **Application Security** > **Policy**.
7. To change the number of days the security policy remains in staging, change the value in the **Staging-Tightening Period** field.

   The security policy does not block traffic during the Staging-Tightening Period even if violations occur. If you want to block traffic that causes violations, set the value of this field to `0`. For details, see the online help.
8. Click **Save**.
9. In the editing context area, click **Apply Policy** to immediately put the changes into effect.
10. For a quick summary of system activity, look at the Overview screen (**Application Security** > **Overview**).

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

Chapter 4

Using Vulnerability Assessment Tools for a Security Policy

Topics:

Overview: Vulnerability assessment policy building

Application Security Manager™ (ASM) integrates with services, such as IBM® Rational® AppScan®, Cenzic® Hailstorm®, and QualysGuard®, as well as WhiteHat Sentinel, that perform vulnerability assessments of web applications. Vulnerability assessment services identify, classify, and report potential security holes or weaknesses in the code of your web site.

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

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

Creating a security policy using vulnerability assessment tool output

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

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

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

1. On the Main tab, click **Application Security** > **Security Policies**.
   The Active Policies screen opens.
2. Click the **Create** button.
   The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.
3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.
   - Select **Existing Virtual Server** and click **Next** to use an existing virtual server (as long as it does not have an HTTP Class profile associated with it).
   - Select **New Virtual Server** and click **Next** to create a new virtual server and pool with basic configuration settings.

   The virtual server represents the web application you want to protect. The system automatically creates an HTTP Class with the same name as the virtual server.

   The Configure Local Traffic Settings screen opens.
4. Configure the new or existing virtual server, and click **Next**.
   The Select Deployment Scenario screen opens.
5. For **Deployment Scenario**, select **Create a policy using third party vulnerability assessment tool output** and click **Next**.
6. From the **Application Language** list, select the language encoding of the application and click **Next**.

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

The Vulnerability Assessments Settings screen opens.

7. From the **Vulnerability Assessment Tool** list, select the vulnerability assessment tool that you use to scan your web application for problems.
8. In the **Configure exceptions for the scanner IP Address** setting, specify any IP addresses that you want the security policy to allow, and how to deal with them.
   a) Type the IP address and netmask of the scanner.
   b) Select the appropriate check boxes for learning suggestions, logging, and blocking traffic from this IP address.
9. Click **Next**.
   The Security Policy Configuration Summary screen opens.
10. Review the settings for the security policy. When you are satisfied with the security policy configuration, click **Finish**.
    The system creates the security policy and opens the Import Vulnerabilities screen specific to the vulnerability assessment tool you are using.
11. In the **Import previously saved vulnerabilities file** field, type the name of the XML file output from the vulnerabilities assessment tool, or browse to the file.

    If using the Cenzic vulnerability assessment tool, additional settings allow you to connect to an existing Cenzic Cloud account, create a trial account, and request a new scan. Refer to the online help for details about the settings.
12. Click **Import**.
    The system imports the vulnerabilities file to the Application Security Manager.

The system creates a baseline security policy for your web application but does not yet protect against the vulnerabilities or enforce the policy.

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

Adding vulnerability assessment to an existing security policy

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

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

1. On the Main tab, click **Application Security** > **Security Policies**.
   The Active Policies screen opens.
2. Click the name of the security policy with which you want to associate a vulnerability assessment tool.
   The Properties screen for the security policy opens.
3. From the Vulnerability Assessments menu, select Settings.
   The Vulnerability Assessments Settings screen opens.
4. From the **Vulnerability Assessment Tool** list, select the vulnerability assessment tool that you use to scan your web application for problems.

Important: *You cannot change the vulnerability assessment tool for a security policy after you import vulnerabilities.*

5. Click **Save**.
6. From the Vulnerability Assessments menu, select Import Vulnerabilities.
   The Import Vulnerabilities screen opens.
7. In the **Import previously saved vulnerabilities file** field, type the name of the XML file output from the vulnerabilities assessment tool, or browse to the file.

   If using the Cenzic vulnerability assessment tool, additional settings allow you to connect to an existing Cenzic Cloud account, create a trial account, and request a new scan. Refer to the online help for details about the settings.
8. Click **Import**.
   The system imports the vulnerabilities file to the Application Security Manager.
9. 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, and imports the vulnerabilities.

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, Application Security Manager™ (ASM™) configures the security policy to protect against them.

1. On the Main tab, click **Application Security** > **Security Policies**.
   The Active Security Policies list opens.
2. Click the name of the security policy integrated with your vulnerability assessment tool.
   The security policy Properties screen opens.
3. From the Vulnerability Assessments menu, click Vulnerabilities.
   The Vulnerabilities screen opens and lists the vulnerabilities that the vulnerability assessment scan discovered.
4. In the Vulnerabilities Found and Verified area, review the vulnerabilities that the assessment tool has detected and verified.

Tip: *Click a row in this table to display details about the vulnerability.*

5. For the vulnerabilities that are shown as **Resolvable**, select the vulnerabilities you want the system to resolve (or ignore), and click the appropriate button.

Option	Description
Resolve and Stage	Updates the security policy to protect again 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.

Option	Description
Resolve	Updates the security policy to protect again 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**.

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

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

The security policy for your web application protects against the vulnerabilities that the vulnerability assessment tool discovered and which you resolved.

You can also review vulnerabilities that ASM cannot resolve automatically, and update the security policy manually to protect against them.

Fine-tuning a security policy

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

Note: *If you are using the Policy Builder to add elements to the security policy, you can skip this task.*

1. On the Main tab, click **Application Security** > **Policy Building** > **Manual**.
   The Traffic Learning screen opens, and lists violations and learning suggestions that the system has found based on real traffic.
2. In the Traffic Learning area, click each violation hyperlink, then review and handle learning suggestions:

Option	Description
Accept	Select a learning suggestion, click **Accept**, and then click **Apply Policy**. The system updates the security policy to allow the file type, URL, parameter, or other element.
Clear	Select a learning suggestion, and click **Clear**. The system removes the learning suggestion and continues to generate suggestions for that violation.
Cancel	Click **Cancel** to return to the Traffic Learning screen.

By default, a security policy is put into a staging-tightening period for seven days. During this time, you can examine learning suggestions and adjust the security policy without blocking traffic.

3. On the Traffic Learning screen, review the violations and consider whether you want to permit any of them (for example, if a violation is causing false positives). Select any violations you do not want the system to trigger, and click **Disable Violation**.
   A popup screen opens, and you can verify that you want to disable the violations or cancel the action.
4. To activate the updated security policy, on the top right of the screen, click **Apply Policy**, then click **OK** to confirm.
5. To view outstanding tasks for the security policy, on the Main tab, click **Application Security** > **Overview**.
   The Overview Summary screen opens.
6. Examine the summary screen for information about recommended tasks that you need to complete.
   a) Review the Tasks to do area, which lists system tasks and security policy tasks that should be completed.
   b) Click the links in the Tasks to do area to go to the screen where you can perform the recommended action.
   c) In the Quick Links area, click any of the links to gain access to common configuration and reporting screens.

The security policy now 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, or if they are false positives that indicate a need to update the security policy.

Enforcing a security policy

To perform enforcement tasks, the security policy must be operating in transparent mode, and have been created manually. 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 **Application Security** > **Policy** > **Blocking**.
   The Settings screen shows the violations that can be detected, and how the security policy responds to requests that cause those violations (whether the system learns information from the illegal request, generates an alarm, or blocks the request).
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For each violation, review the settings so you understand how the security policy handles requests that cause the violation.

Option	Description
Learn	If selected, the system generates learning suggestions for requests that trigger the violation.
Alarm	If selected, the system records requests that trigger the violation in the Charts screen, the Syslog (`/var/log/asm`), and possibly in local or remote logs (depending on the settings of the logging profile).

Option	Description
Block	If selected (and the enforcement mode is set to **Blocking**), the system blocks requests that trigger the violation.

4. For the **Enforcement Mode** setting, select **Blocking**.
5. Click **Save**.
6. On the Main tab, click **Application Security** > **Policy**.
7. To change the number of days the security policy remains in staging, change the value in the **Staging-Tightening Period** field.

   The security policy does not block traffic during the Staging-Tightening Period even if violations occur. If you want to block traffic that causes violations, set the value of this field to `0`. For details, see the online help.
8. Click **Save**.
9. In the editing context area, click **Apply Policy** to immediately put the changes into effect.
10. For a quick summary of system activity, look at the Overview screen (**Application Security** > **Overview**).

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

Chapter 5

Creating a Security Policy for XML Applications

Topics:

Overview: Creating a security policy for web services

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

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

Considerations for developing XML security

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

- Does the web application use a WSDL or XML schema (XSD) file to validate the XML documents? Some web services use a WSDL or XML schema document to validate whether the incoming traffic complies with XML language rules. If the application uses a WSDL or XSD file, you need a copy of the file.
- Does the application use a URL or parameter to point to the server that you want to protect? You need to know the URLs or parameters that the application uses.

Creating a security policy for web services

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

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

1. On the Main tab, click **Application Security** > **Security Policies**.
   The Active Policies screen opens.
2. Click the **Create** button.
   The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.
3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.
   - Select **Existing Virtual Server** and click **Next** to use an existing virtual server (as long as it does not have an HTTP Class profile associated with it).
   - Select **New Virtual Server** and click **Next** to create a new virtual server and pool with basic configuration settings.

   The virtual server represents the web application you want to protect. The system automatically creates an HTTP Class with the same name as the virtual server.

   The Configure Local Traffic Settings screen opens.
4. Configure the new or existing virtual server, and click **Next**.
   The Select Deployment Scenario screen opens.

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

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

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

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

8. Click **Next**.
   The Configure Attack Signatures screen opens.
9. To configure attack signatures, move the systems used by your web application from the **Available Systems** list into the **Assigned Systems** list.
   The system adds the attack signatures needed to protect the selected systems.
10. Retain the default value of **Enabled** for the **Signature Staging** setting.
    New and updated attack signatures remain in staging for seven days.
11. Click **Next**.
    The Security Policy Configuration Summary screen opens.
12. Review the settings for the security policy. When you are satisfied with the security policy configuration, click **Finish**.
    The system creates the security policy, and the Create New XML Profile screen opens and displays the message: `The initial configuration of the web application is complete. You can now create a new XML profile.`

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

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

Creating a basic XML profile

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

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

1. If you are on the Create New XML Profile screen, skip to step 2. If not, at the top of the screen, click the **Create new XML profile** link.
   The Create New XML Profile screen opens.
2. For **Profile Name**, type a unique name.
3. Select the **Use XML Blocking Response Page** check box to send an XML response page when the security policy blocks a request that contains XML content that does not comply with this XML profile.

4. To allow SOAP messages to have attachments, select the **Allow Attachments in SOAP Messages** check box.
5. In the Defense Configuration area, for **Defense Level**, select **High** (the default value), **Medium**, or **Low** to specify the level of protection the security policy provides for XML applications and services. The system determines the defense configuration settings. You can review the settings by selecting **Advanced** next to Defense Configuration.
6. Click **Create**.
   The Associate XML Profile screen opens.
7. For the **Associate XML Profile** setting, specify whether to associate the XML profile with a URL or a parameter:

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

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

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

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

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

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

Creating an XML profile with WSDL validation

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

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

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

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

   If the XML Profiles screen is displayed, you are done creating the profile. Otherwise, the Associate XML Profile screen opens, and you can continue with the next step.
10. For the **Associate XML Profile** setting, specify whether to associate the XML profile with a URL or a parameter:

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

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

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

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

The security policy includes the XML profile with WSDL validation.

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

Creating an XML profile with XML schema validation

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

Follow these steps to incorporate the schema file into the XML profile.

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

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

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

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

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

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

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

Reviewing the status of an XML security policy

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

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

1. On the Main tab, click **Application Security** > **Policy**.
   The screen shows the properties of the current edited policy.
2. Review the messages in the identification and messages area to learn about the security policy status.

Status Message	Description
The initial configuration of the security policy is complete. Checking to see if ASM is detecting traffic.	The Application Security Manager™ is parsing and analyzing received requests. Allow the system several minutes to analyze requests.
The ASM did not detect any traffic.	Verify the networking configuration (check the VLAN, self IP address, pool, HTTP class, and virtual server).
ASM detected traffic successfully. Waiting for a minimum of 10000 requests and at least one hour from running the wizard for the *name* security policy. The ASM detected n requests during x hours and y minutes.	Application Security Manager detected traffic and will sample requests until it processes at least 10,000 requests, and at least one hour has passed since you started the Deployment wizard.
Processing XML violations for at least one hour for the *name* security policy. The ASM found *n* new XML violations during *xx* minutes and *yy* seconds.	After successfully detecting traffic and sampling requests, the Application Security Manager processes XML violations. Based on what it finds in the traffic sample and the violations, Application Security Manager automatically adjusts security policy settings to match the traffic and eliminate false positives. The system samples requests for at least one hour.
The system did not detect any new XML violations over the last hour for the *name*	For at least an hour, none of the traffic going to or from the application has caused XML violations. When

Status Message	Description
security policy. You can now go to the Traffic Learning page to fine-tune the security policy.	you see this message, you can fine-tune the security policy.
Timed out while waiting for sufficient number of requests for the security policy. Checking XML violations status.	The system processed insufficient traffic to finish building the security policy. Check to be sure that traffic can access the web application.

Fine-tuning an XML security policy

Before you can complete this task, you must have created a security policy using the web services deployment scenario, and have seen the message:

```
The system did not detect any new XML violations over the last hour
```

When no XML violations have occurred for at least an hour, the security policy includes learning suggestions based on the traffic. You can evaluate each suggestion and decide whether to add it to the security policy.

1. In the identification and messages area of the screen, click the **Traffic Learning** link.

   

   Tip: *If you do not see the link, click* ***Policy Building*** > ***Manual****.*

   The Traffic Learning screen opens, and lists violations that the system has found based on real traffic.
2. In the Traffic Learning area, click each violation hyperlink, then review and handle learning suggestions:

Option	Description
Accept	Select a learning suggestion, click **Accept**, and then click **Apply Policy**. The system updates the security policy to allow the file type, URL, parameter, or other element.
Clear	Select a learning suggestion, and click **Clear**. The system removes the learning suggestion and continues to generate suggestions for that violation.
Cancel	Click **Cancel** to return to the Traffic Learning screen.

   By default, a security policy is put into a staging-tightening period for seven days. During this time, you can examine learning suggestions and adjust the security policy without blocking traffic.
3. On the Traffic Learning screen, review the violations and consider whether you want to permit any of them (for example, if a violation is causing false positives). Select any violations you do not want the system to trigger, and click **Disable Violation**.
   A popup screen opens, and you can verify that you want to disable the violations or cancel the action.
4. To activate the updated security policy, on the top right of the screen, click **Apply Policy**, then click **OK** to confirm.

The security policy includes elements unique to your web service or XML application but it is not blocking the requests that cause violations.

Enforcing a security policy

To perform enforcement tasks, the security policy must be operating in transparent mode, and have been created manually. 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 **Application Security** > **Policy** > **Blocking**.
   The Settings screen shows the violations that can be detected, and how the security policy responds to requests that cause those violations (whether the system learns information from the illegal request, generates an alarm, or blocks the request).
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For each violation, review the settings so you understand how the security policy handles requests that cause the violation.

Option	Description
Learn	If selected, the system generates learning suggestions for requests that trigger the violation.
Alarm	If selected, the system records requests that trigger the violation in the Charts screen, the Syslog (`/var/log/asm`), and possibly in local or remote logs (depending on the settings of the logging profile).
Block	If selected (and the enforcement mode is set to **Blocking**), the system blocks requests that trigger the violation.

4. For the **Enforcement Mode** setting, select **Blocking**.
5. Click **Save**.
6. On the Main tab, click **Application Security** > **Policy**.
7. To change the number of days the security policy remains in staging, change the value in the **Staging-Tightening Period** field.

   The security policy does not block traffic during the Staging-Tightening Period even if violations occur. If you want to block traffic that causes violations, set the value of this field to `0`. For details, see the online help.
8. Click **Save**.
9. In the editing context area, click **Apply Policy** to immediately put the changes into effect.
10. For a quick summary of system activity, look at the Overview screen (**Application Security** > **Overview**).

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

Chapter 6

Using Rapid Deployment

Topics:

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 header
- 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)
- Evasion technique detected
- Access from disallowed Geolocation
- Access from disallowed User/Session/IP
- Request length exceeds defined buffer size
- Disallowed file upload content detected
- Failed to convert character
- Modified ASM™ cookie

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

You can implement Rapid Deployment in two ways:

- As a fixed policy that does not change unless you configure additional security features (choose **Rapid Deployment security policy**).
- By using Real Traffic Policy Builder® to develop the policy by automatically adding elements to the security policy (choose **Rapid Deployment security policy with Policy Builder enabled**).

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

- Select **Existing Virtual Server** and click **Next** to use an existing virtual server (as long as it does not have an HTTP Class profile associated with it).
- Select **New Virtual Server** and click **Next** to create a new virtual server and pool with basic configuration settings.

The virtual server represents the web application you want to protect. The system automatically creates an HTTP Class with the same name as the virtual server.

The Configure Local Traffic Settings screen opens.

4. Configure the new or existing virtual server, and click **Next**.
The Select Deployment Scenario screen opens.
5. For **Deployment Scenario**, select **Create a policy manually or use templates** and click **Next**.
The Configure Security Policy Properties screen opens.
6. From the **Application Language** list, select the language encoding of the application.

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

7. From the **Application-Ready Security Policy** list, select one of the following options:

Option	Description
Rapid Deployment security policy	Creates a simple security policy that protects against known vulnerabilities, such as evasion attacks, data leakage, and buffer overflow attacks.
Rapid Deployment security policy with Policy Builder enabled	Creates a simple security policy that protects against known vulnerabilities, and starts the Policy Builder which can add elements to the policy based on examining application traffic, put them in staging, and enforce them when ready.

8. For the **Staging-Tightening Period** field, retain the default setting of 7 days.
Staging and tightening allow you to test the security policy entities for false positives before enforcing them.
During the staging-tightening 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.
9. Click **Next**.
The Configure Attack Signatures screen opens.
10. To configure attack signatures, move the systems used by your web application from the **Available Systems** list into the **Assigned Systems** list.
The system adds the attack signatures needed to protect the selected systems.
11. Retain the default value of **Enabled** for the **Signature Staging** setting.
New and updated attack signatures remain in staging for seven days, and during that time, they are not enforced (according to the learn, alarm, and block flags selected for each of the signature sets).
12. If using the **Rapid Deployment security policy** (without Policy Builder), you can select **Enabled** for the **Apply Signatures to Responses** setting to have the system use the signatures to inspect responses.
13. Click **Next**.
The Security Policy Configuration Summary screen opens.
14. Review the settings for the security policy. When you are satisfied with the security policy configuration, click **Finish**.
The system creates the security policy and opens the Properties screen.

When you first create a rapid deployment security policy, it 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, but does not block the request.

Fine-tuning a security policy

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

Note: *If you are using the Policy Builder to add elements to the security policy, you can skip this task.*

1. On the Main tab, click **Application Security** > **Policy Building** > **Manual**.
   The Traffic Learning screen opens, and lists violations and learning suggestions that the system has found based on real traffic.
2. In the Traffic Learning area, click each violation hyperlink, then review and handle learning suggestions:

Option	Description
Accept	Select a learning suggestion, click **Accept**, and then click **Apply Policy**. The system updates the security policy to allow the file type, URL, parameter, or other element.
Clear	Select a learning suggestion, and click **Clear**. The system removes the learning suggestion and continues to generate suggestions for that violation.
Cancel	Click **Cancel** to return to the Traffic Learning screen.

   By default, a security policy is put into a staging-tightening period for seven days. During this time, you can examine learning suggestions and adjust the security policy without blocking traffic.
3. On the Traffic Learning screen, review the violations and consider whether you want to permit any of them (for example, if a violation is causing false positives). Select any violations you do not want the system to trigger, and click **Disable Violation**.
   A popup screen opens, and you can verify that you want to disable the violations or cancel the action.
4. To activate the updated security policy, on the top right of the screen, click **Apply Policy**, then click **OK** to confirm.
5. To view outstanding tasks for the security policy, on the Main tab, click **Application Security** > **Overview**.
   The Overview Summary screen opens.
6. Examine the summary screen for information about recommended tasks that you need to complete.
   a) Review the Tasks to do area, which lists system tasks and security policy tasks that should be completed.
   b) Click the links in the Tasks to do area to go to the screen where you can perform the recommended action.
   c) In the Quick Links area, click any of the links to gain access to common configuration and reporting screens.

The security policy now 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, or if they are false positives that indicate a need to update the security policy.

Enforcing a security policy

To perform enforcement tasks, the security policy must be operating in transparent mode, and have been created manually. 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 **Application Security** > **Policy** > **Blocking**.
   The Settings screen shows the violations that can be detected, and how the security policy responds to requests that cause those violations (whether the system learns information from the illegal request, generates an alarm, or blocks the request).
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For each violation, review the settings so you understand how the security policy handles requests that cause the violation.

Option	Description
Learn	If selected, the system generates learning suggestions for requests that trigger the violation.
Alarm	If selected, the system records requests that trigger the violation in the Charts screen, the Syslog (`/var/log/asm`), and possibly in local or remote logs (depending on the settings of the logging profile).
Block	If selected (and the enforcement mode is set to **Blocking**), the system blocks requests that trigger the violation.

4. For the **Enforcement Mode** setting, select **Blocking**.
5. Click **Save**.
6. On the Main tab, click **Application Security** > **Policy**.
7. To change the number of days the security policy remains in staging, change the value in the **Staging-Tightening Period** field.

   The security policy does not block traffic during the Staging-Tightening Period even if violations occur. If you want to block traffic that causes violations, set the value of this field to `0`. For details, see the online help.
8. Click **Save**.
9. In the editing context area, click **Apply Policy** to immediately put the changes into effect.
10. For a quick summary of system activity, look at the Overview screen (**Application Security** > **Overview**).

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

Chapter 7

Using Application-Ready Security Templates

Topics:

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
- Microsoft Sharepoint® 2003, 2007, 2010
- Oracle® Applications 11i
- Oracle® Portal 10g
- Lotus Domino® 6.5
- SAP NetWeaver® 7
- PeopleSoft® Portal Solutions 9

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

Creating a security policy from an application template

You can create a security policy only if you have performed the basic system configuration tasks including defining a VLAN, a self IP address, a local traffic pool, an application security class, and a virtual server, according to the needs of your networking environment.

You can use application-ready templates to create a security policy quickly. The Deployment wizard takes you through the steps required.

1. On the Main tab, click **Application Security** > **Security Policies**.
   The Active Policies screen opens.
2. Click the **Create** button.
   The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.
3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.
   - Select **Existing Virtual Server** and click **Next** to use an existing virtual server (as long as it does not have an HTTP Class profile associated with it).
   - Select **New Virtual Server** and click **Next** to create a new virtual server and pool with basic configuration settings.

   The virtual server represents the web application you want to protect. The system automatically creates an HTTP Class with the same name as the virtual server.

   The Configure Local Traffic Settings screen opens.
4. Configure the new or existing virtual server, and click **Next**.
   The Select Deployment Scenario screen opens.
5. For **Deployment Scenario**, select **Create a policy manually or use templates** and click **Next**.
   The Configure Security Policy Properties screen opens.
6. From the **Application Language** list, select the language encoding of the application.

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

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

   Staging and tightening allows you to test the security policy entities for false positives without enforcing them.

   The security policy provides learning suggestions when requests are processed that do not meet the security policy entity's settings, but the security policy does not alert or block that traffic, even if those requests trigger violations.
9. Click **Next**.
   The Security Policy Configuration Summary screen opens.
10. Review the settings for the security policy. When you are satisfied with the security policy configuration, click **Finish**.
    The system creates the security policy and opens the Properties screen.

When you first create the security policy, it operates in transparent mode (meaning that it does not block traffic). When the system receives a request that violates the security policy, the system logs the violation event, but does not block the request.

Fine-tuning a security policy

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

Note: *If you are using the Policy Builder to add elements to the security policy, you can skip this task.*

1. On the Main tab, click **Application Security** > **Policy Building** > **Manual**.
   The Traffic Learning screen opens, and lists violations and learning suggestions that the system has found based on real traffic.
2. In the Traffic Learning area, click each violation hyperlink, then review and handle learning suggestions:

Option	Description
Accept	Select a learning suggestion, click **Accept**, and then click **Apply Policy**. The system updates the security policy to allow the file type, URL, parameter, or other element.
Clear	Select a learning suggestion, and click **Clear**. The system removes the learning suggestion and continues to generate suggestions for that violation.
Cancel	Click **Cancel** to return to the Traffic Learning screen.

   By default, a security policy is put into a staging-tightening period for seven days. During this time, you can examine learning suggestions and adjust the security policy without blocking traffic.

3. On the Traffic Learning screen, review the violations and consider whether you want to permit any of them (for example, if a violation is causing false positives). Select any violations you do not want the system to trigger, and click **Disable Violation**.
   A popup screen opens, and you can verify that you want to disable the violations or cancel the action.
4. To activate the updated security policy, on the top right of the screen, click **Apply Policy**, then click **OK** to confirm.
5. To view outstanding tasks for the security policy, on the Main tab, click **Application Security** > **Overview**.
   The Overview Summary screen opens.
6. Examine the summary screen for information about recommended tasks that you need to complete.
   a) Review the Tasks to do area, which lists system tasks and security policy tasks that should be completed.
   b) Click the links in the Tasks to do area to go to the screen where you can perform the recommended action.
   c) In the Quick Links area, click any of the links to gain access to common configuration and reporting screens.

The security policy now 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, or if they are false positives that indicate a need to update the security policy.

Enforcing a security policy

To perform enforcement tasks, the security policy must be operating in transparent mode, and have been created manually. 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 **Application Security** > **Policy** > **Blocking**.
   The Settings screen shows the violations that can be detected, and how the security policy responds to requests that cause those violations (whether the system learns information from the illegal request, generates an alarm, or blocks the request).
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For each violation, review the settings so you understand how the security policy handles requests that cause the violation.

Option	Description
Learn	If selected, the system generates learning suggestions for requests that trigger the violation.
Alarm	If selected, the system records requests that trigger the violation in the Charts screen, the Syslog (`/var/log/asm`), and possibly in local or remote logs (depending on the settings of the logging profile).
Block	If selected (and the enforcement mode is set to **Blocking**), the system blocks requests that trigger the violation.

4. For the **Enforcement Mode** setting, select **Blocking**.
5. Click **Save**.
6. On the Main tab, click **Application Security** > **Policy**.
7. To change the number of days the security policy remains in staging, change the value in the **Staging-Tightening Period** field.

   The security policy does not block traffic during the Staging-Tightening Period even if violations occur. If you want to block traffic that causes violations, set the value of this field to `0`. For details, see the online help.
8. Click **Save**.
9. In the editing context area, click **Apply Policy** to immediately put the changes into effect.
10. For a quick summary of system activity, look at the Overview screen (**Application Security** > **Overview**).

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

Appendix
A

Security Policy Elements in Each Policy Type

Topics:

Security policy elements included in each policy type

The elements that the system can automatically add to a security policy depend on the policy type you select for automatic policy building. The policy types you can select when creating a security policy automatically are **Fundamental**, **Enhanced**, and **Comprehensive**. The following table shows which elements are included in each policy type. They are listed in the order in which they are found in the Security Policy Elements area of the Configuration screen.

Security policy element	Fundamental	Enhanced	Comprehensive
HTTP Protocol Compliance	Yes	Yes	Yes
Evasion Techniques Detected	Yes	Yes	Yes
File Types	Yes	Yes	Yes
File Types: Lengths	Yes	Yes	Yes
Attack Signatures	Yes	Yes	Yes
URLs	No	No	Yes
URLs: Meta Characters	No	No	Yes
Parameters	No	Yes	Yes
Parameters: Name Meta Characters	No	No	Yes
Parameters: Value Lengths	No	Yes	Yes
Value Meta Characters	No	No	Yes
Cookies	No	Yes	Yes
Allowed Methods	No	Yes	Yes
Request Length Exceeds Defined Buffer Size	Yes	Yes	Yes
Content Profiles	No	No; Yes if JSON/XML payload detection selected	No; Yes if JSON/XML payload detection selected
Content Profiles: Automatically detect advanced protocols	No	No; Yes if JSON/XML payload detection selected	No; Yes if JSON/XML payload detection selected
Host Names	Yes	Yes	Yes
CSRF URLs	No	No	No

Index

T

V

W

X