BIG-IP® Application Security Manager™: Getting Started

Version 11.5

Table of Contents

Legal Notices

Publication Date

This document was published on January 27, 2014.

Publication Number

MAN-0285-08

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, APM, Application Acceleration Manager, Application Security Manager, ARX, AskF5, ASM, BIG-IP, BIG-IQ, Cloud Extender, CloudFucious, Cloud Manager, Clustered Multiprocessing, CMP, COHESION, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5 [DESIGN], F5 Certified [DESIGN], F5 Networks, F5 SalesXchange [DESIGN], F5 Synthesis, f5 Synthesis, F5 Synthesis [DESIGN], F5 TechXchange [DESIGN], Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, LineRate, LineRate Systems [DESIGN], LROS, LTM, Message Security Manager, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, SalesXchange, ScaleN, Signalling Delivery Controller, SDC, SSL Acceleration, software designed applications services, SDAC (except in Japan), StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TechXchange, TMOS, TotALL, Traffic Management Operating System, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WebSafe, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

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

Patents

This product may be protected by one or more patents indicated at:
http://www.f5.com/about/guidelines-policies/patents

Export Regulation Notice

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

RF Interference Warning

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

FCC Compliance

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

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

Canadian Regulatory Compliance

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

Standards Compliance

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

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 Intel QuickAssist kernel module, library, and headers software licensed under the GNU General Public License (GPL).

This product includes software licensed from Gerald Combs (gerald@wireshark.org) under the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or any later version. Copyright ©1998 Gerald Combs.

This product includes software developed by Thomas Williams and Colin Kelley. Copyright ©1986 - 1993, 1998, 2004, 2007

Permission to use, copy, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Permission to modify the software is granted, but not the right to distribute the complete modified source code. Modifications are to be distributed as patches to the released version. Permission to distribute binaries produced by compiling modified sources is granted, provided you

1. distribute the corresponding source modifications from the released version in the form of a patch file along with the binaries,

2. add special version identification to distinguish your version in addition to the base release version number,
3. provide your name and address as the primary contact for the support of your modified version, and
4. retain our contact information in regard to use of the base software.

Permission to distribute the released version of the source code along with corresponding source modifications in the form of a patch file is granted with same provisions 2 through 4 for binary distributions. This software is provided "as is" without express or implied warranty to the extent permitted by applicable law.

This product contains software developed by Google, Inc. Copyright ©2011 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product contains software developed by the RE2 Authors. Copyright ©2009 The RE2 Authors. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

This product includes software developed by Digital Envoy, Inc.

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 later.

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.

This product includes software written by Makamaka Hannyaharamitu ©2007-2008.

This product includes software developed by Jeremy Ashkenas and DocumentCloud, and distributed under the MIT license. Copyright © 2010-2013 Jeremy Ashkenas, DocumentCloud.

This product includes gson software, distributed under the Apache License version 2.0. Copyright © 2008-2011 Google Inc.

Chapter

1

Introduction to Application Security Manager

What is Application Security Manager?

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

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

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

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

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

When to use application security

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

You can use ASM™ in many ways:

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

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

Types of attacks ASM protects against

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

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

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

Chapter 2

Performing Basic Configuration Tasks

About basic networking configuration terms

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

local traffic policy

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

pool

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

self IP address

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

virtual server

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

VLAN (virtual local area network)

A logical grouping of network devices. You create a VLAN and associate the physical interfaces on the BIG-IP system with the VLAN. You can use a VLAN to logically group devices that are on different network segments.

Overview: Performing basic networking configuration tasks

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

Next, you must configure the BIG-IP system on your network before you can run the Application Security Manager™ (ASM) Deployment wizard to create a security policy. The specific tasks you need to perform depend on your company's networking configuration, and which of the other BIG-IP system features are in use.

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

Task summary

Creating a VLAN

Creating a self IP address for a VLAN

Creating a local traffic pool for application security

Creating a virtual server

Creating a VLAN

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

1. On the Main tab, click **Network** > **VLANs**.
   The VLAN List screen opens.
2. Click **Create**.
   The New VLAN screen opens.
3. In the **Name** field, type a unique name for the VLAN.
4. 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 from 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 IPv4 or IPv6 address.

   This IP address should represent the address space of the VLAN that you specify with the **VLAN/Tunnel** setting.
5. In the **Netmask** field, type the network mask for the specified IP address.
6. From the **VLAN/Tunnel** list, select the VLAN to associate with this self IP address.
   - 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.

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

Creating a local traffic pool for application security

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

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

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

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

Creating a virtual server

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

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

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.
5. In the **Service Port** field, type `80`, or select **HTTP** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.

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

About additional networking configuration

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

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

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

Chapter

3

Creating a Security Policy Automatically

Deployment scenarios when creating security policies

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

Deployment scenario	Description
Create a 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®, QualysGuard®, HP WebInspect, or a generic scanner if using another tool. Based on the results from an imported vulnerability report, Application Security Manager™ creates a policy that automatically mitigates the vulnerabilities on your web site. You can also review and fine-tune the policy. When the security policy includes all the protections that you need and does not produce any false positives, you can enforce the security policy.

Overview: Automatic policy building

You can use the Application Security Manager™ to 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.

Task summary

Creating a security policy automatically
Reviewing security policy status
Reviewing outstanding security policy tasks

Creating a security policy automatically

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

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

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

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

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

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

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

   The name of the new or existing virtual server becomes the name of the security policy.

   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. If you do not want the security policy to distinguish between HTTP and HTTPS URLs, clear the **Differentiate between HTTP and HTTPS URLs** check box. Otherwise, leave it selected.
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. For the **Signature Staging** setting, verify that the default option **Enabled** is selected.

    Note: *Because the Real Traffic Policy Builder® begins building the security policy in Blocking mode, you can keep signature staging enabled 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.
12. Click **Next**.
    The Configure Automatic Policy Building screen opens.
13. For **Policy Type**, select an option to determine the security features to include in the policy.

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

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

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

Option	Description
Fast	Use if your application supports a small number of requests from a small number of sessions; for example, useful for web sites with less traffic. However, choosing this option may present a greater chance of adding false entities to the security policy.
Medium	Use if your application supports a medium number of requests, or if you are not sure about the amount of traffic on the application web site. This is the default setting.
Slow	Use if your application supports 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 to the security policy and enforces the elements.

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

Option	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 when you select this option.

Option	Description
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.

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

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

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

How the security policy is built

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

The Policy Builder builds the security policy as follows:

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

The Policy Builder automatically discovers and populates the security policy with the policy elements (such as file types, URLs, parameters, and cookies). 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 **Security** > **Application Security** > **Policy Building** > **Status (Automatic)**. The Status (Automatic) screen opens where you can see the automatic policy building status, file types, URLs, parameters, and cookies that were added to the security policy.
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.

Option	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. If you did not associate a virtual server, you need to do that to process traffic.
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 staging.

Reviewing outstanding security policy tasks

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

1. On the Main tab, click **Security** > **Overview** > **Application** > **Action Items**.
   The Action Items screen opens.
2. Examine the summary screen for information about recommended tasks that you need to complete.
   - Review the Suggested Action Items area, which lists system tasks and security policy tasks that should be completed.
   - Click the links to go to the screen where you can perform the recommended actions.
   - 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 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 **Security** > **DoS Protection**. You need to create a DoS profile with Application Security enabled to configure Layer 7 DoS protection.
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 **Security** > **Application Security** > **Anomaly Detection** > **Brute Force Attack Prevention**.
IP Address Intelligence	Logs and blocks attacks from IP addresses that are in the IP Address Intelligence Database and are considered to have a bad reputation. Click **Security** > **Application Security** > **IP Addresses** > **IP Address Intelligence**.
Web scraping detection	Mitigates web scraping (web data extraction) on web sites by attempting to determine whether a web client source is human. Click **Security** > **Application Security** > **Anomaly Detection** > **Web Scraping**.
CSRF protection	Prevents cross-site request forgery (CSRF) where a user is forced to perform unwanted actions on a web application where the user is currently authenticated. Click **Security** > **Application Security** > **CSRF Protection**.
Sensitive data masking	Protects sensitive data in responses such as a credit card number, U.S. Social Security number, or custom pattern. Click **Security** > **Application Security** > **Data Guard**. Create sensitive parameters if needed (they are also masked); click **Security** > **Application Security** > **Parameters** > **Sensitive Parameters**. As an additional protection, set the Mask Credit Card Numbers in Request Log option in the policy properties.
Anti-virus protection through an ICAP server	Configures the system as an Internet Content Adaptation Protocol (ICAP) client so that an external ICAP server can inspect HTTP file uploads for viruses before releasing the content to the web server. To set up the ICAP server, click **Security** > **Options** > **Application Security** > **Integrated Services** > **Anti-Virus Protection**. To set the blocking settings (alarm and/or block) of the Virus Detected violation, click **Security** > **Application Security** > **Blocking**. Also check that the values of the system variables `icap_uri` and `virus_header_name` correspond to the ICAP server (**Security** > **Options** > **Application Security** > **Advanced Configuration** > **System Variables**).

Chapter 4

Using Vulnerability Assessment Tools for a Security Policy

Overview: Vulnerability assessment policy building

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

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

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

Task summary

Creating a security policy using vulnerability assessment tool output
Associating a vulnerability assessment tool with an existing security policy
Configuring system-wide Cenzic settings
Importing vulnerability assessment tool output
Resolving vulnerabilities
Fine-tuning a security policy
Enforcing a security policy
Creating a security policy integrated with WhiteHat Sentinel
Creating a vulnerability file
Resolving vulnerabilities
Fine-tuning a security policy
Enforcing a security policy

About using Policy Builder with scanner policies

When you develop a security policy using third party vulnerability assessment tool or scanner output, you have the option of enabling automatic policy building. If you enable automatic policy building, the system turns on the Real Traffic Policy Builder®. The system then automatically builds the policy based on what it learns from your web application traffic, and uses logic to prevent false positives. You also use external scanning tools (WhiteHat Sentinel, QualysGuard, IBM AppScan, Cenzic Hailstorm, and others) to suggest how to build your policy to protect against vulnerabilities. You can then import the vulnerabilities detected by the scanner, then choose whether or not to update the security policy for each problem found.

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

- The Policy Builder might remove a URL that the scanner added to the list of CSRF-protected URLs.
- The Policy Builder might allow file upload of executable files on a parameter after the scanner disallowed it.
- The Policy Builder might add an allowed method after the scanner disallowed it.
- The Policy Builder might disable attack signatures on parameters, cookies, and at the policy level after the scanner enabled them.

If you do not enable the Policy Builder when creating the security policy, you can turn it on after you have imported the vulnerabilities. The Real Traffic Policy Builder can be enabled (or disabled) on the Policy Building Settings screen.

Creating a security policy using vulnerability assessment tool output

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

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

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

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

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

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

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

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

   The name of the new or existing virtual server becomes the name of the security policy.

   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, then click **Next**.

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

7. For **Enforcement Mode** specify whether or not the system blocks traffic that violates the security policy.

- Leave the value set to **Transparent**, the default value, if you want to review and fine-tune the security policy before placing it in Blocking mode.
- If you want the system to enforce the security policy immediately, select **Blocking**.

8. If the application is case-sensitive, select the **Security Policy is case sensitive** check box. Otherwise, leave it cleared.

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

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

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

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

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

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

13. If you want to use automatic policy building, leave the **Real Traffic Policy Builder** check box selected.

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

    If selected, the system runs the Policy Builder when you finish creating the policy.
14. Click **Next**.
    The Security Policy Configuration Summary screen opens.
15. Review the settings for the security policy. When you are satisfied with the security policy configuration, click **Finish**.
    The system creates the security policy and opens the vulnerability assessment settings screen specific to the tool you are using. For most tools, you can import the results of a vulnerabilities scan in an XML file.
16. If using the Cenzic Hailstorm or WhiteHat Sentinel, you can connect with these tools on the Vulnerabilities Assessments Settings screen that opens. If you have an account, click **Connect**.

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

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

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

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

Associating a vulnerability assessment tool with an existing security policy

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

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

1. On the Main tab, click **Security** > **Application Security** > **Vulnerability Assessments** > **Settings**. The Vulnerabilities Assessments: Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. From the **Vulnerability Assessment Tool** list, select the vulnerability assessment tool that you use to scan your web application for problems, or select **Generic Scanner** if your tool is not listed.

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

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

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

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

Configuring system-wide Cenzic settings

Before you can connect to Cenzic Hailstorm or Cenzic Cloud, the system needs to have an Internet connection and have DNS configured. If you have an account with Cenzic, you need the user name and password.

If you want to use Cenzic Hailstorm as your vulnerability assessment tool, you can configure system-wide Cenzic settings. This is useful if you want to use a Cenzic account to import vulnerabilities for multiple security policies because you only have to set it up once. If you do not have an account with Cenzic, you can open a trial account and run a free scan to find and resolve vulnerabilities in your web application.

1. On the Main tab, click **Security** > **Options** > **Application Security** > **Integrated Services** > **Cenzic Settings**.
2. If you have an account with Cenzic Cloud, connect to Cenzic as follows:
   a) For **Connection Status**, click **Connect**.
   The Connect with Cenzic Cloud popup screen opens.
   b) Type the **User Name** and **Password**, then click **Submit**.

   The system sets up a system-wide connection with Cenzic Cloud.
3. If you want to open a trial account with Cenzic Cloud, connect as follows:
   a) For **Connection Status**, click the **Open Cenzic Cloud Trial Account** link.
   The Open Cenzic Cloud Trial Account popup screen opens.

b) Register with Cenzic by typing your customer information and setting up an account.

The system sets up a system-wide connection with Cenzic Cloud.

4. To establish a connection to a Cenzic ARC Server instead of Cenzic Cloud, in the **Cenzic ARC Server address** field, type the local Cenzic ARC server IP address or fully qualified domain name.

   Note: *If you configure a local Cenzic ARC Server IP address, you will not have the option to share the site mapping with the Cenzic tool.*

5. Click **Save** to save your settings.

If you have existing security policies that are configured to use the Cenzic vulnerability assessment tool, those security policies will automatically connect to this Cenzic account. The system warns you that configuring system-wide Cenzic account settings replaces existing security policy-specific Cenzic connections. If you create new security policies that use the Cenzic vulnerability assessment tool, they will use the system-wide Cenzic account settings.

If you configure a Cenzic ARC server IP address, you will not have the option to open a trial account in the Cenzic Cloud, and all communications are made with your local Cenzic server.

Importing vulnerability assessment tool output

In order to import vulnerability assessment tool output into a security policy, 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 is configured to use a vulnerability assessment tool, you can import the vulnerability assessment tool output into that security policy.

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

   If using the Cenzic or WhiteHat vulnerability assessment tools, additional settings allow you to connect to an existing account, create a trial account, and request a new scan. Refer to the online help for details about the settings.

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

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

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

Resolving vulnerabilities

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

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

1. On the Main tab, click **Security** > **Application Security** > **Vulnerability Assessments**.
   The Vulnerabilities screen opens and lists the vulnerabilities that the vulnerability assessment scan discovered. They are categorized in to those which are resolvable using ASM™ and those which are not.
2. 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.*

3. From the **View** and **Vulnerabilities with** lists, you can filter the vulnerabilities that are displayed.

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

   ASM reviews the prerequisites and then displays a list of the changes it will make to fix the vulnerability.
5. If you agree with the changes, click **Resolve**.
   ASM modifies the security policy to protect against the vulnerabilities for which you clicked **Resolve** and ignores the rest. In the Vulnerabilities list, the ASM Status column for the vulnerability changes to Mitigated or Mitigated (In Staging), if appropriate.
6. Click **Apply Policy** to save the changes to the security policy.
   The system updates the security policy to prevent the handled vulnerabilities from reoccurring.
7. If using WhiteHat Sentinel, select all of the vulnerabilities you dealt with and click **Retest** to have the WhiteHat Sentinel service verify that the vulnerability has been dealt with.

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

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 **Security** > **Application Security** > **Policy Building** > **Manual Traffic Learning**.
   The Manual Traffic Learning screen opens, and lists violations and learning suggestions that the system has made 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 Manual 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 Manual 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 put the security policy changes into effect immediately, click **Apply Policy**.
5. On the Main tab, click **Security** > **Overview** > **Application** > **Action Items**.
   The Action Items screen opens.
6. Examine the Action Items screen for information about recommended actions that you need to complete.
   a) Review the Suggested Action Items area, which lists system tasks and security policy tasks that should be completed.
   b) Click the links in the Suggested Action Items 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 Manual 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

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

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

1. On the Main tab, click **Security** > **Application Security** > **Blocking**.
   The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For the **Enforcement Mode** setting, select **Blocking**.
4. For each violation, review the settings so you understand how the security policy handles requests that cause the violation, and adjust if necessary.

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 system log (`/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.

Tip: *Click the information icon preceding a violation for a description of it.*

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

   The security policy does not block traffic during the Enforcement Readiness Period even if violations occur.
9. If you want to block traffic that causes violations, you need to enforce violations. One way to do this is:
   a) Set the **Enforcement Readiness Period** to `0`.
   b) Click **Save**.
   c) On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Enforcement Readiness**.
   d) Click **Enforce Ready**.
10. To put the security policy changes into effect immediately, click **Apply Policy**.
11. For a quick summary of system activity, look at the Overview screen (**Security** > **Overview** > **Application**).

    The Summary screen displays statistical information about Application Security traffic.

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

Chapter 5

Using WhiteHat Sentinel for a Security Policy

Overview: Vulnerability assessment policy building

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

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

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

Task summary

Creating a security policy using vulnerability assessment tool output
Associating a vulnerability assessment tool with an existing security policy
Configuring system-wide Cenzic settings
Importing vulnerability assessment tool output
Resolving vulnerabilities
Fine-tuning a security policy
Enforcing a security policy
Creating a security policy integrated with WhiteHat Sentinel
Creating a vulnerability file
Resolving vulnerabilities
Fine-tuning a security policy
Enforcing a security policy

Creating a security policy integrated with WhiteHat Sentinel

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

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

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

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

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

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

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

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

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

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

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

   The name of the new or existing virtual server becomes the name of the security policy.

   The Select Deployment Scenario screen opens.
5. For **Deployment Scenario**, select **Create a policy using third party vulnerability assessment tool output** 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. For **Enforcement Mode** specify whether or not the system blocks traffic that violates the security policy.

   - Leave the value set to **Transparent**, the default value, if you want to review and fine-tune the security policy before placing it in Blocking mode.
   - If you want the system to enforce the security policy immediately, select **Blocking**.
8. If the application is case-sensitive, select the **Security Policy is case sensitive** check box. Otherwise, leave it cleared.

   Important: *You cannot change this setting after you have created the security policy.*
9. If you do not want the security policy to distinguish between HTTP and HTTPS URLs, clear the **Differentiate between HTTP and HTTPS URLs** check box. Otherwise, leave it selected.

10. Click **Next**.
    The Vulnerability Assessments Settings screen opens.
11. From the **Vulnerability Assessment Tool** list, select **WhiteHat Sentinel**.
12. In the **Configure exceptions for the scanner IP Address** setting, specify any IP addresses that you want the security policy to allow (for example, the IP address of the vulnerabilities assessment tool), and how to deal with them.
    a) Type the IP address and netmask of the vulnerabilities assessment tool.

       You can add `%n` after an IP address to specify a route domain, where `n` is the route domain identification number.
    b) Select the appropriate check boxes for learning suggestions, logging, and blocking traffic from this IP address.

13. If you want to use automatic policy building, leave the **Real Traffic Policy Builder** check box selected.

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

    If selected, the system runs the Policy Builder when you finish creating the policy.
14. Click **Next**.
    The Security Policy Configuration Summary screen opens.
15. Review the settings for the security policy. When you are satisfied with the security policy configuration, click **Finish**.
    The system creates the security policy and opens the vulnerability assessment settings screen specific to the tool you are using. For most tools, you can import the results of a vulnerabilities scan in an XML file.
16. Verify that the **Vulnerability Assessment Tool** is set to **WhiteHat Sentinel**.
17. For **WhiteHat Web API Key**, type the key generated and supplied by WhiteHat Sentinel for your web application.

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

18. 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.
19. On the menu bar, click **Vulnerabilities**.
20. Next, import the vulnerabilities from the WhiteHat Sentinel server. Click **Import**.
    The Import WhiteHat Sentinel Verified Vulneabilities popup screen opens.
21. For **Import Method**, select how to import the vulnerability report:

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

22. 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. The policy type is Vulnerability Assessment.

Note: *When integrating with WhiteHat Sentinel, Application Security Manager has to recognize whether a request is coming from the WhiteHat server. This enables ASM to communicate with WhiteHat Sentinel so the WhiteHat portal can mark fixed vulnerabilities as `Mitigated by WAF`. ASM identifies requests sent by WhiteHat Sentinel using the published source IP of the WhiteHat Sentinel service. However, ASM does not see the original source IP address of requests if 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` system variables 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 **Security** > **Application Security** > **Vulnerability Assessments**.
   The Vulnerabilities screen opens and lists the vulnerabilities that the vulnerability assessment scan discovered. They are categorized in to those which are resolvable using ASM™ and those which are not.
2. 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.*

3. From the **View** and **Vulnerabilities with** lists, you can filter the vulnerabilities that are displayed.

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

   ASM reviews the prerequisites and then displays a list of the changes it will make to fix the vulnerability.
5. If you agree with the changes, click **Resolve**.
   ASM modifies the security policy to protect against the vulnerabilities for which you clicked **Resolve** and ignores the rest. In the Vulnerabilities list, the ASM Status column for the vulnerability changes to Mitigated or Mitigated (In Staging), if appropriate.
6. Click **Apply Policy** to save the changes to the security policy.
   The system updates the security policy to prevent the handled vulnerabilities from reoccurring.
7. If using WhiteHat Sentinel, select all of the vulnerabilities you dealt with and click **Retest** to have the WhiteHat Sentinel service verify that the vulnerability has been dealt with.

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

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 **Security** > **Application Security** > **Policy Building** > **Manual Traffic Learning**.
   The Manual Traffic Learning screen opens, and lists violations and learning suggestions that the system has made 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 Manual 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 Manual 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 put the security policy changes into effect immediately, click **Apply Policy**.
5. On the Main tab, click **Security** > **Overview** > **Application** > **Action Items**.
   The Action Items screen opens.
6. Examine the Action Items screen for information about recommended actions that you need to complete.
   a) Review the Suggested Action Items area, which lists system tasks and security policy tasks that should be completed.
   b) Click the links in the Suggested Action Items 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 Manual 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

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

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

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

The Settings screen opens.

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

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 system log (`/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.

Tip: *Click the information icon preceding a violation for a description of it.*

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

   The security policy does not block traffic during the Enforcement Readiness Period even if violations occur.
9. If you want to block traffic that causes violations, you need to enforce violations. One way to do this is:
   a) Set the **Enforcement Readiness Period** to `0`.
   b) Click **Save**.
   c) On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Enforcement Readiness**.
   d) Click **Enforce Ready**.
10. To put the security policy changes into effect immediately, click **Apply Policy**.
11. For a quick summary of system activity, look at the Overview screen (**Security** > **Overview** > **Application**).

    The Summary screen displays statistical information about Application Security traffic.

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

Chapter 6

Creating a Security Policy for Web Services

Overview: Creating a security policy for web services

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

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

Considerations for developing XML security

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

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

Task summary

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

About XML security

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

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

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

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

Creating a security policy for web services

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

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

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

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

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

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

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

   The name of the new or existing virtual server becomes the name of the security policy.

   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. If you do not want the security policy to distinguish between HTTP and HTTPS URLs, clear the **Differentiate between HTTP and HTTPS URLs** check box. Otherwise, leave it selected.
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.
12. Click **Next**.
    The Security Policy Configuration Summary screen opens.
13. 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.

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

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

Option	Description
URL	Validates XML data found in requests to this URL.

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

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

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

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

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

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

Creating an XML profile with WSDL validation

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

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

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

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

   The Create New XML Profile screen opens.
2. For **Profile Name**, type a unique name.
3. Select the **Use XML Blocking Response Page** check box to send an XML response page when the security policy blocks a request that contains XML content that does not comply with this XML profile.
4. In the Validation Configuration area, for the **File** option of the **Configuration Files** setting, navigate to the WSDL document.
5. Click **Upload**.
   The screen lists the uploaded file.
6. If the imported file references another URL (and the setting is available), for **Import URL**, type the URL.

7. To allow SOAP messages to have attachments, select the **Allow Attachments in SOAP Messages** check box.
8. In the Defense Configuration area, for **Defense Level**, select **High** (the default value), **Medium**, or **Low** to specify the level of protection you want the security policy to provide for XML applications and services.
   The system adjusts the defense configuration settings according to your choice. You can review the settings by selecting **Advanced** next to Defense Configuration.
9. Click **Create**.

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

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

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

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

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

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

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

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

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

Creating an XML profile with XML schema validation

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

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

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

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

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

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

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

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

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

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

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

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

Reviewing the status of an XML security policy

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

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

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

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

Status Message	Description
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* ***Security*** *>* ***Application Security*** *>* ***Policy Building*** *>* ***Manual Traffic Learning****.*

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

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

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

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

1. On the Main tab, click **Security** > **Application Security** > **Blocking**.
   The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For the **Enforcement Mode** setting, select **Blocking**.
4. For each violation, review the settings so you understand how the security policy handles requests that cause the violation, and adjust if necessary.

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 system log (`/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.

Tip: *Click the information icon preceding a violation for a description of it.*

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

   The security policy does not block traffic during the Enforcement Readiness Period even if violations occur.
9. If you want to block traffic that causes violations, you need to enforce violations. One way to do this is:
   a) Set the **Enforcement Readiness Period** to `0`.
   b) Click **Save**.
   c) On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Enforcement Readiness**.
   d) Click **Enforce Ready**.
10. To put the security policy changes into effect immediately, click **Apply Policy**.
11. For a quick summary of system activity, look at the Overview screen (**Security** > **Overview** > **Application**).

    The Summary screen displays statistical information about Application Security traffic.

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

Flowchart for configuring XML security policy

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

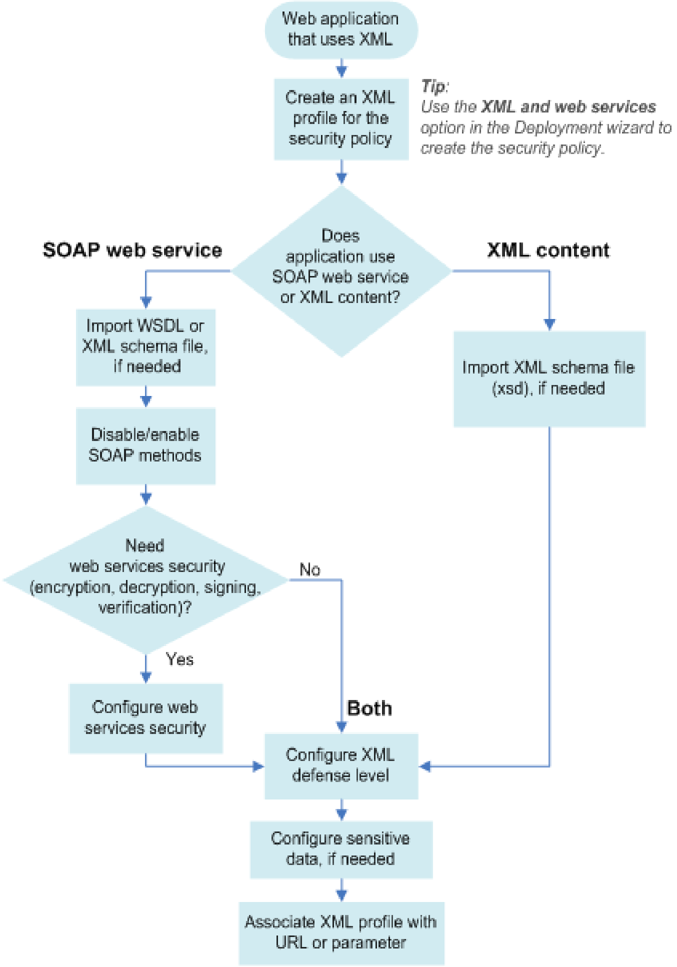
Web application that uses XML
Create an XML profile for the security policy
Tip:
Use the XML and web services option in the Deployment wizard to create the security policy.
Does application use SOAP web service or XML content?
SOAP web service
XML content
Import WSDL or XML schema file, if needed
Disable/enable SOAP methods
Import XML schema file (xsd), if needed
Need web services security (encryption, decryption, signing, verification)?
No
Yes
Configure web services security
Both
Configure XML defense level
Configure sensitive data, if needed
Associate XML profile with URL or parameter

Figure 1: Securing XML applications

Chapter 7

Using Rapid Deployment

Overview: Rapid deployment

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

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

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

Task summary

Creating a security policy using rapid deployment
Fine-tuning a security policy
Enforcing a security policy

Creating a security policy using rapid deployment

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

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

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

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

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

The Configure Local Traffic Settings screen opens.

4. Configure the new or existing virtual server, and click **Next**.

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

   The name of the new or existing virtual server becomes the name of the security policy.

   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 **Rapid Deployment security policy**.

   Some systems may include the option **Rapid Deployment security policy with Policy Builder enabled**. This option 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 **Enforcement Readiness Period**, retain the default setting of `7` days.

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

   During the enforcement readiness period, the security policy provides learning suggestions when it processes requests that do not meet the security policy; but the security policy does not alert or block that traffic, even if those requests trigger violations. You can review new entities and decide which are legitimate and include them in the security policy.
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), and only generate alerts for traffic that matches the signature. At the end of the staging period, the system automatically enforces the signatures that did not receive any hits.
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.

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

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 **Security** > **Application Security** > **Policy Building** > **Manual Traffic Learning**. The Manual Traffic Learning screen opens, and lists violations and learning suggestions that the system has made 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 Manual 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 Manual 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 put the security policy changes into effect immediately, click **Apply Policy**.
5. On the Main tab, click **Security** > **Overview** > **Application** > **Action Items**.
   The Action Items screen opens.
6. Examine the Action Items screen for information about recommended actions that you need to complete.
   a) Review the Suggested Action Items area, which lists system tasks and security policy tasks that should be completed.
   b) Click the links in the Suggested Action Items 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 Manual 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

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

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

1. On the Main tab, click **Security** > **Application Security** > **Blocking**.
   The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For the **Enforcement Mode** setting, select **Blocking**.
4. For each violation, review the settings so you understand how the security policy handles requests that cause the violation, and adjust if necessary.

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 system log (`/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.

   Tip: *Click the information icon preceding a violation for a description of it.*

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

   The security policy does not block traffic during the Enforcement Readiness Period even if violations occur.
9. If you want to block traffic that causes violations, you need to enforce violations. One way to do this is:
   a) Set the **Enforcement Readiness Period** to `0`.
   b) Click **Save**.
   c) On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Enforcement Readiness**.
   d) Click **Enforce Ready**.
10. To put the security policy changes into effect immediately, click **Apply Policy**.
11. For a quick summary of system activity, look at the Overview screen (**Security** > **Overview** > **Application**).

    The Summary screen displays statistical information about Application Security traffic.

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

Chapter

8

Using Application-Ready Security Templates

Overview: Using application-ready security templates

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

- Microsoft ActiveSync® 1.0, 2.0
- Microsoft Outlook Web Access Exchange® 2003, 2007, 2010
- Microsoft Outlook Web Access Exchange® with Microsoft ActiveSync® 2003, 2007
- 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.

Task summary

Creating a security policy from an application template
Fine-tuning a security policy
Enforcing a security policy

Creating a security policy from an application template

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

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

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

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

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

The Configure Local Traffic Settings screen opens.

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

   The name of the new or existing virtual server becomes the name of the security policy.

   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 **Security** > **Application Security** > **Policy Building** > **Manual Traffic Learning**.
   The Manual Traffic Learning screen opens, and lists violations and learning suggestions that the system has made 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 Manual 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 Manual 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 put the security policy changes into effect immediately, click **Apply Policy**.
5. On the Main tab, click **Security** > **Overview** > **Application** > **Action Items**.
   The Action Items screen opens.
6. Examine the Action Items screen for information about recommended actions that you need to complete.
   a) Review the Suggested Action Items area, which lists system tasks and security policy tasks that should be completed.
   b) Click the links in the Suggested Action Items 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 Manual 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

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

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

1. On the Main tab, click **Security** > **Application Security** > **Blocking**.
   The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For the **Enforcement Mode** setting, select **Blocking**.
4. For each violation, review the settings so you understand how the security policy handles requests that cause the violation, and adjust if necessary.

Option	Description
Learn	If selected, the system generates learning suggestions for requests that trigger the violation.

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

Tip: *Click the information icon preceding a violation for a description of it.*

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

   The security policy does not block traffic during the Enforcement Readiness Period even if violations occur.
9. If you want to block traffic that causes violations, you need to enforce violations. One way to do this is:
   a) Set the **Enforcement Readiness Period** to `0`.
   b) Click **Save**.
   c) On the Main tab, click **Security** > **Application Security** > **Policy Building** > **Enforcement Readiness**.
   d) Click **Enforce Ready**.
10. To put the security policy changes into effect immediately, click **Apply Policy**.
11. For a quick summary of system activity, look at the Overview screen (**Security** > **Overview** > **Application**).

    The Summary screen displays statistical information about Application Security traffic.

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

Appendix A

Security Policy Elements in Each Policy Type

Security policy elements included in each policy type

The elements that the system adds to a security policy depend on the policy type you select for automatic policy building. You can set the policy type when creating the security policy in the Deployment wizard or later by modifying the policy settings (**Security** > **Application Security** > **Policy Building** > **Settings** > **)**. When the policy type is set or modified, the Application Security Manager™ (ASM) assigns the Explicit Entities Learning settings as follows.

Table 1: Explicit Entities Learning Settings for Each Policy Type

Security policy element	Fundamental	Enhanced	Comprehensive	Vulnerability Assessment
File Types	Add All Entities	Add All Entities	Add All Entities	Never (wildcard only)
URLs	Never (wildcard only)	Selective	Add All Entities	Never (wildcard only)
Parameters	Selective (wildcard only)	Selective	Add All Entities	Never (wildcard only)
Cookies	Never (wildcard only)	Selective	Selective	Never (wildcard only)
Redirection Domains	Add All Entities	Add All Entities	Add All Entities	Add All Entities

Table 2: Explicit Entities Learning Settings

Setting	Description
Add All Entities	The Policy Builder includes all of the website entities. This option creates a large set of security policy entities with a granular object level configuration and high security level.
Selective	This option applies only to the * wildcard. When false positives occur, the system adds or suggests adding an explicit entity with relaxed settings. This option provides a good balance between security, policy size, and ease of maintenance.
Never (Wildcard Only)	When false positives occur, the system suggests relaxing the settings of the wildcard entity. This option creates a security policy that is easy to manage but may result in overall relaxed application security.

Depending on which policy type you select, ASM™ includes a different set of policy elements in the Automatic Policy Building Settings.

Table 3: Policy Elements

Security Policy element	Fundamental	Enhanced	Comprehensive	Vulnerability Assessment
HTTP Protocol Compliance	Yes	Yes	Yes	Yes
Evasion Techniques Detected	Yes	Yes	Yes	Yes

Security Policy element	Fundamental	Enhanced	Comprehensive	Vulnerability Assessment
File Type Lengths	Yes	Yes	Yes	No
Attack Signatures (Applies to policy, parameter, content profile, and cookie signatures)	Yes	Yes	Yes	Yes
URL Meta Characters	No	Yes	Yes	No
Parameter Name Meta Characters	No	No	Yes	No
Parameter Value Lengths	No	Yes	Yes	No
Value Meta Characters (for Parameters and Content Profiles)	No	No	Yes	No
Allowed Methods	No	Yes	Yes	Yes
Request Length Exceeds Defined Buffer Size	Yes	Yes	Yes	No
Header Length	Yes	Yes	Yes	No
Cookie Length	Yes	Yes	Yes	No
Failed to Convert Character	Yes	Yes	Yes	Yes
Content Profiles	No	Yes	Yes	No
Automatically detect advanced protocols	No	No; but Yes if JSON/XML payload detection selected	No; but Yes if JSON/XML payload detection selected	No
Host Names	Yes	Yes	Yes	Yes
CSRF URLs	No	No	Yes	Yes

Note: *In the table, Yes means the element is automatically included in the policy type; No means it is not included.*

Index