## **Oracle® Adaptive Access Manager** Proxy Web Publishing Configuration 10g (10.1.4.3.0)

December 2007



Oracle Adaptive Access Manager Proxy Web Publishing Configuration, 10g (10.1.4.3.0)

Copyright © 2007, Oracle. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

# Contents

Preface	4
Documentation	4
Introduction	6
Architecture	6
	_
web Publishing Rule Creation	/
Web Listener Creation	18
	. 10
Troubleshooting	. 23
	0

# **Preface**

The Oracle® Adaptive Access Manager Proxy Web Publishing Configuration provides information on creating web publishing rules and listeners so that Web applications and the WebUIO can be accessible from the Internet. The Oracle Adaptive Access Manager's Universal Installation Option (UIO) offers multi-factor authentication to Web applications without requiring any change to the application code. The Oracle® Adaptive Access Manager Proxy and The Oracle® Adaptive Access Manager Proxy Web Publishing Configuration are guides specific to the UIO deployment.

#### **Documentation**

The Oracle Adaptive Access Manager 10g documentation includes the following:

- The Oracle® Adaptive Access Manager API Integration Guide, which provides information on natively integrating the client portion of the Adaptive Risk Manager Online solutions. In an API integration, the client application invokes the Adaptive Risk Manager Online APIs directly and manages the authentication and challenge flows.
- The Oracle® Adaptive Access Manager Database Installation Guide (Oracle), which provides information about installing the Adaptive Access Manager schema into an Oracle database. Access to the Adaptive Access Manager schema is a requirement of the Adaptive Access Manager Application Server, which hosts the Adaptive Strong Authenticator and the Adaptive Risk Manager. Note that the Adaptive Manager Access Manager schema needs to be installed into the Oracle database before proceeding to the installation of the proxy.
- The Oracle® Adaptive Access Manager Database Installation Guide for SQL Server 2005, which provides information about installing the Adaptive Access Manager schema into SQL Server 2005. Access to the Adaptive Access Manager schema is a requirement of the Adaptive Access Manager Application Server, which hosts the Adaptive Strong Authenticator and the Adaptive Risk Manager. Note that the Adaptive Manager Access Manager schema needs to be installed into SQL Server 2005 before proceeding to the installation of the proxy.
- The Oracle® Adaptive Access Manager Proxy Integration Guide, which provides programming information and instructions on the installation of the Adaptive Access Manager proxy, one of the components in the Adaptive Access Manager UIO deployment. The Oracle Adaptive Access Manager's Universal Installation Option (UIO) offers multi-factor authentication to Web applications without requiring any change to the application code. The Oracle® Adaptive Access Manager Proxy and The Oracle® Adaptive Access Manager Proxy Web Publishing Configuration are guides specific to the UIO deployment.
- The Oracle® Adaptive Access Manager Proxy Web Publishing Configuration, which
  provides information on creating web publishing rules and listeners so that Web
  applications and the WebUIO can be accessible from the Internet. The Oracle
  Adaptive Access Manager's Universal Installation Option (UIO) offers multi-factor
  authentication to Web applications without requiring any change to the application
  code. The Oracle® Adaptive Access Manager Proxy and The Oracle® Adaptive
  Access Manager Proxy Web Publishing Configuration are guides specific to the UIO
  deployment.

- The Oracle® Adaptive Risk Manager Online Installation Guide, which provides information on the installation of the administration user interface of Oracle Adaptive Access Manager. Adaptive Risk Manager Online is the administration user interface of Oracle Adaptive Access Manager, a set of web-based administration tools that provides sophisticated fraud monitoring, analysis, and tracking by user location, device, time of day, type of transaction, as well as a host of other factors, and evaluates these factors against a set of customizable rules.
- The Oracle® Adaptive Access Manager LDAP Configuration Guide, which provides information on how to configure the Oracle Adaptive Access Manager Application Server to allow a user to be authenticated via a user identifier and password. The intended audience of this manual are users of WebLogic and Tomcat who want to use LDAP to set up users instead of the functionality in WebLogic and Tomcat.
- The Oracle® Adaptive Access Manager Import/Export Manual, which provides information importing groups, rule templates, and models from the Adaptive Access Manager schema.
- The Oracle® Adaptive Risk Manager Online Customer Care API Guide, which provides information about the Adaptive Risk Manager Online Customer Care API and provides the XML definition for each of the APIs.
- The Oracle® Adaptive Access Manager Database Tables Archiving and Purging Procedure, which provides information on the purge and archive scripts in the Oracle Adaptive Access Manager Database Tables of Microsoft SQL Server 2005. The procedure to trigger the scripts and information on verification and validation of script results are also provided.
- The Oracle® Adaptive Access Manager SQL Server Maintenance Guide, which provides instructions to set up The Oracle Adaptive Access Manager Maintenance Plan to purge and archive scripts in the Oracle Adaptive Access Manager database tables of Microsoft SQL Server 2005. The manual also discusses in detail how to trigger the scripts and provides information on the verification and validation of script results.
- The Oracle® Adaptive Risk Manager™ Administrator's Guide, which provides step-bystep instructions for creating and managing groups, creating models that contain rules, and customizing and managing rules.
- The Oracle® Adaptive Risk Manager<sup>™</sup> Dashboard and Reporting Guide, which provides detailed instructions on how to use the dashboard and reporting functionality within the Oracle® Adaptive Risk Manager Online. The Oracle® Adaptive Risk Manager Online includes a dashboard that provides a high-level overview of users and devices that have generated alerts and the alerts themselves, and it contains a comprehensive collection of reports on users, locations, devices, and security alerts.
- The Oracle® Adaptive Risk Manager™ Customer Care Administration Guide, which provides information on creating new customer cases and administering them.

## Introduction

Oracle Adaptive Access Manager's Universal Installation Option (UIO) offers added multifactor authentication to Web applications without requiring any change to application code. The purpose of this document is to explain the creation of web publishing rules and listeners in Microsoft ISA for Adaptive Access Manager Applications. This document is intended for integrators who install and configure Microsoft ISA to support multiple Web applications.

## Architecture

The following diagram shows an Adaptive Access Manager UIO deployment.



The Adaptive Access Manager proxy intercepts the HTTP traffic between the client (browser) and the server (web application) and performs appropriate actions, such as redirecting to the Adaptive Strong Authenticator, to provide multi-factor authentication and authorization. The Adaptive Strong Authenticator in turn communicates with Adaptive Risk Manager to assess the risk and takes the appropriate actions, such as permitting the login, challenging the user, blocking the user, and other actions.

The Adaptive Access Manager Proxy uses the API provided by Microsoft ISA Server to monitor the HTTP traffic and perform various actions. Microsoft ISA Server 2006 or 2004 Standard Edition should be installed and web publishing rules for web applications should be created before installing the Adaptive Access Manager Proxy. For the details on installing and configuring ISA server, refer to the Microsoft ISA Server setup documentation. Web publishing rule creation and listener creation are explained further in this document.

# Web Publishing Rule Creation

In a typical deployment, Web applications and the Adaptive Access Manager WebUIO run on machines in an internal network and are not directly accessible from the Internet. Only the Adaptive Access Manager Proxy machine, which runs Microsoft ISA Server, will be accessible from the Internet. Web applications can be made accessible from the Internet via Web publishing rules in the Microsoft ISA Server. This section provides steps-by-step instructions to create Web publishing rules.

To create a new web publishing rule:

1. Start Microsoft ISA management console: Start Menu > All Programs > Microsoft ISA Server > ISA Server Management.

The Internet Security & Acceleration Server screen appears.

🕮 Microsoft Internet Security and Acceleration Serve	r 2006			
Eile Action View Help				
Microsoft Internet Security and Acceleration Server 2006     BIGBANK-DEV     Monitoring     Firewall Policy     Wintal Private Networks (VPN)	Microsoft Internet Accelera Standard Edit	t Security & ation Server 2006	Firewall Policy	
🗄 🔆 Configuration	Ouden a	Name	Astian	Toolbox V Tasks V Help
		DieBael, see		Protocols
		ыуранк-арр	Allow	Users 🔘
	2	BigBank-Web-Uio	Sellow 🕑	Content Types 🛞
	🖃 💽 3	Allow-HTTP	⊘ Allow	<u>S</u> chedules 🛞
				Network Objects
		New - Edit Delete		
				The two results      The
	🛨 💽 4	Allow-Outbound	⊘ Allow	Computers
	Last	Default rule	S Deny	<ul> <li>□ Address Ranges</li> <li>□ Subnets</li> <li>□ Computer Sets</li> <li>□ URL Sets</li> <li>□ Domain Name Sets</li> <li>□ Web Listeners</li> <li>□ Web Listeners</li> <li>□ Bharosa Proxy Listener</li> <li>□ Server Farms</li> </ul>
Done				

2. In the left pane, expand the local machine name to display its sub tree.

3. Right click Firewall Policy and select New/Web Site Publishing Rule.

The New Web Publishing Rule Wizard appears.



4. When the New Web Publishing Rule Wizard appears, enter a name for the rule such as "Bharosa WebUIO" or "Online Banking Application" and click Next.

The Select Rule Action screen appears.

New Web Publishing Rule Wizard
Select Rule Action Specify how you want this rule to respond when the rule conditions are met.
Action to take when rule conditions are met:
< <u>B</u> ack <u>N</u> ext > Cancel

#### 5. Select Allow and click Next.

The Publishing Type screen appears.

New Web Publishing Rule Wizard 🛛 🗙
Publishing Type Select if this rule will publish a single Web site or external load balancer, a Web server farm, or multiple Web sites.
<ul> <li>Publish a single Web site or load balancer;</li> <li>Use this option to publish a single Web site, or to publish a load balancer in front of several servers.</li> <li>Help about <u>publishing a single Web site or load balancer</u></li> </ul>
<ul> <li>Publish a server <u>f</u>arm of load balanced Web servers</li> <li>Use this option to have ISA Server load balance requests between a server farm (mirrored servers).</li> <li>Help about <u>publishing server farms</u></li> </ul>
<ul> <li>Publish <u>m</u>ultiple Web sites</li> <li>Use this option to publish more than one Web site. A new rule will be created for each site published.</li> <li>Help about <u>publishing multiple Web sites</u></li> </ul>
< Back Next > Cancel

6. Select "Publish a single web site or load balancer" and click Next. The Server Connection Security screen appears.

New Web Publishing Rule Wizard	×
Server Connection Security Choose the type of connections ISA Server will establish with the publis server or server farm.	hed Web
<ul> <li>Use SSL to connect to the published Web server or server farm</li> <li>ISA Server will connect to the published Web server or server farm using HTTPS (recommended).</li> </ul>	https://
O Use non-secured connections to connect the published Web server or server farm ISA Server will connect to the published Web server or server farm using HTTP.	http://
When publishing over SSL, an appropriately named SSL server ce installed on the published server, or on each server in the server	rtificate must be farm.
Help about <u>server connection security</u>	
< <u>B</u> ack <u>N</u> ext >	Cancel

#### 7. Select one of the connection options and click Next.

- If the Web application is listening on SSL, select "Use SSL to connect to the published Web server or server farm."
- If the Web application is not listening on SSL, select "Use non-secured connections to connect to the published Web server or server farm."

The Internal Publishing Details screen appears for specifying the internal site name.

ew Web Publishing Rule V	lizard				×
Internal Publishing Det Specify the internal na	<b>ails</b> me of the Web	site you are publish	ing.		
The internal site name is th Typically, this is the name ir	e name of the W Iternal users typ	/eb site you are pul pe into their browse	blishing as it app ers to reach the	pears internally. Web site.	
Internal site name:	BIGBANK	-DEV			
ISA Server may not be able computer name or IP addre must be specified if ISA Ser Use a computer name of	to connect to ti is is specified. F ver cannot reso r IP address to (	he server hosting t for example, the co lve the internal site connect to the publ	ne published Wi mputer name o name. ished server	eb site unless its r IP address	
⊆omputer name or IP addr	ess:	192.168.63.87		Browse	]
		< <u>B</u> ack	Next >	Cancel	

- 8. Enter the internal site name for the Web application to be published. For a single Web site, this is typically the machine name where the Web server runs.
- 9. If the IP address or the machine name of the Web application to be published is known, select the checkbox "Use a computer name or IP address..." and enter the IP address or the machine name.
- 10. Click Next.

The Internal Publishing Details screen appears for specifying the path.

New Web Publishing Rule	Wizard	×
Internal Publishing De Specify the internal p can publish the entire	<b>tails</b> ath and publishing options of the published Web site. You Web site, or limit access to a specified folder.	
Enter the name of the file of within a folder use /*. Exar	or folder you want to publish. To include all files and subfolde nple: folder/*.	rs
Path (optional):	/*	
Based on your selection, th	ne following Web site will be published:	
Web site:	https://BIGBANK-DEV/*	
Forward the original ho name field on the previ	st header instead of the actual one specified in the Internal ous page	site
	< <u>B</u> ack <u>N</u> ext >	Cancel

### 11. Enter the name of the file or folder you want to publish and click Next.

To include all files and subfolders within a folder, enter /\*. If you need to publish more than one file or folder, enter only the first file/folder. The remaining files can be entered later by editing the rule.

The Public Name Detail screen appears.

New Web Publishing Rule Wi	zard
Public Name Details Specify the public domai published site.	n name (FQDN) or IP address users will type to reach the
<u>A</u> ccept requests for: Only requests for this public r	This domain name (type below):
Pyblic name:	www.bigbank-bharosa.com Example: www.contoso.com
Path (optional):	/*
Based on your selections, rec	quests sent to this site (host header value) will be accepted:
Site:	o://www.bigbank-bharosa.com/*
	< <u>B</u> ack <u>N</u> ext > Cancel

#### 12. Enter the path entered in the previous step in the Path field.

#### 13. From the Accept request for list, select one of the following items:

- To restrict access to the application using certain domain name(s) only, select "This domain name" and enter the domain name in the "Public name" field. If more than one domain needs to be permitted, enter only the first domain name. The remaining name can be entered later by editing the rule.
- To permit access without restriction on the domain name, select "Any domain name."
- 14. Click Next.

The Select Web Listener screen appears.

New Web Publishing Rule W	izard	×
Select Web Listener The Web listener specif computer listens for inc	ies the IP addresses and port on which the ISA Ser oming Web requests.	ver
Web listener:		
Bharosa Proxy Listener		<u>E</u> dit
Listener properties:		New
Property	Value	146
Description Networks Port(HTTP) Port(HTTPS) Authentication methods	External,Internal,Local Host 80 Disabled No Authentication	
	< <u>B</u> ack <u>N</u> ext >	Cancel

### 15. From the Web Listener list, select Bharosa Proxy Listener and click Next.

If the list is empty, create the listener by clicking "New" and following the instructions in the next section.

The Authentication Delegation screen appears.

New Web Publishing Rule Wizard 🛛 🗙
Authentication Delegation Authentication delegation is the method ISA Server uses to authenticate the session it opens with the published site.
Select the method used by ISA Server to authenticate to the published Web server:
No delegation, and client cannot authenticate directly
Description If the published Web server requests HTTP authentication, ISA Server will not pass the authentication request to the user. The user will not be able to authenticate to the published Web server. The client request will be denied.
Help about <u>authentication delegation</u>
< <u>B</u> ack <u>N</u> ext > Cancel

16. Select "No delegation and client cannot authenticate directly" from the list and click Next.

The User Sets screen appears.

New Web Publishing Rule Wizard	×
<b>User Sets</b> You can apply the rule to requests from all users. Or, you can limit acces specific user sets.	ss to
This rule applies to requests from the following user sets:	
All Users	<u>A</u> dd
	<u>E</u> dit
	<u>R</u> emove
1	
< <u>B</u> ack <u>N</u> ext >	Cancel

17. Confirm that only All Users is in the box and click Next.

If All Users is not in the list, update the User Sets using the Add and Remove buttons and click Next.

The Completing the New Web Publishing Rule Wizard screen appears.

New Web Publishing Rule Wiz	ard	×
Microsoft Internet Security & Acceleration Server 2006	Completing the New Web Publishing Rule Wizard	
	You have successfully completed the New Web Publishing Rule Wizard. The new Web Publishing Rule will have the following configuration:	
	Name: Online Banking Application Action: Allow Publishing Type Publish a single Web site. Connect the published Web server using HTTP5 Yes To close the wizard, click Finish.	
	< <u>B</u> ack Finish Cancel	

### 18. Double click the newly created rule.

The Online Banking Application Properties screen appears.

Online Banking Application Properties
Bridging Users Schedule Link Translation Authentication Delegation Application Settings General Action From To Traffic Listener Public Name Paths
<u>⊺</u> his rule applies to:
Requests for the following Web sites
Web sites and IP addresses:
www.bigbank-bharosa.com     Add      Edit <u>E</u> emove
Public web site names have to be registered with the Domain Name System (DNS). Help about <u>registering web site names with DNS</u>
OK Cancel Apply

19. If more than one file or folders need to be published, select the Paths tab and add all the paths.

Online Banking A	pplication P	roperties			? ×
Bridging Authentic General Action This rule app forwarding a it to the corre	Users ation Delegatio From To ies to requests request, ISA Se sponding intern	Sched n   Traffic   for these exte rver modifies   al path on the	ule   App  Listener   mal paths the extern Web serv	Link Trans lication Setting Public Name . Before al path and m ver.	slation gs e Paths aps
External Pai <same as="" in<br=""><same as="" in<br=""><same as="" in<br=""><same as="" in<br=""><same as="" in<="" td=""><td>th     ternal&gt; / ternal&gt; / ternal&gt; / ternal&gt; /</td><td>nternal Path /fauio40/* /fauio/* /edison/* /bigbank40/* /bigbank/*</td><td></td><td>Add Edit</td><td></td></same></same></same></same></same>	th     ternal> / ternal> / ternal> / ternal> /	nternal Path /fauio40/* /fauio/* /edison/* /bigbank40/* /bigbank/*		Add Edit	
I Paths must b another path. Example: /pa paths.	e distinct from e This is true for thA/* and /pat	ach other. A r external and i hB/* are distir	path cann nternal pa not externa	ot be a prefix ths. al and internal	of
		OK	Can	icel	Apply

20. To allow more than one domain name to be used to access the application, select the Public Name tab and add all the domain names.

Online Banking Application Properties	×
Bridging Users Schedule Link Translation Authentication Delegation Application Settings General Action From To Traffic Listener Public Name Paths	
I his rule applies to: Requests for the following Web sites ₩eb sites and IP addresses:	
www.bigbank-bharosa.com     Mgd     Agd     Edit <u>E</u> emove	
Public web site names have to be registered with the Domain Name System (DNS). Help about <u>registering web site names with DNS</u>	
OK Cancel Apply	

21. Select the Action tab.

Online Baı	nking Ap	plication	Proper	ties				? X
Bridg A General	ing   uthentica Action	Users tion Delega From T	tion	Sched   Traffic	lule   App Listener	Link lication 9 Public	Transla Settings Name	tion Paths
Action	i to take:							
• Aļ	ow							
O <u>D</u> e	eny							
Re the For	<u>B</u> edirect format h example	HTTP requ uests to an ttp://URL. : http://widy	alternatio gets.mici this rule	e Web p rosoft.co	b page: bage, Spe bom/denied	cify a loc 1.htm.	ation ir	
			0	К	Car	ncel	<u>A</u>	pply

22. Click the checkbox next to "Log requests matching this rule" to deselect it and click OK.

You return to the Internet Server & Acceleration Server screen.

🕮 Microsoft Internet Security and Acceleration Serve	er 2006					_ 🗆 ×
Eile Action View Help						
$\Leftarrow \rightarrow   \textcircled{1} \textcircled{1} \textcircled{2} \textcircled{2} \textcircled{3} \textcircled{3} \textcircled{3} \textcircled{3} \textcircled{3} \textcircled{3} \textcircled{3} 3$	۵. 💽 🖲 ۱					
Microsoft Internet Security and Acceleration Server 2006     BIGBANK-DEV     Monitoring     Firewall Policy     Virtual Private Networks (VPN)     Configuration	Microsoft* Internet Accelera Standard Edi	t Security & ation Server 2006 ion uply Discard	To save changes and	update the co	Firewall	Policy
	Firewall Po	licy			Toolbox Tasks Help	
	Order 🔺	Name	Action	Proto	Protocols	
	<b>_</b> ]1	BigBank-app	🥝 Allow	👰 ні	 Users	8
	2 🗐	BigBank-Web-Uio	⊘ Allow	🖳 н	Content Types	8
	<b>⊟ ?</b> 3	Allow-HTTP	🥝 Allow	00 6C 00 8C 00 н1 00 н1 00 н1	<u>Schedules</u> Network Objects New → Edit Delete	8
		Allow-Outbound	🥝 Allow	HI V All	Image: Metwork Sets Image: Computers	
	I Last	Default rule	S Deny	All	Address Ranges Subnets Computer Sets URL Sets URL Sets Domain Name Sets Web Listeners Sharosa Proxy List Server Farms	ener
-						
Done				ļ		

23. Click Apply.

# **Web Listener Creation**

To create a web listener:

1. Start Microsoft ISA management console: Start Menu > All Programs > Microsoft ISA Server > ISA Server Management.

The Internet Security & Acceleration Server screen appears.



- 2. In the left pane, expand the local machine name to display its sub tree.
- 3. Select Firewall Policy.
- 4. Click the Toolbox tab in the right pane.
- 5. Right click on Web Listeners and select New Web Listener.

The Welcome to the New Web Listener Wizard appears.

New Web Listener Definition	Wizard	×
Microsoft Internet Security & Acceleration Server 2006	Welcome to the New Web Listener Wizard This wizard helps you create a new Web listener. Web listeners specify how ISA Server listens for and authenticates incoming Web requests from clients.	
	<u>W</u> eb listener name: Bharosa Proxy Listener To continue, click Next.	
	<u> ≺ B</u> ack <u>N</u> ext > Cancel	

6. Enter Bharosa Proxy Listener in the Web Listener Name field and click Next. The Client Connection Security screen appears.

New Web Listener Definition Wizard
Client Connection Security Select what type of connections this Web Listener will establish with clients.
Bequire SSL secured connections with clients  ISA Server will publish servers only over HTTPS to the clients (recommended).
© Do not require SSL secured connections with clients ISA Server will publish servers over HTTP. Client credentials will be sent unencrypted to the ISA Server computer.
When publishing over SSL, an appropriately named SSL server certificate must be installed on the ISA Server computer.
Help about web listener client connections
< <u>B</u> ack <u>N</u> ext > Cancel

7. Select "Require SSL secured connections with clients" and click Next.

The Web Listener IP Addresses screen appears.

New Web Listener Definition Wizard	×
Web Listener IP Addresses Specify the ISA Server networks, and th will listen for incoming Web requests.	he IP addresses on those networks, that
Listen for incoming Web requests on these	networks:
Name	Selected IPs
🗹 🎯 External	<all addresses="" ip=""></all>
🗹 📥 Internal	<all addresses="" ip=""></all>
🗹 📥 Local Host	<all addresses="" ip=""></all>
🔲 📥 Quarantined VPN Clients	<all addresses="" ip=""></all>
Select.	IP <u>A</u> ddresses o clients through this Web Listener if the clients ssion.
	< <u>B</u> ack <u>N</u> ext > Cancel

8. Select External, Internal, and Local host and click Next.

The Listener SSL Certificates screen appears.

Use a <u>s</u> ingle certif	icate for this Web List	ener	Coloris Continents
sky-iis	/		Select Lettificate
Assign a certificat	e ror each IP address	C	0
II Address	NEWOIK	Jerver	Ceruncate
			Select Certificate

- 9. Select "Use single certificate for this Web Listener."
- 10. Click Select Certificate and install the certificate.
- 11. Click Next.

The Authentication Settings screen appears.

New Web Listener Definition Wizard		×
Authentication Settings Select how clients will authenticate to ISA Se their credentials.	erver, and how ISA Server will validate	
Select how clients will provide credentials to IS/	A Server:	
No Authentication		
Select how ISA Server will validate client crede	ntials:	
Mindows (Active Directory)	C RADIUS <u>O</u> TP	
C LDAP (Active Directory)	C RSA S <u>e</u> curID	
C RADIUS		
Help about authentication settings		
	< <u>B</u> ack <u>N</u> ext> C	Cancel

### 12. Select No Authentication from the list and click Next.

The Single Sign On Settings screen appears.



13. Click Next.

The Completing the New Web Listener Wizard screen appears.

New Web Listener Definition	Wizard	×
Microsoft Internet Security & Acceleration Server 2006	Completing the New Web Listener Wizard You have successfully completed the New Web Listener Wizard. The new listener will have the following configuration: Name: Bharosa Proxy Listener1 Client Connection: Secure (SSL/HTTPS) Listen on: External.Internal.Local Host Client Authentication Method: No Authentication SSD Enabled: No To close this wizard, click Finish.	
	< <u>B</u> ack Finish Cancel	

### 14. Click Finish.

The Internet Security & Acceleration Server screen appears.

Microsoft Internet Security and Acceleration Server	er 2006				
<u> Eile A</u> ction <u>V</u> iew <u>H</u> elp					
⇐ →   🖻 📧   😫 🖄 🏜 🚰 🗙 😔 📀 🔹	😥 🖲 🔹				
Microsoft Internet Security and Acceleration Server 2006     BigBANK-DEV     Monitoring     Sirewall Policy     Firewall Policy     Sirewall Policy     Configuration	Microsoft Interne Acceler Standard Ed	t Security & ation Server 2006 tion pply Discard	To save changes and	update the co	Firewall Policy
	Firewall Po	licy			Toolhox Tasks Hein
	Order 🔺	Name	Action	Proto	Protocols
	<b>e</b> 🛛 1	BigBank-app	🥝 Allow	Щні	<u>U</u> sers
	2 🧓	BigBank-Web-Uio	⊘ Allow	Щні	Content Types
	<b>=</b> 💽 3	Allow-HTTP	🧭 Allow	00 60 00 80 00 H1 00 H1 00 H1	Schedules     Image: Comparison of the sector
	🕀 📝 4	Allow-Outbound	🥝 Allow	🔍 All	Computers
	I Last	Default rule	O Deny	All	Address Ranges     Subnets     Computer Sets     Omputer Sets     Omain Name Sets     Web Listeners     John Sarosa Proxy Listener     Server Farms

15. Click Apply.

The Listener you just created is located under Network Objects/Web Listener.

# Troubleshooting

If you experience any problems:

- .Net2.0 Framework should be installed and enabled to successfully register the Bharosa Proxy DLL.
- Ensure the database access credentials are correct when the Firewall logging properties in Microsoft ISA use SQL Database as the Log Storage Format.
- It is recommended that you define IP Exceptions for Trusted IPs (like Router IP) when Flood Mitigation settings are enabled to mitigate flood attacks and worm propagation.