

# NetIQ Advanced Authentication Framework

# Smartphone Authentication Dispatcher Installation Guide

Version 5.1.0

# Table of Contents

	1
Table of Contents	2
Introduction	
About This Document	
System Requirements	4
Installing and Removing Smartphone Authentication Dispatcher	
Installing Smartphone Authentication Dispatcher	5
Removing Smartphone Authentication Dispatcher	9
Microsoft Windows 7/Microsoft Windows Server 2008 R2	9
Microsoft Windows Server 2012	
Configuring Smartphone Authentication Dispatcher	10
Configuring Smartphone Authentication Dispatcher via Group Policy	11
Configuring Smartphone Authentication Dispatcher to Work Through HTTP Proxy	14
Multiple Dispatchers Support in v4.10 R3	15
Multiple Dispatchers Support Configuration	15
Smartphone Dispatcher Configurer	16
Dispatchers Database	17
Collision	19
Time Synchronization	19
Internal State Synchronization	
Multiple Dispatchers Support in v4.11	21
Multiple Dispatchers Support Overview	
Installing Application Request Routing	23
Configuring Application Request Routing	
Migrating Smartphone Authentication Dispatcher	
Index	

## Introduction

#### **About This Document**

### **Purpose of the Document**

This Smartphone Authentication Dispatcher Installation Guide is intended for all system administrators and describes how to use the client part of NetlQ Advanced Authentication Framework solution. In particular, it gives instructions as for how to install Smartphone Authentication Dispatcher.

For more general information on NetlQ Advanced Authentication Framework<sup>™</sup> and the authentication software you are about to use, see NetlQ Advanced Authentication Framework – Client User's Guide.

Information on managing other types of authenticators is given in separate guides.

### **Document Conventions**

**Warning.** This sign indicates requirements or restrictions that should be observed to prevent undesirable effects.

Bimportant notes. This sign indicates important information you need to know to use the product successfully.

**ONOTES.** This sign indicates supplementary information you may need in some cases.

**?** Tips. This sign indicates recommendations.

- Terms are italicized, e.g.: *Authenticator*.
- Names of GUI elements such as dialogs, menu items, buttons are put in bold type, e.g.: the **Logon** window.

# System Requirements

The following system requirements should be fulfilled:

• Microsoft Windows Server 2008 R2 SP1/Microsoft Windows Server 2012

# Installing and Removing Smartphone Authentication Dispatcher

NetIQ Advanced Authentication Framework<sup>™</sup> package includes Smartphone authentication dispatcher, which is responsible for establishing connection between the NetIQ Smartphone Authenticator and Smartphone authentication provider

After the upgrade of Smartphone Authentication Dispatcher v1.1.32 and earlier to v.1.1.44 and later, the push messaging will not work during up to 6 hours and the app will need to be opened manually. After that time, if during 6 hours after upgrade the app was not opened, it must be opened manually for the first time.

#### **Installing Smartphone Authentication Dispatcher**

**Smartphone Authentication Dispatcher** is designed to provide connection between the NetIQ Smartphone Authenticator and Smartphone authentication provider. Smartphone Authentication Dispatcher receives HTTP requests from a mobile device that is running the mobile part of NetIQ. Also it serves requests from Smartphone authentication provider.

Moreover Smartphone Authentication Dispatcher transfers Push Notifications to mobile devices that are running NetIQ Smartphone Authenticator through the special proxy-server (proxy.authasas.com).

Smartphone Authentication Dispatcher monitors the status of authentication and provides special APIs for BSP (and other exterior applications). It performs a range of tests that verify data authenticity.

😵 Only one Smartphone Authentication Dispatcher can be installed in an environment.

Before the installation of Smartphone Authentication Dispatcher make sure that .NET Framework 4.5 is installed on your computer.

Smartphone Authentication Dispatcher should have the Internet access (it should have an access to proxy.authasas.com via https protocol, port 443).

The start of installation may be frozen for a time up to 1 minute in the case of offline mode. This delay occurs due to check of digital signature of component.

😵 Smartphone Authentication Dispatcher can be installed on the server only.

To install Smartphone Authentication Dispatcher:

1. Run **SaDispatcher.msi**. The **Smartphone Authentication Dispatcher Setup** window will be displayed.

Smartphone Authentication Dispatcher Setup						
S	Welcome to the Smartphone Authentication Dispatcher Setu	o Wizard				
	The Setup Wizard will install Smartphone Authors Dispatcher on your computer. Click Next to co Cancel to exit the Setup Wizard.	entication ntinue or				
	Back Next	Cancel				

2. Click **Next** to install to the default folder or click **Change** to choose another.

Smartphone Authentication Dispat	tcher Setup	
Destination Folder		
Click Next to install to the default fold	er or dick Change to choose another.	
Install Smartphone Authentication Dispa	atcher to:	
-		
C:\Program Files\SAD\		
Change		
	Back Next	Cancel

3. Click **Install** to begin the installation. Click **Back** to review or change any of your installation settings. Click **Cancel** to exit the wizard.

🝘 Smartphone Authentication Dispatcher Setup	
Ready to install Smartphone Authentication Dispatcher	Ð
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.	
Back Install	Cancel

4. Please wait while the Setup Wizard installs Smartphone Authentication Dispatcher.



5. Click the **Finish** button to exit the Setup Wizard.



#### **Removing Smartphone Authentication Dispatcher**

In this chapter:

- Microsoft Windows 7/Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012

Microsoft Windows 7/Microsoft Windows Server 2008 R2

- 1. In the Start menu, select Control panel and then double-click Programs and Features.
- 2. Select Smartphone Authentication Dispatcher and click Uninstall.
- 3. Confirm the removal.
- 4. Wait a few seconds until the removal is completed.

#### **Microsoft Windows Server 2012**

- 1. In the Search menu, select Apps > Control Panel > Programs > Programs and Features.
- 2. Select Smartphone Authentication Dispatcher and click Uninstall.
- 3. Confirm the removal.
- 4. Wait a few seconds until the removal is completed.

## **Configuring Smartphone Authentication Dispatcher**

In this chapter:

- <u>Configuring Smartphone Authentication Dispatcher via Group Policy</u>
- Configuring Smartphone Authentication Dispatcher to Work Through HTTP Proxy
- Multiple Dispatchers Support In v4.10 R3
- Multiple Dispatchers Support In v4.11

#### Configuring Smartphone Authentication Dispatcher via Group Policy

After the installation of both server components (SaDispatcher.msi and SaProvider.msi), the Smartphone Authentication Dispatcher policy will be successfully added to Group Policy Management Editor. To activate a policy:

- In Group Policy Management Editor, double-click the policy name.
- In the properties dialog, click **Enabled**.

The **Smartphone Authentication Dispatcher** policy allows you to configure Dispatcher API interfaces. It has the following options:

- Protocol and address of Dispatcher interface that intended for serving SaProvider requests. Supported protocols are 'http' and 'https'.
- Protocol and address of Dispatcher interface that intended for serving MOBILE requests. Supports 'http' protocol only. It is the "endpoint" which will accept connections from mobile devices.
- URL to load into mobile devices during enrollment. This URL will be used by device to access to the Dispatcher from 3G/WI-FI. This address will be encoded into QR code, scanned by mobile device and used by it to connect to Smartphone authentication Dispatcher.
- List of dispatchers. Should contain semicolon separated IP's or DNS names (in case of multiple dispatchers).
- TCP port number on which the dispatcher should accept connections from Smartphone AD service.

To save changes, click the **Apply** button.

💭 Smartphone Authentication Dispat	cher policy		<u> </u>
Smartphone Authentication Dispate	cher policy	Previous Setting Next Setting	
Not Configured     Comment:			<u> </u>
Enabled			
C Disabled			-
Supported on:			<u> </u>
Options:	1	Help:	
Protocol and address of Dispatcher inte intended for serving SaProvider request protocols are 'http', 'https'. The address http://dispatcher:port/ or https://dispa http://11.0.8.250/bsp/ Protocol and address of Dispatcher inte	erface that ts. Supported is should be tcher:port/.	Smartphone Authentication Dispatcher Policy allows you to configure Dispatcher API interfaces.	4
intended for serving MOBILE requests. 'http' protocol only.	Supports		
URL to load into mobile devices during This URL will be used by device to acce Dispatcher from 3G/Wi-Fi.	enrollment. ss to the		
http://11.0.8.250/mobile/			
List of dispatchers. Should contain sem separated IPs or DNS names.	icolon		
127.0.0.1			
TCP port number on which the dispatch accept connections from Smartphone A	ner should AD service		
6000			<b>•</b>
		OK Cancel A	pply

The changes take effect after group policy refresh and restart of Smartphone authentication dispatcher.

While upgrading Smartphone Authentication Dispatcher from v.1.1.32 and below to v.1.1.44 and above, it is required to change 'rpc' protocol to 'http' in policy settings.

So Try to open the URL from the **DispExternalMobileInterface** parameter together with the specified port number in browser on the smartphone. There should be displayed the following message: "*Smartphone dispatcher is running*".

After the installation of Smartphone authentication dispatcher, the cluster mode is disabled by default .

It is required to specify an applicable value for the **DisplpList** parameter only in case of multiple dispatchers.

To disable an applicable Dispatcher interface, specify the **disabled** value in the registry for the corresponding parameter. As a result the disabled interface will not be started after the launch of Smartphone authentication dispatcher.

To access the Smartphone Authentication Dispatcher policy in the Group Policy Management Editor console, expand the following path: Computer Configuration -> Policies -> Administrative Templates -> Smartphone Authentication Dispatcher.

#### Registry settings:

HKEY\_LOCAL\_MACHINE\SOFTWARE\(Wow6432Node\)Policies\BioAPI\BSP\SaDispatcher **DispBspInterface**:

- value type: REG\_SZ
- value data: http:<IPAddressForBSPConnections>:<port>
- description: rpc:<IPAddressForBSPConnections>:<port> is protocol and address of Dispatcher interface that are intended for serving SaProvider requests

#### **DispDataPort**:

- value type: REG\_DWORD
- value data: 0x00001770 (6000)
- description: 6000 displays the TCP port number that is used to accept connections from Smartphone AD service

#### DispExternalMobileInterface:

- value type: REG\_SZ
- value data: http://<ExternalIPForMobileConnections>:<port>
- description: http://<ExternalIPForMobileConnections>:<port> is URL to load into mobile devices during enrollment

#### DisplpList:

- value type: REG\_SZ
- value data: http://<DispatcherIPAddress>
- description: http://<DispatcherIPAddress> is IP address of an applicable dispatcher

#### **DispMobileInterface**:

- value type: REG\_SZ
- value data: http://<IPAddressForMobileConnections>:<port>/
- description: http://<IPAddressForMobileConnections>:<port>/ is protocol and address
  of Dispatcher interface that are intended for serving mobile requests

# Parameters enclosed in angle brackets (<parameter>) should be replaced with applicable values (including angle brackets).

 $\mathfrak{S}$  These settings should be applied on Authenticore Server and workstations.

### Configuring Smartphone Authentication Dispatcher to Work Through HTTP Proxy

To configure Smartphone Authentication Dispatcher to work through HTTP proxy, follow the steps:

- 1. Open the SaDispatcher.exe.config file.
- Add proxyAddress="<IP address of http proxy><port>" and useDefaultProxy="false" attributes to the <binding> tag. E.g.:

```
<system.serviceModel>
<bindings>
<basicHttpBinding>
<br/><binding name="BasicHttpsBinding_IPushSenderProxy"
closeTimeout="00:00:05" openTimeout="00:00:05" receiveTimeout="00:00:05"
sendTimeout="00:00:05"
proxyAddress="http://<IP Address>:<port>" useDefaultWebProxy="false">
<security mode="Transport"/>
</binding>
</basicHttpBinding>
</bindings>
<client>
<endpoint address="https://proxy.authasas.com/OobProxy/Service.svc"
binding="basicHttpBinding" bindingConfiguration="BasicHttpsBinding_IPushSenderProxy"
contract="IPushSenderProxy" name="BasicHttpsBinding_IPushSenderProxy"/>
</client>
</system.serviceModel>
```

#### Multiple Dispatchers Support in v4.10 R3

Multiple dispatchers support provides with an opportunity of exchanging updates between dispatchers and keeping data in actual state. In case of installation of several dispatchers, the workflow will be the following:

- The main dispatcher receives data which should be saved in the local database (a new device registration information, push ID update from the registered device, etc.).
- The main dispatcher writes new data in its local database.
- The main dispatcher sends notifications to all specified subsidiary dispatchers.
- All subsidiary dispatchers load updates from the main dispatcher.

In this chapter:

- Multiple Dispatchers Support Configuration
- Smartphone Dispatcher Configurer
- Dispatchers Database
- <u>Collision</u>
- Time Synchronization
- Internal State Synchronization

#### Multiple Dispatchers Support Configuration

To configure multiple dispatchers support:

- 1. For the main dispatcher:
  - Open the SaService.exe.config file on the server.
  - Specify the following values:

    - <add key="DispMobileInterface" value="disabled"/>
    - <add key="DispExternalMobileInterface" value=""/>
    - <add key="DispSyncInterface" value="https://<IPAddressForSynchronization>:
       <port>"/>
  - Save the file.

C The **DispMobileInteface** value should be set to **disabled**. Otherwise the dispatcher will use the value that is specified in the **Smartphone Authentication Dispatcher** policy.

- 2. For the subsidiary dispatcher:
  - Open the **SaService.exe.config** file on the server.
  - Specify the following values:
    - <add key="DispBspInterface" value="disabled"/>
    - <add key="DispMobileInterface" value="http://<IPAddressForMobileConnections>:<port>"/>
    - <add key="DispExternalMobileInterface" value=""/>
  - Save the file.

The **DispBspInterface** value should be set to **disabled**. Otherwise the dispatcher will use the value that is specified in the **Smartphone Authentication Dispatcher** policy.

Cluster options are not related to any of the domain policies because cluster nodes work outside the domain infrastructure.

All dispatchers use a special network interface for communication with each other. To configure it, it is required to specify the same **DispSyncInterface** value in the **SaService.exe.config** file for every dispatcher.

The **externaldisps.txt** file is used for storing configuration information about all dispatchers. This file contains URI and password for each of dispatchers. When the dispatcher starts, it reads this file, finds itself and gets a password to use it in decryption of incoming messages. All dispatchers know all passwords and use them during synchronization exchange.

#### Smartphone Dispatcher Configurer

B It is highly recommended to use configuration tool instead of direct modification of **SaService.exe.config** file.

The **Smartphone dispatcher configurer** is intended to avoid the modification of **SaService.exe.config** file. The modified **SaService.exe.config** file will be replaced by next update and all configured options will be lost.

The **Smartphone dispatcher configurer** has a single window which is split into two text areas:

- The Local parameters text area contains configurable parameters and comments.
- The **Cluster members** text area contains the cluster node list.

SaService.exe.config file.

Smartphone dispatcher of	configurer – 🗖 🗙
Dispatcher ID	
2c1d98e1-d9c7-4b80-b28b-369db3fbed38	Restart dispatcher Start dispatcher Stop dispatcher
Local parameters (override policies)	Cluster members DispSyncInterfaces and passwords list
# These options override Smartphone policy settings.	# External dispatchers which will work together : ^
# For comments and to turn off a line please use # symbol.	# Sync interface looks like HTTP URI. Password c
# To disable any of these interfaces and WCFs services use "disable"	# Each dispatcher which should work in cluster ma
# 17/ 7	# After the dispatcher started, it loads this fill
#DispBspInterface rpc:0.0.0.0:10114	# will use the password to decrypt all incoming :
#DispMobileInterface http://0.0.0.08756	# DO NOI FORGEI IO CONFIGURE Sabispathcer.exe.col
Dispsyncinterrace http://0.0.0.0:6000	#
#	# nup://address:port/ password
# External mobile interface address which will be added into QK	http://172_16_0_155:6000/
#	http://172.16.0.109:6000/ paw0
* # Dispatchers which are running together in cluster mode should	# http://172.16.0.154:6000/ psw2
ExternalDispatchersListFile ~/externaldisps.txt	
Save params	Load cluster list Save cluster list

After specifying all required parameters, click the **Save params** button to save the configuration. Then click **Restart dipatcher**.

The **Smartphone dispatcher configurer** saves parameters to the predefined **props.config** file. This file will not be overwritten during update. All parameters, that are specified in the **props.config** file, override parameters specified in the **Smartphone Authentication Dispatcher** policy and **SaService.exe.config** file.

#### **Dispatchers Database**

Dispatchers have their own local databases. Every row in the database of the main dispatcher contains the following servicing records:

- **GUID** global unique identifier;
- **DT** date and time of adding or updating the record;
- **Version** data version of the added or changed record.

In case of multiple dispatchers installation, the main dispatcher will exchange all updates and all data will be kept in actual state.



- 1. Dispatcher A receives data that should be saved into the local database (new device registration information or push ID update from the registered device).
- 2. Dispatcher A writes new data to its local database.
- 3. Dispatcher A sends notifications to all known dispatchers.
- 4. All known dispatchers load updates from dispatcher A.
- 5. All known dispatchers write new data to their local databases.
- 🚺 Any known dispatcher can act as the main dispatcher (dispatcher A).

The data version number is incremented every time the data is changed in the database. After the data is changed, the main dispatcher runs a set of background threads which send notifications to all subsidiary dispatchers. The notification contains source dispatcher ID and data version. The subsidiary dispatcher, which received a notification, checks the last stored data version of the main dispatcher. If the received data version is newer than the stored version, the dispatcher finds the sender's URI by known sender ID. When the URI has been found, the subsidiary dispatcher asks the main dispatcher for data changes, which were done between last known data version and the version from notification. The main dispatcher sends an answer with a set of required data.

#### Collision

Collision is a situation when the subsidiary dispatcher gets an update from the main dispatcher and this update contains a record with the same GUID as a record which the main dispatcher contains already in its database. In this situation the subsidiary dispatcher compares DT fields to decide which of these two records is newer. Only newer records will be accepted.

#### **Time Synchronization**

Each dispatcher asks the configured NTP server (by default <u>time.windows.com</u>) every 3600 seconds during its work. The time received from NTP server is used to calculate a correction for a system. All data records contain the corrected time.

😵 The value of time synchronization can be changed in the configuration file.

#### Internal State Synchronization

Internal state of the dispatcher is a set of authentication statuses and their synchronization objects. Unlike the data synchronization, internal state synchronization works with locks. It means that every event which comes to the main dispatcher from outside (except subsidiary dispatchers) causes a sequence of communications between the main dispatcher and subsidiary dispatchers. After the data update on all secondary dispatchers, the main dispatcher changes its internal state in accordance with received event.

As a result the dispatcher can support distributed Smartphone authentication. E.g., NetIQ Smartphone Authenticator can request salt from the main dispatcher, and after that NetIQ Smartphone Authenticator can send authentication answer to one of the subsidiary dispatchers.



### Multiple Dispatchers Support in v4.11

Starting from NetIQ Advanced Authentication Framework v4.11 multiple dispatchers support is available only through ARR/IIS.

In this chapter:

- Multiple Dispatchers Support Overview
- Installing Application Request Routing
- <u>Configuring Application Request Routing</u>

#### Multiple Dispatchers Support Overview

Both NetIQ Smartphone Authenticator and Smartphone authentication provider should have access to Smartptone authentication dispatcher through ARR/IIS.

Smartphone AD service is intended to serve extended AD/LDS scheme which stores Push ID. Push ID is a variable data. It is used to send popup (push) notifications. Smartphone AD service connects to all dispatchers whose IP addresses are included into the <u>Smartphone</u> <u>Authentication Dispatcher policy</u>. Smartphone AD service uses the same TCP port for all dispatchers. The dispatcher and the AD service interact with each other throug RPC protocol.

The figure below illustrates the Smartphone authentication dispatcher workflow.



The next figure illustrates Smartphone authentication dispatcher workflow when Smartphone AD service is installed on multiple machines.



#### Installing Application Request Routing

To install ARR and all its components in the appropriate order, use the Microsoft Web Platform Installer. Follow the steps:

- 1. Go to the Official Microsoft IIS Site.
- 2. Open the <u>Application Request Routing</u> page and click **Install this extension**.
- 3. Click Install Now. The installation file will be downloaded on your computer.
- 4. Run the installation file. The Web Platform Installer will be launched.
- 5. Click Install.
- 6. Click **I accept** if you agree to the license terms of the third party and Microsoft software. Wait until the components are installed.
- 7. View the list of products that were installed. Click **Finish**.
- 8. Click Exit to close the Web Platform Installer.

### **Configuring Application Request Routing**

After the installation of Application Request Routing, it is required to create a Server Farm and add dispatchers to it.

To configure Application Request Routing, follow the steps:

1. Open IIS Manager and expand the nodes in the **Connections** pane.

2		Internet Information S	ervices (IIS) Manager	_ 🗆 🗙
	ver Farms 🔸			🖸 🖂 🏠 🔞 •
File View Help				
Connections	Server Farms			Actions
				 Create Server Farm
ASmith (ASmith (Ann)	Name	Status		Help
	Features View 💦 Content View			
Ready				¶.:

- 2. Right-click **Server Farm** and then click **Create Server Farm**. The **Create Server Farm** wizard launches.
- 3. On the **Specify Server Farm Name** page, enter the name of the server farm. Click **Next** to continue.

Create Server Farm	?	×
Specify Server Farm Name		
Server farm name: Dispatchers  ✓ Online		
Previous Next Finish	Cance	2

4. On the **Add Server** page, enter the dispatcher IP address. Click **Add**.

	Crea	te Server Fai	rm		?	×
Add Server						
Server address:			Add	1		
✓ Online			Add			
Advanced settings			Remove			
Server Address Sta	atus					
	P	revious	Next	Finish	Cancel	

5. Enter IP addresses of other dispatchers. When you are finished adding servers to the farm, click **Finish**.

		Create Serv	er Farm		? ×
Add Server					
Server address:			Add		
✓ Online Advanced settings			Remove	]	
Server Address	Status				
172.16.0.156	Online				
172.16.0.155	Online				
	[	Previous	Next	Finish	Cancel

6. The **Rewrite Rules** dialog box is displayed. Click **No** to create the rule later.



7. Expand the **Server Farms** node and click the name of the created farm. Double-click the **Routing Rules** item on the **Server Farm** page.

8	Internet Information Services (IIS) Manager	- 🗆 🗙
€ → ASmith → Se	rver Farms → Dispatchers →	🔯 🖂 🟠 i 🕢 🗸
File View Help		
Connections	Conver Form	Actions
2		🗙 Remove Server Farm
Asmith (Asmith\Ann)	Group by: Area	Take Server Farm Offline
Sites	Server Farm	Add Servers
Server Farms		
	Caching Health Test Load Balance Monitoring Proxy Routing Server	
	Features View 🕼 Content View	
Ready		• <u>1.</u> :

8. On the Routing Rules page, select the **User URL Rewrite to inspect incoming requests** and **Enable SSL offloading** checkboxes. Click **Apply** in the **Actions** pane to save changes.

<b>8</b> ]	Internet Information Services (IIS) Manager	- • ×
G → ASmith → Se	nver Farms → Dispatchers →	🖸 🛛 🟠 🔞 🗸
File View Help		
Connections	Routing Rules         Use this feature to define simple URL Rewrite rules in Application Request Routing. For advanced scenarios, follow the URL Rewrite link.         Routing         I Use URL Rewrite to inspect incoming requests         I Enable SSL offloading         Requests with the following extensions are not forwarded:         Example: *.jpg, *.css, *.gif         Requests with the following patterns are not forwarded:         Example: /images/*, */templates/*	Actions       Apply       Cancel       Advanced Routing       URL Rewrite       Help
Configuration: 'localhost' application	Host.config	9 <u>1.</u> ;

9. After the saving the changes, click **URL Rewrite** in the **Advanced Routing** subsection of the **Actions** pane.

8) 	Internet Information Services (IIS) Manager	- 🗆 🗙
G → ASmith → Se	nver Farms → Dispatchers →	🖸 🐼 🟠 🔞 🗸
File View Help		
Connections Asmith (ASmith)(Ann) Asmith (ASmith)(Ann) Connection Pools Connection	Souting Rules         Use this feature to define simple URL Rewrite rules in Application Request Routing. For advanced scenarios, follow the URL Rewrite Infine.         Routing         Image: Im	Alerts The changes have been successfully saved. Actions Apply Cancel Advanced Routing URL Rewrite P Help
Configuration: 'localhost' application	Host.config	<b>1</b> .:

10. On the **URL Rewrite** page, click **Add Rule(s)** in the **Actions** pane.

<b>6</b> ]	Internet Information Services (IIS) Manager – 🗖 🔀							
€ 🧿 📲 → ASmith →								😰 🛛 🟠 🕡 •
File View Help								
Connections	URL Rewrite           Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.           Inbound rules that are applied to the requested URL address:						Actions Add Rule(s) Manage Server Variables View Server Variables	
▲ ∰ Server Farms	Name	Input		Match	Pat	tern		Manage Providers
Dispatchers	ARR_Dispatchers_loadb	URL Path		Matches	*			View Providers
								Outbound Rules
								View Preconditions
								View Custom Tags
	<						>	🕑 Help
	Outhound rules that are applied t	o the headers of t	he content of a					
	Name	Input	Match	Pattern	Action Type	Action Value	C+	
	Name	input	Watch	Pattern	Action Type	Action value	30	
	×						7	
	Features View 🕞 Content View	v						
Configuration: 'localhost' application	Host.config							¶.:

11. In the **Add Rule(s)** window, select **Blank rule** to create a new inbound rule without any preset values. Click **OK** to continue.

Add Rule(s)	?	×
Select a rule template:		
Inbound rules       Blank rule     Rule with rewrite map       Request blocking		
Inbound and Outbound Rules           Inbound and Outbound Rules           Image: State of the st		-
Outbound rules		
Search Engine Optimization (SEO)		
Select this template to create a new inbound rule without any preset values. This template opens the "Edit Ru you can use to define a new rewrite rule for changing the requested URL address.	le" page	that
ОК	Cancel	

- 12. On the **Edit Inbound Rule** page, specify the name of the new rule.
- 13. In the **Match URL** group box, do the following:
  - Select Matches the Pattern from the Requested URL dropdown.
  - Select Regular Expressions from the Using dropdown.
  - Specify the .\* value in the **Pattern** text field.
  - Select the **Ignore case** checkbox.

Internet Information Services (IIS) Manager	- 🗆 🗙
Solution → ASmith →	🛂 🖂 🚱 •
File View Help	
Pile View Help     Connections	Actions Apply Cancel Back to Rules Help
Configuration: 'localhost' applicationHost.config	• <u>1</u> .:

14. In the **Conditions** group box, click the **Add** button to add a condition.

<b>6</b>	Internet Information Services (IIS) Manager						- 🗆 🗙	
G → ASmith →							🛂 🖂 🚱 •	
File View Help								
File     View     Help       Connections       Image: Connections	Conditions Logical groupi Match All	Edit Inbound Rule         Ignore case         Conditions         Logical grouping:         Match All         Input       Type         Pattern         Input					Actions Apply Cancel Back to Rules Help	
	Track capt	ure groups across conditio	ins		Move Down	*		
Configuration: 'localhost' application	Host.config						¶.:	

- 15. In the Add Condition window, perform the following actions:
  - Specify the **{HTTP\_COOKIE}** value in the **Condition input** text field.
  - Select Matches the Pattern from the Check if input string dropdown.

- Specify the **ASASession=([0-9,A-Fa-f]+)** value in the **Pattern** text field.
- Click **OK** to continue.

Add Conditio	on ? ×
Condition input: {HTTP_COOKIE}	
Check if input string: Matches the Pattern	
Pattern: ASASession=([0-9,A-Fa-f]+)	Test pattern
✓ Ignore case	
	OK Cancel

16. In the **Server Variables** group box, click the **Add** to set server variable.

Internet Information Services (IIS) Manager	- 🗆 🗙
Solution → ASmith →	📴 🖂 🟠 I 🕡 🔹
File View Help	
Connections	Actions Apply
Configuration: 'localhost' applicationHost.config	<b>9</b> 1.:

- 17. In the Set Server Variable window, perform the following actions:
  - Specify the **LB\_COOKIE** value in the **Server variable name** text field.
  - Specify the **{C:1}** value in the **Value** text field.
  - Click **OK** to continue.

Set Server Variable ?	×
Server variable name:	
LB_COOKIE	•
Value:	
{C:1}	
Replace the existing value	
OK Cance	

- 18. In the **Action** group box, perform the following actions:
  - Select Route to Server Farm from the Action type dropdown.
  - Select the Stop processing of subsequent rules checkbox.
  - Click **Apply** in the **Actions** pane to save changes.

<b>V</b> ]	Internet Information Services (IIS) Manager – 🗖 🔼							
G → ASmith →			🔤 🖂 🙆 •					
File View Help								
Connections	Gill Edit Inbound Rule		Actions					
Asmith (ASmith\Ann) Application Pools Sites Server Farms 	Action       Move Up         Action type:       Move Down         Action Properties       Scheme:         Scheme:       Server Farm:         Path:       //(R:0)         Intp://v       Dispatchers         Stop processing of subsequent rules		<ul> <li>in Apply</li> <li>in Cancel</li> <li>in Back to Rules</li> <li>in Help</li> </ul>					
Configuration: 'localhost' applicationH	lost.config		• <b>1</b> .:					

- 19. Click the name of the farm in the **Connections** pane.
- 20. On the Server Farm page, double-click the Load Balance item.



- 21. On the **Load Balance** page, perform the following actions:
  - Select Server variable hash from the Load balance algorithm dropdown.
  - Specify the LB\_COOKIE value in the Server variable text field.
  - Click Apply in the Actions pane to save changes.

<b>6</b> ]	Internet Information Services (IIS) Manager	- 🗆 🗙
G → ASmith → Se	🖸 🛛 🟠 🔞 🗸	
File View Help		
Connections Asmith (Asmith (Ann)) Asmith (Asmith (Ann)) Constant of the second seco	Image: Content View	Actions       Actions       Apply       Cancel       Image: The point of the point o
Configuration: 'localhost' application	Host.config	¶1.:

- 22. Click the name of the server farm and double-click the **Routing Rules** item.
- 23. On the **Routing Rules** page, click **URL Rewrite** in the **Advanced Routing** subsection of the **Actions** pane.
- 24. Select the default rule (ARR\_Dispatchers\_loadbalance). Click **Move Down** in the **Inbound Rules** subsections of the **Actions** pane.

<b>6</b>	Internet Information Services (IIS) Manager – 🗖 🗖							×	
								🕶 📨 🕻	) I 🕜 🔹
File View Help									
Connections								Actions	
2									
ASmith (ASmith\Ann)	Provides rewriting capabilities base Inbound rules that are applied to	sed on rules for t the requested U	he requested UR: RL address:	L address and the co	ntent of an HTTP res	ponse.		Manage Server Varial View Server Variables	bles
a 🇊 Server Farms	Name	Input		Match	Patt	ern		Manage Providers	
	🗉 🚞 ARR_Dispatchers_loadb	URL Path		Matches	*			View Rewrite Maps	
Press Servers	🖲 🚞 Dispatcher Cookie Base	URL Path		Matches	.*			Conditions	
								Add	
								Inbound Rules	
	< Outbound rules that are applied t	o the headers or	the content of a	n HTTP response:			>	Edit Rename X Remove Disable Rule	
	Name	Input	Match	Pattern	Action Type	Action Value	St	<ul> <li>Move Up</li> <li>Move Down</li> </ul>	
								Outbound Rules	
								View Preconditions View Custom Tags	
	Features View Content View	N					>		
Configuration: 'localhost' application	Host.config								¶.:

8	Internet Information Services (IIS) Manager – 🗖								×			
G → ASmith →								🖸 🗵 🟠	• •			
File View Help												
Connections								Actions				
之								Add Rule(s)				
<ul> <li>Asmith (ASmith\Ann)</li> <li>Application Pools</li> <li>Sites</li> </ul>	Provides rewriting capabilities base Inbound rules that are applied to	sed on rules for the the requested URL	e requested URL . address:	address and the conte	ent of an HT	TP response.		Manage Server Variable View Server Variables	es			
Server Farms	Name	Input		Match		Pattern		Manage Providers				
	😑 🚰 Dispatcher Cookie Base	URL Path		Matches		*		View Rewrite Maps				
press Sciences	APP Dispatchers loadh	{HTTP_COOKIE}		Matches the Pattern	1	ASASession=([0-9,A-Fa	-f]+)	Conditions				
	ARK_Dispatchers_loadb	UKL Path		Matches				Add				
								Inbound Rules				
	<ul> <li>Outbound rules that are applied t</li> </ul>	o the headers or th	ne content of an	HTTP response:	-		>	Edit Rename Remove				
	Name	Input Match		Pattern Actio	Action Ty	Action Type Action Value		Disable Rule				
											Move Down	
								Outbound Rules				
								View Preconditions				
								View Custom Tags				
	<						>	🕜 Help				
	🔚 Features View ि Content View	v										
Configuration: 'localhost' application	Host.config								•1.:			

Solution All ARR/IIS parameters are stored in the **applicationHOST.config** file. The file is located in **C:\Windows\System32\inetsrv\config\**.

### Migrating Smartphone Authentication Dispatcher

In case of migrating Smartphone Authentication Dispatcher from one server to another, it is required to save its data storage file. The **SaDispatcherDb**-\*\*\*.sdf data storage file is located in **C:\ProgramData** folder on the server with the installed Smartphone Authentication Dispatcher. Copy this file to the **C:\Program Data** folder on the new server and run Smartphone Authentication Dispatcher.

# Index

	Α
Application 21, 23-24 Authentication 1, 3, 5, 9-11, 14-15, 17, 21-22, Authenticator 3, 5, 20, 22	37
	с
Client 3 Control 9 Control panel 9 Create 24	
	D
Database 15, 17	
	E
Edit 30	
	L
List 11 Local 16 Logon 3	
	М
Microsoft Windows Server 2008 4 Microsoft Windows Server 2012 9	
	Р
Policy 10-11 Protocol 11	
	S
Server 13, 24 Support 10, 15, 21-22 System 4	
	U

User 28

Windows 36 Windows 7 9