SSO for BOC Management Office[®] Products with Windows Authentication and IIS







Table of Contents

1	Introduction	3
2	Prerequisites	3
3	Set Up Users	3
4	Configure Tomcat	4
5	Set Up IIS 8/8.5/10	7
6	Adapt Authentication Configuration of the Web Application	23
7 Proc	Using the Reverse Proxy to Automatically Log In to the BOC Management Office	∋® 25
8	Frequently Asked Questions	25



1 Introduction

This document explains how to enable Single Sign-On (SSO) for a BOC Management Office[®] product with Windows authentication and IIS. It provides step by step instructions how to install the Microsoft Internet Information Services (IIS), connect with a Tomcat web container and forward requests to that container in a way that simulates an IDM scenario.

The currently logged in system (Windows domain) user will be used for authentication (SSO login). This means that the user is logged in automatically when opening the BOC Management Office[®] product and does not have to enter his credentials again.

2 **Prerequisites**

For the steps described in the upcoming chapters, the following prerequisites are required:

- The user account that runs the setup must have administrator rights on the target machine.
- The BOC Management Office[®] product must be installed and running properly.

3 Set Up Users

Single sign-on with Windows authentication and IIS is possible with standard product users and with system users. The following variants are possible:

- 1. Standard users are created manually in the Administration
- 2. System users are created on-the-fly when they log in for the first time

If you choose **variant 1**, set up the users in the Administration now. The option *Trusted login* needs to be enabled for all users. The usernames must match exactly with the login names of the Windows users who want to access the BOC Management Office[®] product.

If you decide to choose **variant 2**, nothing needs to be done now.

Important note: How to create users manually is described in the Administration Help. Please refer to the section "Create Users" for details.



4 Configure Tomcat

This chapter describes how to configure Tomcat for this scenario.

- In the file server.xml in "<TOMCAT>/conf", the AJP connector needs to be configured. Look for a comment similar to <!-- Define an AJP 1.3 Connector on port 8009 -->.
- 2. Add the following attributes to the connector:
 - tomcatAuthentication="false",
 - packetSize="65536",
 - secretRequired="true" and secret="<your secret keyword>"

Note: For the attribute secret, choose a strong and secure secret keyword. Only requests from <u>workers</u> with this secret keyword will be accepted.

Make sure you configure the Tomcat AJP connector according to the latest security guidelines of the documentation specific to your Tomcat version. At the time of writing, this is the current recommended way to secure the AJP connector. Please also make sure to protect the used ports from the outside.

Example:

```
<Connector protocol="AJP/1.3" port="8009" redirectPort="8443"
tomcatAuthentication="false" packetSize="65536"
secretRequired="true" secret="<your secret keyword>"/>
```

- 3. In a browser, navigate to https://downloads.apache.org/tomcat/tomcat-connectors/jk/binaries/windows/ and download the latest version of the Tomcat connector (e.g. tomcat-connectors-1.2.49-windows-x86_64-iis.zip).
- 4. Create a new folder "<*TOMCAT*>/*connector*", then extract the zip file, and copy the contained file isapi redirect.dll to that new folder.
- 5. Start **Notepad++** or a similar editor.
- 6. In the folder "<TOMCAT>/connector", create a new file called isapi_redirect.properties. Edit it as follows (adapt the path to Tomcat as necessary):

Configuration file for the Jakarta ISAPI Redirector # The path to the ISAPI Redirector Extension, relative to the website # This must be in a virtual directory with execute privileges extension_uri=/jakarta/isapi_redirect.dll # Full path to the log file for the ISAPI Redirector



```
log_file=C:\Program Files\Apache Software Foundation\Tomcat
10.1\logs\isapi_redirect.log
# Log level (debug, info, warn, error or trace)
log_level=info
# Full path to the workers.properties file
worker_file=C:\Program Files\Apache Software Foundation\Tomcat
10.1\connector\workers.properties
# Full path to the uriworkermap.properties file
worker_mount_file=C:\Program Files\Apache Software
Foundation\Tomcat 10.1\connector\uriworkermap.properties
```

7. Again in the folder "<TOMCAT>/connector", create a new file called workers.properties. Edit it as follows:

```
#
# The workers that jk should create and work with
#
worker.list=myworker
#
# Defining a worker named myworker and of type ajp13
# Note that the name and the type do not have to match.
#
worker.myworker.type=ajp13
worker.myworker.host=localhost
worker.myworker.port=8009
worker.myworker.max packet size=65536
```



Enter the secret keyword that you used in the Tomcat AJP
configuration

worker.myworker.secret=<your secret keyword>

8. Again in the folder "<TOMCAT>/connector", create a new file called uriworkermap.properties. Edit it as follows if the web application is in a specific path (replacing <webappname> with the name of the web application in Tomcat):

```
/<webappname>/* = myworker
/<webappname> = myworker
!/<webappname>/rest/* = myworker
!/<webappname>/oauth2/* = myworker
!/<webappname>/websocket/* = myworker
!/<webappname>/websocket = myworker
```

If the web application is deployed as the ROOT web application, the configuration should look like this:

```
/* = myworker
/*/* = myworker
!/rest/* = myworker
!/oauth2/* = myworker
!/websocket/* = myworker
!/websocket = myworker
```

Done! Tomcat is now ready to cooperate with IIS.



5 Set Up IIS 8/8.5/10

This chapter describes how to install IIS 8/8.5/10 using Windows Server 2012 as an example.

IIS 8 is included in Windows Server 2012 and Windows 8.0. IIS 8.5 is included in Windows Server 2012 R2 and Windows 8.1. IIS 10 is included in Windows Server 2016, Windows Server 2019 and Windows 10.

Important note: If IIS is already installed on the machine, proceed to chapter 6.

- 1. Open Server Manager.
- 2. Under Manage menu, select Add Roles and Features.



Fig. 1: Server Manager – Select Add Roles and Features

- 3. Under Server Roles, select Web Server (IIS).
- 4. Under *Web Server Role (IIS) Role Services*, in addition to the options selected by default, make sure the following entries are checked:

Web Server

Security

✓ Windows Authentication Application Development

- ✓ CGI
- ✓ ISAPI Extensions
- ✓ ISAPI Filters
- ✓ WebSocket Protocol



5. Click *Install* to finish the installation.

b	Add Roles and Features Wizard	_ 🗆 X
Installation progr	CSS DESTIN	ATION SERVER IS85.testboc.eu
Before You Begin	View installation progress	
Installation Type	() Feature installation	
Server Selection		
Server Roles	Installation started on IIS85.testboc.eu	
Features	Web Server (IIS)	^
Confirmation	Web Server	
Results	Common HTTP Features	
	Static Content	
	Default Document	
	Directory Browsing	
	HTTP Errors	
	Security	
	Request Filtering	
	Windows Authentication	\sim
	You can close this wizard without interrupting running tasks. View task progress or page again by clicking Notifications in the command bar, and then Task Details. Export configuration settings	open this
	< Previous Next > Close	Cancel

Fig. 2: Server Manager – Installation progress

- 6. Download and install the following additional modules for IIS:
 - URL Rewrite
 - Application Request Routing
- 7. Make sure that nothing on your machine is running on port 80, as IIS will try to use that port.
- 8. After everything is installed you can open a browser and navigate to "*http://localhost*". You should see the following:



Fig. 3: Navigate to http:/localhost



9. On the *Start* screen, click *Control Panel*, click *Administrative Tools*, and then double-click *Internet Information Services (IIS) Manager*.

🖄 l ⊋ 📗 = l			Shortcut Tools	Application Tools	Administrative Tools					
File Home	Share Vie	ew	Manage	Manage					~ ()	
	• Control P	anel	 All Control Pa 	anel Items 🕨 Admin	istrative Tools	~ ¢	Search Administrati	ve Tools	Q	
A Favorites					Name	Date modified	Туре	Size		
Desktop					Terminal Services	22.08.2013 17:39	File folder			
🐌 Downloads					Component Services	22.08.2013 08:57	Shortcut		2 KB	
🔢 Recent places	5				🛃 Computer Management	22.08.2013 08:54	Shortcut		2 KB	
					befragment and Optimize Drives	22.08.2013 08:47	Shortcut		2 KB	
🖉 🌉 This PC					🛃 Event Viewer	22.08.2013 08:55	Shortcut		2 KB	
🛯 🎥 Desktop					훩 Internet Information Services (IIS) Manager	22.08.2013 08:50	Shortcut		2 KB	
📗 Documents					😥 iSCSI Initiator	22.08.2013 08:57	Shortcut		2 KB	
🛯 🚺 Downloads					🛃 Local Security Policy	22.08.2013 08:54	Shortcut		2 KB	
🛯 🍑 Music					DDBC Data Sources (32-bit)	22.08.2013 01:56	Shortcut		2 KB	
📄 📔 Pictures					📷 ODBC Data Sources (64-bit)	22.08.2013 08:59	Shortcut		2 KB	
🔋 📔 Videos					Performance Monitor	22.08.2013 08:52	Shortcut		2 KB	
🕍 Local Disk (C	:)				Resource Monitor	22.08.2013 08:52	Shortcut		2 KB	
					here a security Configuration Wizard	22.08.2013 08:45	Shortcut		2 KB	
👊 Network					🔁 Server Manager	22.08.2013 08:55	Shortcut		2 KB	
					🖓 Services	22.08.2013 08:54	Shortcut		2 KB	
					🖾 System Configuration	22.08.2013 08:53	Shortcut		2 KB	
					👰 System Information	22.08.2013 08:53	Shortcut		2 KB	
					Task Scheduler	22.08.2013 08:55	Shortcut		2 KB	
					🔗 Windows Firewall with Advanced Security	22.08.2013 08:45	Shortcut		2 KB	
					🔊 Windows Memory Diagnostic	22.08.2013 08:52	Shortcut		2 KB	
					🔀 Windows PowerShell (x86)	22.08.2013 17:37	Shortcut		3 KB	
					Windows PowerShell ISE (x86)	22.08.2013 08:55	Shortcut		2 KB	
					Windows PowerShell ISE	22.08.2013 08:55	Shortcut		2 KB	
					🐌 Windows Server Backup	22.08.2013 08:53	Shortcut		2 KB	
24 items 1 item s	elected 1,10 KE	3			د [111				

Fig. 4: Open the Internet Information Services Manager

Important note: If during the following steps you find that a required feature is not installed, add it through the Server Manager.

10. In the *Connections* pane, select the root element. In the *Home* pane, open the *ISAPI and CGI Restrictions*.

v j	Internet Information Services (IIS) Manager	- 0 ×
File View Help		₩ ≥ 9 € .
File View Help Connections Co	Fite: • @ Go • @ Show All Group by: Area • @ • Is Is Is Is Authentic CGI Compression Default Directory Error Pages FatCGI Handler HTTP IsAPI and IsAPI Filters Logging MIME Types Modules IsAPI Filters Coging MIME Types Modules IsaPi Endition Erver Worker Certificates Processes Configurat Feature Shared Shared Shared Editor Delegation Configurat Shared Shared	Actions Open Feature Manage Server Restart Stop View Application Pools View Stes Get New Web Platform Components Help

Fig. 5: Open ISAPI and CGI Restrictions



11. In the Actions pane, click Add... to add the isapi redirect.dll.



Fig. 6: Add isapi_redirect.dll

12. Choose a *Description* and set *ISAPI or CGI path* to the physical location of the isapi_redirect.dll. Select the option "Allow extension path to execute".

Edit ISAPI or CGI Restriction ? ×							
ISAPI or CGI path: C:\Program Files\Apache Software Foundation\Tomcat 😂\coni 🔐							
Description:							
isapi_redirect.dll							
✓ Allow extension path to execute							
OK Cancel							

Fig. 7: Select the option "Allow extension path to execute"



13. In the *Connections* pane, select the *Default Web Site*. In the *Home* pane open *ISAPI Filters*.

9	Internet Information Services (IIS) Manager	- 0 ×
 Image: A state Image: A state<th>Sites > Default Web Site ></th><th>□ ≥ \} 0 ·</th>	Sites > Default Web Site >	□ ≥ \} 0 ·
File View Help Connections Connections Start Page Connection Start Page Start Page Connection Start Page Start	Image: Second and a second	Actions Open Feature Suppore Edit Dremissions Edit Stee Bindings Basic Settings View Applications View Virtual Directories Manage Website Start Start Start Browse Website Browse Vbolkte Browse Vbolkte Configure Limits Hep
< 111 >	Teatures View a Content View	
Ready		63

Fig. 8: Select the Default Web Site and in the Home pane open the ISAPI-Filter

14. In the Actions pane, click Add... to create an ISAPI filter. Choose a Filter name. Set Executable to the physical location of the isapi redirect.dll.

	Add ISAPI Filter	? X
Filter name:		
isapi_redirect		
Executable:		
C:\Program Files\Apache	Software Foundation\Tomcat 🕼	Aconnector
	ОК	Cancel

Fig. 9: Create an ISAPI filter



15. In the *Connections* pane, right click the *Default Web Site* and click *Add Virtual Directory*.... The *Alias* of this directory should be *Jakarta*. The *Physical path* should point to the directory where you have placed the isapi redirect.dll:

Site name: Default Web Site Path: / Alias: Jakarta Example: images Physical path: C:\Program Files\Apache Software Foundation\Tomcat ` Pass-through authentication Connect as Test Settings OK Cancel	Add Virtual Directory ? 🗙
Alias: Jakarta Example: images Physical path: C:\Program Files\Apache Software Foundation\Tomcat ` Pass-through authentication Connect as Test Settings OK Cancel	Site name: Default Web Site Path: /
Jakarta Example: images Physical path: C:\Program Files\Apache Software Foundation\Tomcat ` Pass-through authentication Connect as Test Settings OK Cancel	Alias:
Example: images Physical path: C:\Program Files\Apache Software Foundation\Tomcat Pass-through authentication Connect as Test Settings OK Cancel	Jakarta
Physical path: C:\Program Files\Apache Software Foundation\Tomcat ` Pass-through authentication Connect as Test Settings OK Cancel	Example: images
C:\Program Files\Apache Software Foundation\Tomcat ` Pass-through authentication Connect as Test Settings OK Cancel	Physical path:
Pass-through authentication Connect as Test Settings OK Cancel	C:\Program Files\Apache Software Foundation\Tomcat
Pass-through authentication Connect as Test Settings OK Cancel	
Connect as Test Settings OK Cancel	Pass-through authentication
OK Cancel	Connect as Test Settings
OK Cancel	
OK Cancer	OK Cancel
	OK

Fig. 10: Create virtual directory "Jakarta"

16. Select the new virtual directory *Jakarta* in the *Connections* pane. In the *Home* pane, open *Handler Mappings*.



Fig. 11: Select virtual directory "Jakarta" and open the Handler Mappings



	Sites > Default Web Site > 1	akarta 🕨				
Ele View Hele	Sites 7 below rice site 7 7					
Connections						Actions
Image Image <t< td=""><td>Handler Map Use this feature to specify the request types. Group by: State</td><td>opings e resources, such as [</td><td>DLLs and managed co</td><td>de, that handle respo</td><td>nses for specific</td><td>Add Managed Handler Add Script Map Add Wildcard Script Map Add Module Mapping</td></t<>	Handler Map Use this feature to specify the request types. Group by: State	opings e resources, such as [DLLs and managed co	de, that handle respo	nses for specific	Add Managed Handler Add Script Map Add Wildcard Script Map Add Module Mapping
A O Default Web Site	Name Enabled	Path	State	Path Type	Handler	Edit Feature Permissions Revert To Parent
	CGI-exe ISAPI-dll OPTIONSverbHandler TRACEVerbHandler StaticFile	.exe .dl	Enabled Enabled Enabled Enabled Enabled	File File Unspecified Unspecified File or Folder	CgiModule IsapiModule ProtocolSuppc ProtocolSuppc StaticFileMods	View Ordered List
111 >>	<	III t View			>	

17. In the Actions pane, click Edit Feature Permissions....

Fig. 12: Edit Feature Permissions

18. Make sure that all check boxes are ticked as you need the right to execute scripts.



Fig. 13: Select all check boxes



File View Help						
Connections						Actions
A, - III 2 I B, C Start Page A C Application Pools	Use this feature to specify the request types.	prings e resources, such as	DLLs and managed co	de, that handle respo	nses for specific	Add Managed Handler Add Script Map Add Wildcard Script Map. Add Module Mapping
a - O Sites	Name	Dath	State	Path Tune	Handler	Edit Feature Permissions
p 💭 Jakarta	Enabled	Faun	Jace	Path type	rianuler	Revert To Parent
	CGI-exe	*.exe	Enabled	File	CaiModule	View Ordered List
	ISAPI-dil	*.dll	Enabled	File	IsapiModule	Help
	OPTIONSVerbHandler		Enabled	Unspecified	ProtocolSuppo	
	TRACEVerbHandler		Enabled	Unspecified	ProtocolSuppc	
	StaticFile		Enabled	File or Folder	StaticFileModu	
	٢.	ш			>	

19. In the Actions pane, click Add Module Mapping....

Fig. 14: Add Module Mapping

20. Type the file name extension *.dll in the *Request path* box. Click *IsapiModule* in the *Module* drop-down list. Set *Executable (optional)* to the physical location of the <code>isapi_redirect.dll</code>. Choose a *Name* for the module mapping.

	Add Mod	ule Map	oing	?	x
Request path:					
*.dll					
Example: *.bas, wsvc.axd	¥.				
Module:					
IsapiModule				~]
Executable (optional):					
C:\Program Files\Apach	Software For	undation\T	omcat 🔍 co	nnector .	
Name:					
Tomcat Redirector					
Request Restrictions					
			ОК	Cance	I

Fig. 15: Add Module Mapping II



21. To the question Do you want to allow this ISAPI extension?, click Yes.



Fig. 16: Add Module Mapping III

22. In the *Connections* pane, select the root element. In the *Home* pane, open *Feature Delegation*.



Fig. 17: Open Feature Delegation



23. Make sure that the default delegation state for *Handler Mappings* is *Read/Write*.

V j	Internet Information Services (IIS) Manager	X
Co		<u> </u>
File View Help		
File View Help Connections Provide the second	egation ethe default delegation state for features at lower levels in IIS Manager.	Actions Set Feature Delegation Read Write Read Only Not Delegated Reset to Inherited Reset All Delegation Cuttom Site Delegation V Heip
< III > Features View 🖧 Conter	nt View	
Configuration: 'localhost' root web.config		·1.:

Fig. 18: Set the default delegation state for the feature "Handler Mappings" to "Read/Write"

24. Select the virtual directory *Jakarta* in the *Connections* pane. In the *Home* pane, open *Authentication*.

9	Internet Information Services (IIS) Manager	_ 0 X
	Sites + Default Web Site + Jakarta +	○ ○ ④ 1 ● •
File View Help Connections S. I S.	Jakarta Home	Actions Open Feature
Start Page	Filter: • Go • • Show All Group by: Area • If IS • Go • • Show All Group by: Area • If Authentication • Go • • Show All Group by: Area • If IS • Go • • Show All Group by: Area • If IS • Go • • Show All Group by: Area • If IS • Go • • Show All Group by: Area • If IS • Go • • Show All Group by: Area • If Authentication • Decument Browsing • If Image: Configure authentication settings for sites and application: • If Image: Image: Configure authentication settings for sites and application: • Statings Management • Configuret • Statings Editor • Statings • Statings Configuret • Editor • Origouret	Septence Edit Permissions Edit Permissions Back Settings Rowse Virtual Directory Advanced Settings Help
Ready		61
		1

Fig. 19: Open Authentication



25. Disable everything but Windows Authentication:

Authentication Start Page Application Pools Sites Application Pools Application Pools Application Pools Application Disabled Application Disabled	AUTRENTICATION Application Pools Sites Default Web Site Diabled Status Asp NET Impersonation Diabled Mindows Authentication Enabled HTTP 401 Challenge Http	21 😣	Authentication			
Group by: No Grouping - Name • Status Response Type Application Pools Group Datult Web Site b 2 Jakarta Group Market Status ASP NET Impersonation Windows Authentication Enabled HTTP 401 Challenge	Application Pools Status Response Type Anonymous Authentication Disabled Anonymous Authentication b Default Web Site ASP.NET Impersonation Disabled Mane Windows Authentication Enabled HTTP 401 Challenge					😧 Help
Application Pools → Gites → D Fault Web Site → → Jakarta Name Status Response Type Anonymous Authentication Disabled Windows Authentication Disabled Windows Authentication Disabled Windows Authentication Disabled HTTP 401 Challenge	Application Pools Name Statu Response Type ▲ Drabled Disabled Disabled ▶ 20 Jakants Windows Authentication Disabled Windows Authentication Enabled HTTP 401 Challenge	art Page	Group by: No Grouping •			
A comprove Authentication Disabled ASP.NET Impersonation Disabled Stabled + Windows Authentication Enabled HTTP 401 Challenge	Sites Anonymous Authentication Disabled A ASP.NET Impersonation Disabled A Mindows Authentication Enabled HTTP 401 Challenge	Application Pools	Name	Status	Response Type	
O Labeled ¹ ⁶ Windows Authentication Disabled ¹ ⁶ Windows Authentication Enabled HTTP 401 Challenge	Objust ASP.NET Impersonation Disabled NS b Windows Authentication Enabled HTTP 401 Challenge	Sites	Anonymous Authentication	Disabled		
▶ 🔊 Jakarta Windows Authentication Enabled HTTP 401 Challenge	b- ∰ Jakarta Windows Authentication Enabled HTTP 401 Challenge	Default Web Site	ASP.NET Impersonation	Disabled 18		
		þ 💭 Jakarta	Windows Authentication	Enabled	HTTP 401 Challenge	

Fig. 20: Deactivate everything but "Windows Authentication"

- 26.Next, Authentication settings for the Default Web Site need to be created. Repeat steps 24 - 25. Make sure to select the Default Web Site in the Connections pane before you start. On the Authentication page, disable everything but Anonymous Authentication.
- 27. In the *Connections* pane, select the *Default Web Site*. In the *Home* pane, open *Request Filtering*.



Fig. 21: Open Request Filtering



Connections		Alerts
Image: Constraint of the second se	Request Filtering Use this feature to configure filtering rules.	iFile name extensions that appear in the list and have Allowed set to False are blocked. No other file nam extensions are blocked.
	File Extension Allowed	Actions
		Allow File Name Extension. Deny File Name Extension
		Edit Feature Settings

28. In the Actions pane, select Edit Feature Settings.

Fig. 22: Edit Feature Settings

29. Make sure that Allow double escaping is allowed. Set Maximum allowed content length (Bytes) to the maximum size of data that IIS should accept, such as for file uploads. To calculate the value in bytes, use the formula 1 MB = 1.048.576 bytes. For example, to allow the import of a 100 MB migration package, set the value to 104857600 bytes. Confirm your changes with OK. These settings will automatically apply to the virtual directory Jakarta as well, unless they are explicitly modified there.

General Allow unlisted file name extensions Allow unlisted verbs Allow high-bit characters Allow double escaping Request Limits Maximum allowed content length (Bytes): 104857600 Maximum URL length (Bytes): 4096 Maximum query string (Bytes): 2048	E	dit Reque	est Filte	ring Set	tings	?	X
 Allow unlisted file name extensions Allow unlisted verbs Allow high-bit characters Allow double escaping Request Limits Maximum allowed content length (Bytes): 104857600 Maximum URL length (Bytes): 4096 Maximum query string (Bytes): 2048 	General						
 Allow unlisted verbs Allow high-bit characters Allow double escaping Request Limits Maximum allowed content length (Bytes): 104857600 Maximum URL length (Bytes): 4096 Maximum query string (Bytes): 2048 	Allow unlist	ted file name	e extensi	ons			
 Allow high-bit characters Allow double escaping Request Limits Maximum allowed content length (Bytes): 104857600 Maximum URL length (Bytes): 4096 Maximum query string (Bytes): 2048 	Allow unlist	ted verbs					
 Allow double escaping Request Limits Maximum allowed content length (Bytes): 104857600 Maximum URL length (Bytes): 4096 Maximum query string (Bytes): 2048 	Allow high-	bit characte	ers				
Request Limits Maximum allowed content length (Bytes): 104857600 Maximum URL length (Bytes): 4096 Maximum query string (Bytes): 2048	Allow doub	le escaping					
Maximum allowed content length (Bytes): 104857600 Maximum URL length (Bytes): 4096 Maximum query string (Bytes): 2048	Request Limits						
104857600 Maximum URL length (Bytes): 4096 Maximum query string (Bytes): 2048	Maximum allo	wed content	length (Bytes):			
Maximum URL length (Bytes): 4096 Maximum query string (Bytes): 2048	104857600						
4096 Maximum query string (Bytes): 2048	Maximum URL	length (Byte	es):				
Maximum query string (Bytes): 2048	4096						
2048	Maximum que	ry string (By	tes):				
	2048						
				OK		Cancel	
				OK		Cancel	

Fig. 23: Edit Request Filtering Settings



30. In the *Connections* pane, select the root element. In the *Home* pane, open *Application Request Routing Cache*.



Fig. 24: Open Application Request Routing Cache

31. In the Actions pane, select Server Proxy Settings.

File View Help					
Connections			Calaba		Actions
21		Request Routing (Lache		Cache Management
	Use this feature to view rur	ntime statistics for Application	n Request Routing. Use the A	ctions	Cache Configuration
Application Pools	to configure disk cache set	tings and manage cached co	ntent.		Cache Control Rules
Server Farms	Drive Location	Priority	Health Status	Maxir	Drive Management
					Add Drive
					Preus
					Server Prox/ASettings
					P Help

Fig. 25: Select Server Proxy Settings

32. Select *Enable proxy*. Under *Custom Headers*, disable *Include TCP port from client IP*. Leave the other settings unchanged. Confirm with *Apply*.

File View Help		
Connections	Application Request Routing	Alerts Server routing rules have not
> • • • • • • • • • • • • • • • • • • •	Use this feature to configure proxy settings for Application Request Routing.	been created. Click "Use URL Rewrite to inspect incoming requests" to create these
	Enable proxy	rules.
	Proxy Setting	Enabling proxy allows
	HTTP version:	requests to be potentially routed to servers outside of
	Pass through \checkmark	your server farm.
	Keep alive	Actions
	Time-out (seconds):	E∕ Apply E∕ CsDel
	120	🗢 Back to ARR Cache
	Reverse rewrite host in response headers	Advanced Routing URL Rewrite
	Custom Headers	🕡 Help
	Preserve client IP in the following header:	
	X-Forwarded-For	
	Include TCP port from client IP	
	Forwarding proxy header value:	
	La la	

Fig. 26: Select Enable Proxy and Apply



33. In the *Connections* pane, select the *Default Web Site*. In the *Home* pane open *URL Rewrite*.



Fig. 27: Open URL Rewrite

34. In the Actions pane, select Add Rule(s).

Connections		wite		Actions	
Application Pools Sites Default Web Site	Provides rewriting ca content of an HTTP r Inbound rules that ar	write pabilities based on rules for the r esponse. re applied to the requested URL a	equested URL address and the	Add Rule(s) Revent to Parent Manage Server Varial View Server Variables	oles
> - 🏭 Server Farms	Name	Input	Match	Manage Providers View Rewrite Maps View Providers	
				Inbound Rules	•
				Import Rules	
				Outbound Rules	•
				View Preconditions View Custom Tags	
	<	_	:	Help	





35. Now, an inbound rule for REST requests needs to created so those specific requests are not processed with the AJP protocol and Windows authentication, but directly forwarded via HTTP to Tomcat. Select *Blank rule* and confirm with *OK*.

Add Rule(s)		?	×
Select a rule template:		1	
Inbound rules	😹 Rule with rewrite map		
Inbound and Outbound Rules	Reverse Proxy		
Search Engine Optimization (SEO) Enforce lowercase URLs Append or remove the trailing sla	Canonical domain name ash symbol		
Select this template to create a new in you can use to define a new rewrite n	nbound rule without any preset values. This template opens the "E ule for changing the requested URL address.	dit Rule" pag	e that
	ОК	Cance	el

Fig. 29: Select Blank Rule and OK

36. Enter a name for the new rule, such as "*REST to Tomcat*". From the *Using* list, select *Wildcards*. In the *Pattern* box, enter ADO*/rest/* if the web application is in a specific path or rest/* if the web application is deployed as the ROOT web application. Under *Action Properties*, in the *Rewrite URL* box, enter the Tomcat URL, including the protocol, host, and port, followed by {PATH_INFO} which dynamically appends the path after the host and port. For example, for a local Tomcat setup with the HTTP/1.1 connector port set to "8000", the URL would be: http://localhost:8000{PATH_INFO}. Confirm with *Apply*, and then click *Back to Rules*.

	C dit Inhound Dulo	Actions
		Apply
i si seng	Name:	🖳 🖒 Cel
ication Pools	REST to Tomcat	🗢 Back to Rules
efault Web Site		😧 Help
er Farms	Match URL 📀	
	Requested URL: Using:	
	Matches the Pattern \checkmark Wildcards \checkmark	
	1 Sheep	
	Pattern:	
	Abu 7/rest - lest pattern	
	✓ Ignore case	
	Conditions	
	Server Vanables	
	Action	
	Action type:	
	Rewrite \vee	
	Action Properties	
	Rewrite URL:	
	Inttp://iocainost:8000(PATH_INFO)	
	C Append duciy string	
	Log rewritten URL	
	Stop processing of subsequent sules	
	L stop processing of storeducit rules	

Fig. 30: Edit REST Rule



- 37.Next, inbound rules for OAuth2 and WebSocket need to be created. Repeat steps **34 36** and enter the following data:
 - OAuth2 rule: Name e.g. "OAuth2 to Tomcat". For Using, select Wildcards. For Pattern, enter ADO*/oauth2/* or oauth2/* if the web application is deployed as ROOT. For Rewrite URL, enter the Tomcat URL followed by {PATH INFO}.
 - WebSocket rule: Name e.g. "WebSocket to Tomcat". For Using, select Wildcards. For Pattern, enter ADO*/websocket or websocket if the web application is deployed as ROOT. For Rewrite URL, enter the Tomcat URL followed by {PATH INFO}? axx socket fwd=true.

ns	Chit Inhound Pule	Act	ions
			Apply
E-# BCGeoglyceng(Name:	I 🖳	Callel
Application Pools	websocket to iomcat		Back to Rules
Default Web Site		0	Help
erver Farms	Match URL		
	Requested URL: Using:		
	Matches the Pattern V Wildcards	~	
	Pattern:		
	ADO*/websocket	Test pattern	
	☑ Ignore case		
	Conditions	 Image: Second sec	
	Server Variables		
		0	
	Action	•	
	Action type:		
	Rewrite		
	Action Properties		
	Provide UPL		
	http://localhost:9000/PATH INFOl2 ave socket fudetrue		
	http://idealiost.coco(PAIn_INPO/:_axx_socket_iwd-tide		
	Annend query string		
	L Log rewritten UKL		

Fig. 31: Edit OAuth2 and WebSocket Rules

- IIS is now configured and can be used as reverse proxy for Tomcat.
 - 38. To finalize the configuration, restart IIS. Select the root folder in the *Connections* pane. In the *Action* pane, click *Restart*.
 - 39. Also restart Tomcat.



6 Adapt Authentication Configuration of the Web Application

The setup of for a BOC Management Office[®] product using Windows authentication and IIS requires the configuration of certain connection parameters and directory service specific properties in the *Administration*:

Enter the URL where the BOC Management Office[®] product is available, click
 Administration, enter your credentials and log in.

Note: The user must have access rights to the "Administration Toolkit" component.

- 2. Go to *Authentication* > *Connectors*, and then click *Create*.
- 3. In the *ID* box, enter a unique name for your connector.
- 4. From the Select type list, select IDM.
- 5. Click *Create*. Once you have created the connector, you can start working on the configuration right away.
- 6. On the IDM connector's *Properties* page, modify the following parameters:
 - Make sure the *Crop the domain extension of the remote username* check box is selected.
 - In the Regular expression to replace strings in the username with another string box, enter the following regular expression: "^.*\\" (without the quotation marks). This cuts the domain identifier from the passed user name because the login procedure only takes user names without domain names. By specifying this, the user name "<DOMAIN NAME>\user" becomes just "user ".

Note: We assume that the users that we want to log in are in one domain, so the usernames that are passed to the BOC Management Office® product by IIS will e.g. be "<DOMAIN NAME>\user", "<DOMAIN NAME>\test" etc.

- 7. On the IDM connector's *User mapping* page, modify the following parameters:
 - Under *Roles*, specify the *Default roles* that should be assigned to automatically created users (<u>variant 2</u>). Define any number of such elements.
 - Under *Groups*, specify the *Default groups* that should be assigned to automatically created users (**variant 2**). If none of the user groups exists, users are assigned to the standard group.
 - Under Repositories, specify the *Baseline assignments* i.e. repositories that will be automatically assigned to every user.
 - Under Synchronize user, set Create user automatically as follows:



- Disable this option if you set up the users manually in the Administration (<u>variant 1</u>)
- Enable this option if users should be created on-the-fly in the database when they log in for the first time (**variant 2**).
- 8. Click *OK* to return to the *Connectors* page.
- 9. Find the IDM connector and select the *Connector enabled* check box.
- 10. Use the drag handle (=) to move the IDM connector to the top of the list, prioritising it as the primary authentication mechanism.

IDM-based authentication is now activated and will be used as the default connector. The standard connector ("Standard Login", the standard login page) is activated as well and can be used in case that additional constraints are defined for the IDM connector. Do not disable the standard connector.

Note: In this chapter, we focus on the minimum essential parameters needed for IDM authentication setup. For a comprehensive overview of all configurable parameters, please refer to the "Authentication" chapter in the Administration Help.

For instance, the login process can be configured to support a hybrid approach with multiple connectors, allowing specific connectors only for requests originating from certain IP addresses. Additionally, LDAP properties can be mapped to BOC Management Office[®] product user groups and system roles, enabling the assignment of tailored permissions based on the user's role and department within the organisation. The IDM connector must be configured to use LDAP coupling in this case.

Done! Restart the Apache Tomcat web server. For users logged in with their domain accounts in a domain which the IIS service can access, SSO is now supported.



7 Using the Reverse Proxy to Automatically Log In to the BOC Management Office® Product

Prerequisites

The following prerequisites must be met so that a user can log in to the BOC Management Office[®] product using Windows authentication and IIS:

- IIS must be reachable for all users that should have access to the BOC Management Office[®] product.
- IIS must have access to the user management component (e.g. Active Directory).
- The web browser must be configured to send the login credentials of the currently logged in users to IIS. This works out of the box for Google Chrome and Microsoft Edge. For other browsers the browser configuration needs to be adapted.

Login

In order to access the BOC Management Office[®] using Windows authentication and IIS:

• Navigate to "*http://localhost/<PRODUCT><VERSION>*" (again, no port as IIS is running on port 80).

The currently logged in Windows user should be directly logged in to the BOC Management Office[®] product.

If you set up the users manually in the Administration (<u>variant 1</u>), a user with a name exactly matching the name of the Windows user must exist in the database. *Trusted login* needs to be enabled for this user.

If users should be created on-the-fly in the database when they log in for the first time (<u>variant 2</u>), a new user is created automatically. The mapping of user attributes (group assignment etc.) is synchronized on each subsequent login.

8 Frequently Asked Questions

The log file for the ISAPI redirector *isapi_redirect.log* is not created. What should I do?

Specify a path without blanks, e.g. create a new folder "C:\Temp", and then adapt the path to the log file in the file <code>isapi_redirect.properties</code> accordingly.

How can I deploy the web application as the ROOT application

- 1. Stop the Apache Tomcat web server.
- 2. Remove the folder \webapps\ROOT in the Tomcat installation directory.
- 3. Rename the WAR file to ROOT.war.
- 4. In the file uriworkermap.properties, remove the name of the web application:



```
/* = myworker
/*/* = myworker
```

5. Restart IIS and the Apache Tomcat web server.